UNIVERSIDAD ESTATAL A DISTANCIA
VICERRECTORÍA ACADÉMICA
ESCUELA DE CIENCIAS DE LA ADMINISTRACIÓN
Programa de Doctorado e n Ciencias de la Administración

DÉFICIT Y OPORTUNIDADES DE LA LEGISLACIÓN COSTARRIC ENSE SOBRE COMERCIO ELECTRÓNICO: UN APORTE DESDE LA PERSPECTIVA DE LA SEGURIDAD, LA PROTECCIÓN DE DATOS Y LOS DERECHOS DEL CONSUMIDOR.

Tesis de Graduación sometida a la consideración
del Tribunal Examinador del Programa de Doctorado en Ciencias de la Administración
de la Escuela de Ciencias de la Administración para optar
al grado de:

Doctor

Por

Susan Chen Sui

San José, Costa Rica
2008

Esta tesis ha sido aceptada y aprobada, en su forma presente, por el Tribunal Examinador del Programa de Doctorado en Ciencias de la Administración de la Escuela de Ciencias de la Administración de la Universidad Estatal a Distancia, como requisito parcial para optar al grado de:

DOCTOR

_____
Dra. Nidia Lobo Solera
Directora del Sistema de Estudios de Posgrado

_____
Dr. Miguel Gutiérrez Alfaro
Director de la Escuela de Ciencias de la Administración

_____
Dr. Miguel Gutiérrez Alfaro
Coordinador del Programa de Doctorado en Ciencias de la Administración

_____
Dr. Alfredo Chirino Sánchez
Director de Tesis

_____
Dra. Gabriela Marín Raventós
Lectora

_____
Dr. Juan Marco Rivero Sánchez
Lector

_____
Susan Chen Sui
Estudiante

Febrero 2008

DEDICATORIA

A Dios, a mi madre y a mis hijas Iris y Julie

AGRADECIMIENTO

A mi director de tesis Dr. Alfredo Chirino Sánchez

Y a mis lectores de tesis:
Dra. Gabriela Marín Raventós
Dr. Juan Marco Rivero Sánchez

Por su invalorable guía, consejos, apoyo y tiempo.

TABLA DE CONTENIDO

TABLA DE CUADROS

TABLA DE FIGURAS

Capítulo 1. El Problema y su importancia

1.1 Planteamiento del problema e importancia

El comercio electrónico se ha desarrollado en los últimos años a un nivel mundial. De acuerdo con el Informe de la UNCTAD (2003), la Economía Digital sigue creciendo con gran empuje. En lo que se refiere a la utilización de Internet, el Informe indica que los países en desarrollo siguen creciendo a un ritmo más rápido que los países desarrollados. A fines de 2002, el número de usuarios de Internet de los países en desarrollo representaban el 32% de los 591 millones de usuarios de Internet del mundo, frente al 28% del año 2001, y que muy bien podrían llegar a representar el 50% en el 2008.

Estas estimaciones, constituyen una indicación razonablemente correcta de hasta qué punto existen en un país determinado las bases de una "economía digital". Indica el informe que los países donde efectivamente existen esas bases, cuyos gobiernos han impulsado el desarrollo de la sociedad de la información desde un principio (como, por ejemplo, el Japón, Malasia, Singapur y los Estados Unidos de América), han sacado provecho de las tecnologías de información y comunicación (TIC's) mucho antes.

Otro informe de Diciembre de 2004 de la UNCTAD, indica que Costa Rica está en segundo lugar en América Latina con un 34% de los hogares con computadoras.

La expansión de las TIC's para la economía nacional, tiene un efecto positivo para todos los factores que afectan a la productividad y en Costa Rica se ha impulsado el desarrollo de la tecnología desde hace varios años.

El Gobierno costarricense ha realizado grandes esfuerzos para informatizar la educación pública, creándose en 1987 la Fundación Omar Dengo para desarrollar programas en el área de informática para la educación primaria y secundaria. Paralelamente, también se ha impulsado el desarrollo de las tecnologías de información y comunicación en la Administración Pública y en el ofrecimiento de éstas a la comunidad nacional. Puede verse el desarrollo que ha tenido Internet, mejorando

cada vez: la capacidad de transmisión, el costo, la cobertura, permitiendo mayor accesibilidad a la red de redes a todos los ciudadanos.

Hoy día se puede ver el fruto de esas decisiones, puesto que Costa Rica está catalogada entre los países latinoamericanos con mejor posición tecnológica para asumir la economía digital.

Sin embargo, el paso a esta economía digital, traerá ventajas y desventajas que deben ser analizadas desde diversos ángulos, como lo son el económico, social, cultural, jurídicos entre otros.

Costa Rica no puede ignorar la revolución que está provocando el desarrollo de las tecnologías de información y comunicación, la cual impacta enormemente en todos los ámbitos de la vida actual y futura.

Aunque las empresas costarricenses y en general la población costarricense apenas están iniciando las experiencias en el campo del comercio electrónico, y el paso sea más lento, se vislumbra en definitiva su desarrollo. Acuña (2006) indica que en América Latina se está expandiendo rápidamente el comercio electrónico, y que en Costa Rica se registró en el año 2005, un crecimiento del 32% con respecto al año anterior, en cuanto a volumen de ventas realizadas por Internet procesadas sólo con productos Visa; alcanzando los 43 millones de dólares. La facturación a través de Visa Internacional de ventas por Internet en América Latina alcanzó los 2 mil millones de dólares en volumen en el 2005. Brasil y México representaban más de la mitad de este volumen total; Venezuela y Chile registraron el mayor crecimiento en el último año, 185% y 100% respectivamente.

La discusión del comercio electrónico se puede realizar desde varias aristas, desde el punto de vista económico, social, cultural, técnico informático y jurídico. Cada uno de estas aproximaciones conlleva un trabajo de gran profundidad y magnitud. Por tal motivo, se propone en esta investigación, abordar únicamente el punto de vista de regulación y técnico informático del comercio electrónico.

Es necesario para ello, y tomando en cuenta la experiencia de otros países, iniciar el análisis del comercio electrónico desde la perspectiva de las condiciones del país en materia jurídica para asumir adecuadamente el desarrollo del comercio electrónico. Este análisis debe realizarse referido a sus leyes, la oportunidad de competencia y nuevos mercados, las posibilidades de inversión, el papel estratégico para el desarrollo de la economía.

La situación concerniente a la regulación del comercio electrónico, es una problemática que está siendo debatida a nivel mundial. Muchos países ya han establecido una legislación al respecto, sin embargo, todavía existen muchos vacíos que no han sido posibles resolver. Estados Unidos y la Unión Europea tiene muy adelantado soluciones a diferentes aspectos de la regulación del comercio electrónico, pero en los países latinoamericanos todavía la regulación de este tipo de transacciones electrónicas está en pañales, y Costa Rica es uno de ellos. En el país se han realizado estudios específicos acerca de la situación jurídica costarricense en materia de comercio electrónico, sin embargo, éstas sólo cubren un aspecto específico de lo regulado.

De acuerdo con Hess (2006), el nuevo Gobierno costarricense[1] tiene un reto en el campo tecnológico, el cual es potenciar el uso de tecnología de punta en toda clase de transacciones públicas y privadas, y específicamente, indica que será necesario trabajar fuertemente en dos campos: gobierno digital y comercio electrónico.

En cuanto al comercio electrónico, indica Hess:

> "convendría explorar vías legales que remuevan barreras existentes a su expansión, así como mecanismos de fomento que lo incentiven." (Hess, 2006, p.36 A).

Indica que los factores críticos de éxito para el crecimiento del comercio electrónico son especialmente los de la seguridad y la privacidad de la información tanto personal como transaccional de los consumidores. Además de otros como los referentes a la publicidad comercial electrónica no solicitada que crece impunemente en Costa Rica.

[1] El artículo periodístico se publica el día 2 de abril 2006, se realizaron elecciones presidenciales el día 5 de febrero de 2006. El nuevo Gobierno costarricense toma posesión el día 8 de mayo de 2006.

Por lo tanto, se trata de establecer unos requisitos "*mínimos"* que han de cumplirse en el comercio electrónico, que garanticen un comercio electrónico de calidad y de acuerdo con la ley.

Con una legislación acorde se pretende facilitar el desarrollo del comercio electrónico, sin detrimento de las garantías de los usuarios. La introducción de las nuevas tecnologías en la sociedad costarricense debe hacerse de tal forma que se lleve a cabo dinamizando el tejido empresarial y, al mismo tiempo, protegiendo suficientemente los derechos de los usuarios, estableciéndose las garantías en forma oportuna.

El fin último es proteger al consumidor, proveedor y Estado de los posibles delitos informáticos que pueden llevarse a cabo por la apertura y el crecimiento de este tipo de comercio.

La intención de la presente investigación es hacer una revisión de las recomendaciones de los organismos internacionales en materia de regulación del comercio electrónico, y conocer las experiencias de los países latinoamericanos que ya han dado pasos a este respecto para identificar tendencias y aspectos importantes en este tema. Para luego hacer un análisis de la situación normativa costarricense con respecto a la problemática jurídica que se plantea y presentar un panorama integral de las condiciones legislativas del país para promover el comercio electrónico.

El trabajo es novedoso puesto que actualmente no existe una evaluación o análisis de las condiciones de la legislación costarricense relacionada con el comercio electrónico, el trabajo pretende dar los primeros pasos de análisis de la situación para llegar a plantear los lineamientos básicos que deban considerarse en ésta y que permita a la vez promover adecuadamente el desarrollo de este tipo de transacciones comerciales.

1.2 Justificación

El ser humano es un ser social. Desde la prehistoria se conoce que el hombre no es un ser solitario, sino que es un ser que vive y se desenvuelve en una comunidad. Guerrero (1986) indica que la sociedad tiene como finalidad asociar a los hombres, el interés público representa esta asociación, de la institución de la sociedad brota el gobierno y del gobierno nace la administración. El que los hombres vivan en sociedad y se hayan dado un gobierno habla de la existencia del Estado, que no es otra cosa, dice Bonnin, que la "organización política del pueblo". Por tanto, "la administración no puede ser considerada como una institución distinta del Estado".

La administración pública se ocupa del hombre en todos sus aspectos, porque en ello va la existencia del Estado. Se preocupa por la indigencia, delincuencia, orfandad, vicio, prostitución, etc. Descansa doblemente en que constituyen un problema moral y a la vez una limitante al desarrollo del Estado. Juzga a estos problemas como fallas del funcionamiento del Estado en su empeño por desarrollar a la sociedad civil, no como lo que son: condiciones estructurales propias de un régimen de producción determinado. Por tanto, más que empeñarse por darles solución de fondo, la ciencia de la administración los concibe como atenuables, como dolencias sociales cuyos efectos pueden ser mitigados. En todo caso, la ciencia de la administración es una teoría del poder del Estado, como lo manifiesta Guerrero (1986).

El Estado se interesa por hombres sanos y bien alimentados, por seres humanos que vivan en condiciones sanitarias adecuadas y al margen del riesgo de las epidemias, asentados en terrenos limpios y cuya agua y aire son puros. El Estado se preocupa del desenvolvimiento del talento humano, por lo cual autoriza el establecimiento de todo tipo de instituciones educativas, bibliotecas, museos, centros recreativos y exposiciones científicas y culturales. Un hombre instruido, capaz de desenvolverse a sí mismo, es un medio a la vez de superación de la sociedad de la que forma parte y por extensión integrante de los medios que el Estado requiere para su desarrollo.

El Estado dicta normas para poder garantizar una convivencia adecuada entre las personas de una sociedad. Estas normas se desarrollan conforme nace la necesidad. Entra entonces a ser parte del entramado de una sociedad las normas jurídicas que la rigen.

Una sociedad establece sus políticas, planes, programas, proyectos e instituciones para encaminarla hacia su desarrollo, y más que eso, hacia una mejor calidad de vida de todos sus habitantes.

Dentro del conjunto de relaciones existente en una sociedad se encuentra la relación comercial que se establece entre los distintos actores de la misma. Este tipo de relación constituye una de las principales que contribuyen al desarrollo de la economía del Estado, y por ende de la sociedad. Y como toda relación, el Estado debe normarla para garantizar la protección de las partes que intervienen.

Por otro lado, desde la perspectiva de la administración de negocios, entre las funciones de la administración se encuentra la de gestionar los procesos necesarios para un adecuado desarrollo de las actividades de la empresa. Y también desde esta perspectiva es necesario conocer las normas y reglas establecidas por el Estado, para realizar negocios con otras empresas así como con los ciudadanos, sin detrimento de las garantías de las partes.

Es deber del Estado proteger a las partes que intervienen en una relación comercial así como de cualquier otro tipo de relación. Y sobre todo de proteger a la parte más débil de esta relación comercial; que en el caso del comercio en la que interviene un consumidor, ésta es la parte más vulnerable.

Por tal razón, la administración de negocios o de empresas debe conocer sobre leyes, procedimientos, derechos y responsabilidades que tiene cuando establece relaciones comerciales, contractuales y de cualquier índole, con otras empresas y sobre todo con consumidores, para realizar negocios y actividades que no vulneren derechos de las partes involucradas.

Indudablemente el desarrollo de las tecnologías de información y comunicación y con ello el propio desarrollo de Internet ha facilitado la globalización de los mercados, en los que circulan libremente bienes, capitales, servicios y personas. Un nuevo orden económico mundial se está desarrollando, que no conoce distancias ni fronteras, aumenta la interdependencia de los mercados y el desarrollo de intercambios económicos ligados a la internacionalización de la actividad empresarial.

El uso efectivo de las tecnologías de información y comunicación en los negocios, el Gobierno y la educación es un elemento importante en la habilidad de todas las naciones de participar en la economía global, y por tanto, es un motor esencial de la competitividad económica (Maclay, 2001).

El crecimiento económico es posible con una buena preparación electrónica, y este es un requisito fundamental para realizar negocios electrónicos exitosos. El grado de desarrollo de una sociedad se mide por la preparación electrónica que haya alcanzado para poder participar de las ventajas y oportunidades que le presenta la nueva economía.

Este nuevo reto de los Gobiernos necesita de políticas y medidas adecuadas para evitar el aumento de la brecha entre los ricos y pobres. Se requiere establecer políticas y medidas que permitan el acceso a las tecnologías a todos los ciudadanos, independiente de su condición socioeconómica.

El comercio electrónico promovido por el desarrollo de Internet es un importante motor para el crecimiento económico mundial del siglo XXI. Permite a los empresarios una mejor gestión de sus almacenes, un menor costo de recursos humanos, comunicación inmediata con los clientes y mejora de los precios para competir en los mercados.

Esta revolución tecnológica está transformando los hábitos de las sociedades y la forma como operan las empresas para mejorar su productividad, mercadeo, distribución y venta.

El comercio electrónico ofrece nuevas oportunidades para los negocios y para los ciudadanos de todo el mundo. Las pequeñas empresas tienen la oportunidad de acceder a mercados mundiales a bajo costo y los consumidores pueden escoger de una amplia gama de productos y servicios.

A la par de todas las ventajas que benefician tanto a las empresas como a las personas, también esta revolución tiene consecuencias negativas que deben dimensionarse y encontrar soluciones que permita la coexistencia de tal revolución comercial y el respeto a los derechos de las personas.

En relación propiamente del consumidor, como uno de los principales agentes económicos de este desarrollo comercial, a nivel mundial se han desarrollado políticas de protección al consumidor debido a la necesidad de humanizar los procesos de globalización con el fin de establecer límites y responsabilidades al libre comercio mundial. Proteger al consumidor es un objetivo que tiene como fin procurar un mejoramiento en el nivel de vida de los ciudadanos, y aumentar la confianza en el mercado.

En la nueva era global, la esencia del mercado es la libre circulación de bienes y servicios, de personas y de dinero entre todos los países, como si fuera un solo país o un solo mercado. Esto significa que existirán empresas instaladas en cualquier parte del mundo ofreciendo una extensa gama de productos o servicios, y que los consumidores podrán tratar libremente con empresas instaladas en los otros países.

La función de ventas evolucionó hacia mercadeo y ahora se amplía a la incorporación formal de la defensa del consumidor, del cuidado de los clientes en una dirección opuesta a la habitual: escuchar sus necesidades, respetar sus derechos, cuidarlos; debe comprender el suministro de información clara y precisa, el cumplimiento de estándares de salud y seguridad, la atención oportuna de las solicitudes y reclamos, y una competencia justa (Ogliastri, 2007).

La libre competencia y la apertura de mercados ha ampliado la oferta de productos y servicios con una infinidad de precios y calidades, y han modificado la relación entre comerciantes y consumidores, pues ahora se realiza en forma anónima, se eliminó la distancia y el tiempo, y no hay posibilidad de negociación.

Anteriormente la legislación castigaba la competencia desleal, ahora tiene importancia todo lo relacionado con el consumidor como promotor de la economía. Antes, el consumidor era solo un comprador en un mercado local de dimensión muy limitada, hoy es un elemento de un mercado de masas, objetivo de una campaña publicitaria agresiva y está sometido a grandes presiones por parte de los grupos empresariales bien organizados.

La protección al consumidor abarca una extensa gama de derechos que conciernen a la mayoría de las actividades mercantiles que realiza un ciudadano común. Es por ello que su finalidad es mantener la confianza del ciudadano en el mercado, y garantizar así un flujo de bienes y servicios en el mercado interno y externo.

La administración debe considerar todos estos aspectos mencionados para poder realizar una gestión de la empresa o negocio acorde con la ley, respetando los derechos de las partes que intervienen en una relación contractual y sobre todo para no vulnerar los derechos de los otros.

La seguridad y confianza en los asuntos que incumben al consumidor debe ser proporcionada por los mismos actores, pero solo los Estados, mediante leyes y políticas nacionales e internacionales, pueden limitar las prácticas fraudulentas o desleales y proteger a la parte más débil en esta relación de comercio. Y la administración de las empresas requiere conocer de éstas leyes para realizar sus actividades acordes con ellas.

Además es un objetivo de las empresas reclutar un mayor número de consumidores y que éstos se mantengan leales a ellas, y esto sólo es posible si las empresas da un trato satisfactorio a sus consumidores, los cuales sin lugar a dudas serán sus clientes

permanentes si reciben bienes y servicios de calidad y un trato justo y equitativo sin vulnerar sus derechos y ofreciéndoles todas las garantías para un negocio o relación contractual satisfactoria.

En la medida que las normas sean claras y completas, habrá menos posibilidades de conflictos, fraudes y vulneración de derechos en una relación contractual o comercial, y será posible dirimir los conflictos de manera ágil y justa para ambas partes.

Como dice Coase (1960, p. 18): “Para llevar a cabo transacciones en el mercado es necesario, entre otras cosas, descubrir con quiénes deseamos transar, informar a la gente qué deseamos intercambiar y en qué términos, conducir a negociaciones que lleven a un convenio, redactar el contrato, llevar a cabo la inspección necesaria para asegurarnos de que los términos del contrato se observan”.

Como puede verse, cualquier transacción económica requiere de mecanismos que protejan a las partes que intervienen de los riesgos relacionados con el intercambio. Por tal motivo, el objetivo del contrato es prever acontecimientos que puedan afectar al objeto de la transacción. Una compra y venta por Internet es una transacción económica, es una relación contractual de compra y venta de bien o servicio, hay un contrato que se establece (en los casos de comercio electrónico, la mayoría son de adhesión).

El contrato debería establecer claramente lo que cada parte debe hacer ante cualquier suceso futuro que afecte al objeto del contrato. Pero como indica Coase (1937), el futuro es incierto, por lo tanto cualquier transacción implica riesgo e incertidumbre.

Por otro lado, todas las operaciones que se deben realizar para establecer una relación contractual satisfactoria, requiere de una minuciosa revisión de ambas partes, y son, a menudo, muy costosas; suficientemente costosas para evitar muchas transacciones que se llevarían a cabo en el mundo. Por lo que se hace necesario establecer las normas de protección, por lo menos para proteger a la parte más vulnerable en cualquier relación contractual. En este sentido, es deber del Estado establecer esos

requisitos mínimos de respeto, esas garantías necesarias para proteger los derechos de los consumidores, para dar seguridad necesaria y permitir una mayor confianza para que todos los ciudadanos puedan participar en el mundo interconectado.

Es indispensable promover una seguridad de los intercambios electrónicos comerciales y crear un marco jurídico transparente y de confianza para los usuarios de la red, los países deben adecuar su marco jurídico a las transacciones electrónicas con el fin de proporcionar seguridad jurídica en el uso de medios electrónicos, facilitar las transacciones por estos medios y lograr una interacción global e integral de los campos en que se utilizan los medios electrónicos.

En este nuevo marco del comercio, que ha revolucionado la misma cultura de consumo, un nuevo reto se presenta: permitir el desarrollo y crecimiento de la economía sin detrimento de los derechos del consumidor. Sin olvidar que para esto, el Estado tiene un deber fundamental, la de promover la posibilidad de participación de todos sus ciudadanos en el mundo interconectado.

Por lo anterior, se justifica la presente investigación con el fin de determinar las necesidades en materia normativa que permita a la administración del Estado proteger a las partes de una transacción. Y por otro lado, a la administración de las empresas realizar sus actividades comerciales considerando el respeto de las garantías de protección a los consumidores.

1.3 Hipótesis de investigación

La legislación costarricense tiene lagunas jurídicas en el campo del comercio electrónico, las cuales evitan que este se desarrolle como sería deseable para un país como Costa Rica que busca inscribirse en la economía digital.

1.4 Objetivos

1.4.1 Objetivo General

Realizar un análisis de legislación comparada para identificar las lagunas jurídicas existentes relacionadas con el comercio electrónico, y plantear líneas de acción oportunas que permitan promover este tipo de transacciones comerciales y evitar algunos de sus efectos contraproducentes para los consumidores, la seguridad y la protección de datos.

1.4.2 Objetivos específicos

1. Identificar los núcleos problemáticos desde la perspectiva jurídica derivados del comercio electrónico, distinguiendo los meramente formales de la configuración de los contratos y transacciones, así como los referidos a la infraestructura tecnológica requerida para su configuración.

2. Explorar la experiencia jurídica comparada en materia de atención a los aspectos formales y tecnológicos del comercio electrónico con el fin de diseñar una línea modelo de atención a la problemática.

3. Aplicar la matriz comparativa a los esfuerzos legislativos nacionales y derivar de allí sus lagunas y aportes a la regulación.

4. Establecer las áreas necesitadas de investigación y discusión de cara a un mejoramiento sustancial del comercio electrónico y de las áreas requeridas de profundización y reflexión.

1.5 Posición epistemológica del investigador

La posición epistemológica del investigador tendrá implicaciones en la construcción metodológica de la investigación. A su vez, la propuesta metodológica considera, entre otras cosas, la naturaleza del objeto de estudio, el tipo de problema de investigación, los objetivos y los aspectos del fenómeno social a tratar.

La epistemología es el quehacer filosófico sobre el conocimiento. Responde las preguntas fundamentales sobre él y entre las que intenta resolver están: a) ¿Es posible el conocimiento?, ¿Cómo se conoce?, ¿Cuál es la relación objeto-sujeto?

Según se respondan esas preguntas así se tendrá una posición epistemológica de un tipo o de otro. El escepticismo, por ejemplo, postula que no es posible ningún conocimiento objetivo. El realismo, en cambio, propone que el conocimiento es posible y que la *imagen* o *reflejo* mental es una reproducción de la realidad exterior al sujeto, por lo tanto, con una realidad objetiva.

Otro aspecto importante en la determinación de la posición epistemológica es la relación sujeto-objeto. ¿El objeto es independiente del sujeto? ¿Cuál existe primero, el sujeto o el objeto? Según se responda, se tendrá un enfoque epistemológico y ontológico, materialista o idealista, escéptico-relativista o realista, etc.

En la tradición heredada de Augusto Comte y el positivismo científico, se ha asumido que el conocimiento es posible y que existe algún grado de correspondencia entre las representaciones y los objetos y que es posible descubrir relaciones, especialmente causales, por medio del método experimental, dando preponderancia al enfoque metodológico cuantitativo.

La preponderancia del positivismo en las academias ha llevado a un predominio, también en las ciencias sociales, de los métodos cuantitativos de investigación y a una cierta descalificación, no declarada abiertamente, de los métodos cualitativos. Así, se

considera que el objeto es independiente del sujeto, que éste no crea a aquél y por lo tanto que la *pureza* de la investigación radica en que el sujeto (investigador) no contamine al objeto, no le agregue nada ni lo reelabore; es decir, se sostiene que el objeto no es transformado por el sujeto en su accionar investigativo.

Este sesgo hacia la investigación cuantitativa, proveniente del positivismo, ha llevado a que en no pocas ocasiones se tienda a considerar, injustificadamente, la investigación no cuantitativa como no científica. Sin lugar a dudas el paradigma "científico-positivo" ha sido el dominante.

Los paradigmas son un conjunto de conocimientos y creencias que forman una visión del mundo (cosmovisión), en torno a una teoría hegemónica en determinado periodo histórico. Cada paradigma se instaura tras una revolución científica, que aporta respuestas a los enigmas que no podían resolverse en el paradigma anterior. Una de sus características fundamentales es su inconmensurabilidad: ya que ninguno puede considerarse mejor o peor que el otro. Además, cuentan con el consenso total de la comunidad científica que los representa.

Los paradigmas cumplen una doble función, por un lado, la positiva que consiste en determinar las direcciones en las que ha de desarrollarse la ciencia normal, por medio de la propuesta de enigmas a resolver dentro del contexto de las teorías aceptadas. Por otro lado, la función negativa del paradigma es la de establecer los límites de lo que ha de considerarse ciencia durante el tiempo de su hegemonía.

Las teorías que se inscriben en un paradigma no pueden traducirse en términos de las teorías que forman el paradigma posterior; cada revolución científica es un cambio total de la percepción del mundo y por lo tanto viene acompañado de un cambio paradigmático. Los paradigmas cambian y se transforman de un modo semejante (aunque en gran escala) al de las hipótesis.

El paradigma, está constituido por supuestos teóricos, leyes y técnicas de aplicación que deberán adoptar los investigadores que se mueven dentro de una determinada

comunidad científica. Los que trabajan dentro de un paradigma, ponen en práctica la ciencia normal. Es probable que al trabajar en ella resulten dificultades. Si estas dificultades se hacen inmanejables, se desarrollará un estado de crisis. Ésta se resolverá con el surgimiento de un paradigma completamente nuevo, el cual cobrará cada vez mayor adhesión o aceptación por parte de la comunidad científica, hasta que finalmente se abandone el paradigma original. Este cambio no es continuo, sino por el contrario es discontinuo y constituye una revolución científica. El nuevo paradigma enmarcará la nueva actividad científica normal, hasta que choque con dificultades y se produzca una nueva crisis y una nueva revolución y por lo tanto el surgimiento de un nuevo paradigma.

Cada revolución es la oportunidad de pasar de un paradigma a otro mejor. Si se desarrolla una crisis, el pasaje de un paradigma a otro se hace necesario, y este paso es esencial para el progreso de la ciencia. Si no hubiera "revoluciones", la ciencia quedaría atrapada o estancada en un solo paradigma y no se avanzaría más allá de él. No es una evolución hacia un objetivo determinado sino, un mejoramiento desde el conocimiento disponible, cada paradigma nuevo es un instrumento para resolver enigmas.

Actualmente, el viejo paradigma dominante está siendo sometido a revisión. Aunque en la ciencias sociales el criterio prevaleciente siga siendo el paradigma de la matematización en su dimensión más cuantitativista y reductora del ciframiento absoluto de las conductas y comportamientos sociales, en las ciencias naturales hace tiempo que dicho paradigma dejó de ser tan fuerte, como lo era antaño. Ello en gran medida asociado a dos grandes principios generados en el siglo XX: el de *incertidumbre* asociado a Heisenberg, y el de la *relatividad*, asociado a Einstein, que transformaron las bases del paradigma clásico desde el punto de vista de las relaciones sujeto/objeto -cualquier medición transforma el objeto medido- y desde el punto de vista de la existencia de un único centro de coordenadas o perspectiva dominante. El principio mismo de causalidad (pilar del edificio positivista) ha sido cuestionado por la Física moderna y otras ciencias.

Más recientemente todavía y en vínculo con la Biología, la Química, la Cibernética y la otras disciplinas científicas, se han ido desarrollando una serie de planteamientos que significan una superación del estrecho paradigma científico. La matematización absoluta y cuantitativista, la medición como control máximo dejaba fuera de sus estrechos límites todo lo relacionado con la vida, con el crecimiento, con el desarrollo de la complejidad, es decir, con lo real y lo social.

Como ha puesto de relieve Beltrán (1985), frente a las pretensiones imperialistas de cualquier modelo metodológico general unidimensional, igualmente válido para todos los niveles y fases de un proceso de investigación social concreta, la complejidad multidimensional de la realidad social determina, por el contrario, la configuración de modelos de análisis (en principio) parciales y diferenciados en correspondencia con los distintos niveles estructurales específicos de la propia realidad social. Se trata de un pluralismo cognitivo de lo social que entraña consecuentemente un pluralismo metodológico y tecnológico.
Esta concepción pluralista plantea, además, la cuestión de la demarcación teórica y de pertinencia metodológica de cualquier modelo concreto de análisis social como una cuestión, ante todo, de especificación del nivel estructural de la realidad social al que corresponde.

Se hacen investigaciones sociales para lograr un saber pragmático que debe atender a todos los niveles de la realidad social, los cuales tienen distinta *naturaleza epistemológica*. En este sentido, se pueden distinguir tres niveles, al menos en la realidad social:

1. Nivel o campo de los *hechos,* conformado por las relaciones de indicación o designación de la proposición, en cuanto puesta en evidencia de cuanto acontece o se hace. Los hechos así configurados como estados individuales aparecen como evidentes en el nivel de lo manifiesto o consciente. En fin, de este modo, los hechos tienden a ser concebidos como procesos fácticos, constituidos por cargas de energía, y por tanto, como una *res extensa cuantificable*.

2. Frente al simple campo de los hechos, la *significación* de la proposición entra la existencia del *universo de los discursos*, donde las significaciones no se establecen por extensión, sino referidas a sí mismas en el cuadro de un sistema de signos. Se trata de proposiciones comunicativas coherentes por su articulación significativa, porque están definidas por una cierta relación codificada entre significante y significado. En principio, los discursos estarían articulados por "lo que se dice", en el contexto de formaciones culturales e ideológicas concretas. Pero la institucionalización de las cosas no les confiere la misma significación concreta en una cultura u otra, pues cada cultura impone un sistema de códigos. Junto a los *culturemas* (unidad significativa de una cultura), los discursos suponen también orientaciones de valor, es decir, proposiciones ideológicas *(ideologemas)*. Nivel en el que confluyen el enfoque cuantitativo (para los culturemas precodificados) con el enfoque cualitativo (para su significación ideológica y proceso de producción simbólica).

3. En un tercer nivel se encuentra el *reino de las motivaciones*. Serían las fuerzas motoras, pulsiones, deseos, que corresponden al porqué de la interacción social; es decir, la intencionalidad y sentido, consciente o no, que configuran los procesos proyectivos. Procesos sólo interpretables con sentido a partir de enfoques cualitativos hermenéuticos.

La distinción de estos tres niveles de la realidad social (hechos, discursos y procesos motivacionales) cumple ante todo con una función metodológica, pues se trata de comprender que en el análisis de la realidad social el investigador encuentra tres tipos de estructuras y tres tipos de lógicas diferentes y con reglas propias: *fácticas*, *significativas* y *motivacionales*. La cuestión de cómo se articulan estos tres niveles en la interacción social es todavía muchísimo más compleja.

El concreto enfoque epistemológico que se adopte influirá en el diseño metodológico, como se ha expresado. A diferencia del diseño cuantitativo (en el que las hipótesis iniciales y arbitrarias marcan su desarrollo siempre secuencial), en el diseño cualitativo

“todo se encuentra sobredeterminado por el objetivo final; son los objetivos los que marcan el proceso de investigación cualitativa, dado que ceñirse a hipótesis previas no haría sino constreñir el propio análisis. El mundo simbólico capturado mediante discursos no se circunscribe en modo alguno a premisas previamente formalizadas para su ulterior verificación. En la investigación cualitativa, por el contrario, se pretende la determinación dialéctica del sentido, mediante la operación de ‘desentrañar significados’ siempre en relación con los objetivos delimitados” (Dávila, 1999: 77).

El enfoque cuantitativo sigue siendo predominante en la mentalidad de la mayoría de los investigadores. Es frecuente el desplazamiento del acento desde los métodos cualitativos a los cuantitativos; un ejemplo de ello es el debate del concepto de clase versus el de estratificación: se trata de estratificar salarios (criterio lineal, mensurable) donde antes se clasificaban por clases (criterio discontinuo, formal), siempre encaminado hacia una cosificación de lo real en la convicción –posición tanto ontológica como epistemológica- de que existe un mundo objetivo susceptible de ser conocido, tratando como una realidad independiente aquello que no es sino una confirmación de las circunstancias que la engendran.

Un enfoque epistemológico que haga énfasis no tanto en la objetividad que debe ser descubierta sino que conciba a la realidad social antes que como *objeto* (externo, independiente) como *relación*, que al final es lo que es, debe conducir a un tratamiento mixto o combinado de metodologías cualitativas y cuantitativas.

Desde la perspectiva cualitativa el hecho social es concebido como relación, no sólo como objeto sino como subjetividad, de la cual también participa el investigador.

Con fundamento en lo anterior, en la presente investigación se hará uso de un metodología principalmente cualitativa, y especialmente la investigación asume una naturaleza documental, descriptiva y hermenéutica, y comparativa y proyectiva, según cada uno de los objetivos.

A continuación se enuncian los principios orientadores del proceso investigativo que orientan la posición epistemológica de la investigadora:

1- Los documentos tienen una historia, un desarrollo y un contexto en el que fueron creados, por lo tanto su análisis debe partir del conocimiento de esta situación.

2- Las condiciones históricas, económicas, sociales, tecnológicas y culturales cambian con el tiempo, por lo que se hace necesario estudiar las nuevas condiciones y circunstancias y analizar la validez de la información aportada por los documentos existentes en esta nueva situación.

3- Cada país tiene su propia realidad, por lo tanto, debe partirse del hecho que no se puede hacer generalizaciones sin antes verificar que las condiciones sociales, culturales, económicas, tecnológicas sean similares.

4- El objeto de estudio está siendo debatido en la actualidad en todo el mundo, y los rápidos avances tecnológicos hacen que se presenten continuamente nuevas situaciones que no se habían previsto, por tal razón, hay que considerar que las condiciones que origina el problema estará en constante y rápida variación y que puede ser posible que las soluciones que se den pasen a ser rápidamente obsoletas. La investigadora tratará de delimitar el tiempo, el contexto y las condiciones de ese contexto para poder trabajar.

5- Con conocimiento de lo anterior, no se puede entonces llegar a tener la solución verdadera y única, sino una aproximación a una buena solución al problema, o por lo menos, líneas generales de acción para mejorar la situación regulatoria de las transacciones comerciales electrónicas del país.

6- El acercamiento al conocimiento y a la verdad es importante en la medida que pueda resolver problemas planteados, y las soluciones que se encuentren son importantes en la medida que puedan usarse o ejecutarse para la toma de decisiones con el fin de solucionar los problemas.

7- Se debe plantear sistemas que den las soluciones a los problemas, y no dejar que sea un asunto de muchos, porque es difícil encontrar soluciones cuando intervienen muchas personas. Los sistemas deben diseñarse para que tome todos los elementos necesarios de la situación problemática y ofrezca la solución del caso. Los problemas deben ser resueltos por sistemas.

Capítulo 2. Antecedentes y Marco Teórico

En este capítulo se expone los antecedentes existentes en materia jurídica en el país. Principalmente resume algunos trabajos de investigación realizados por autores costarricenses en la temática de regulación del comercio electrónico. Además presenta el marco conceptual y teórico del trabajo de investigación: establece el concepto de comercio electrónico y su evolución histórica, así como sus ventajas y desventajas; desarrolla la problemática jurídica y técnica que trae consigo este tipo de transacciones, y en los aspectos que analizará esta investigación; presenta los mecanismos técnicos de seguridad informáticos existentes y por último resume las dos leyes modelos propuestos por la CNUDMI para regular el comercio electrónico.

2.1 Antecedentes

El comercio electrónico es una nueva modalidad de hacer negocios a nivel mundial que en un futuro puede convertirse en la modalidad más utilizada de hacer comercio. Esta nueva modalidad de comerciar tiene un impacto evidente en las economías y las culturas de los países.

Para las empresas que exploten completamente su potencial, el comercio electrónico ofrece la posibilidad de grandes cambios que modifican radicalmente las expectativas de los clientes y redefinen los mercados así como crean mercados completamente nuevos. Todas las empresas, incluidas las que ignoran las nuevas tecnologías, sentirán el impacto de estos cambios en el mercado y las expectativas de los clientes. Igualmente las personas se enfrentarán con nuevas formas de adquirir bienes y servicios, acceder a información e interactuar con otras personas en el mundo. Las posibilidades se han extendido y las limitaciones geográficas y de tiempo se han eliminado.

Por otro lado, las transacciones de tipo electrónico son contratos atípicos en prácticamente todos los países y esa condición hace que sea necesaria su regulación, no sólo en Costa Rica, sino en todos los países del mundo.

En el caso de Costa Rica, es necesario dar la debida importancia al principio de seguridad jurídica, para impulsar la actividad comercial y facilitar al Estado la realización de su labor de vigilancia en relación con el artículo 42 de la Ley de Promoción de la Competencia y Defensa efectiva del Consumidor, además de su labor de fiscalización para el cumplimiento de todas las leyes en general. Recientemente, en el mes de setiembre de 2005, se publicó en La Gaceta Oficial la nueva "Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos" en el país. Este es un paso importante para el país, debido a que le permitirá dar seguridad a las transacciones públicas y privadas, y sobre todo a las comerciales electrónicas.

Algunos autores costarricenses han analizado diferentes aspectos de la problemática jurídica relacionada con el comercio electrónico así como aspectos para la promoción de este tipo de comercio, como a continuación se resume.

De acuerdo con Echegaray (2001), la Ley de Promoción de la Competencia y Defensa efectiva del Consumidor salvaguarda los derechos de la parte más desprotegida en las transacciones comerciales, a saber, el consumidor. No obstante las nuevas tecnologías hacen necesario analizar si dicha legislación es adecuada para garantizar la protección de este en el entorno del nuevo comercio electrónico. A este respecto, él hace un análisis de esta Ley y llega a las siguientes conclusiones:

1- Sobre el ámbito de aplicación señala:

> "...se debe indicar que nuestra legislación mantiene una posición amplia en cuanto a su aplicación, así se abarcan el comercio en general, tanto público como privado. En este sentido la legislación nacional de protección de los consumidores se amolda a la Ley Modelo sobre Comercio Electrónico, en cuanto abarca no solo la totalidad de las transacciones comerciales, sino que también abarca la relación entre el consumidor y los proveedores de servicios públicos." (Echegaray, 2001, p. 125).

2- Indica que las definiciones relativas a los procesos de comercialización de bienes y servicios, en ambos casos se diferencian por cuanto en

> "... la Ley Modelo se regula la específica de mensajes de datos, mientras que en la Ley se protege al consumidor final de bienes y servicios, dentro del proceso de comercialización en general" (Echegaray, 2001, p.125),

por lo que sí se hace necesario elementos que aclaren la materia relativa a comercio electrónico para evitar confusiones sobre éstos dentro de los márgenes de aplicación de la Ley.

3- También Echegaray (2001) menciona, sobre la normativa acerca de la formación y validez del contrato por medio informáticos, que:

> "se encuentra regulada por nuestro ordenamiento jurídico general, así el Código de Comercio, el Civil, y el respectivo Código Procesal" (Echegaray, 2001, p. 126).

Dice que éstos tienen soluciones jurídicas aceptables para la solución de los problemas, reduciendo la discusión a una simple actividad probatoria adecuada y regulada por el Código Procesal Civil.

4- Indica Echegaray (2001) que el artículo 368 del Código Procesal Civil, regula adecuadamente la problemática del documento electrónico pues indica que podrá considerarse como documento todo objeto que tenga carácter representativo o declarativo, características que cumple el documento electrónico. De igual forma mediante la aplicación de los procedimientos adecuados para determinar la autenticidad de las partes y la integridad del documento, cumple con los requisitos de ser inalterable, legible, de determinación del lugar y tiempo en que se creó y de estabilidad.

5- Menciona este mismo autor acerca de la incorporación por remisión que esta otorga un grado de incertidumbre en cuanto a la protección de los derechos del consumidor, pues:

> "...nuestra Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor no contempla en forma adecuada la incorporación por remisión respecto de cláusulas contractuales ligadas por vínculos electrónicos que el aceptante debe necesariamente conocer al momento de oprimir el botón de "aceptar", pues se haría incurrir al consumidor en un error o engaño por desconocimiento de la totalidad del contrato" (Echegaray, 2001, p.127).

En resumen, indica Echegaray (2001) que es necesaria una labor integradora, para extraer de las diferentes normas que son aplicables al comercio electrónico, y hacer referencia a ellas dentro de una normativa que implemente un órgano certificador de documentos y firmas electrónicas, en conjunto con las definiciones técnicas relativas al comercio electrónico (tales como correo electrónico, intercambio electrónico de datos, etc.) definiciones que se podrán hacer extensivas a los demás campos normativos. Con

la aprobación de la Ley de Firma Digital y Certificados Digitales es posible que esto último quede resuelto.

Concluye que:

> "...la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor y su Reglamento son adecuadas para la protección de los derechos de los consumidores en el comercio electrónico, debiendo en cuanto al comercio electrónico en general echar mano a las definiciones técnicas necesarias, así como a la incorporación por remisión de cláusulas integradas al documento electrónico por medio de vínculos que deben ser necesariamente conocidos por el consumidor al momento de otorgar su consentimiento en el contrato" (Echegaray, 2001, p. 129).

El desarrollo de este tipo de comercio en el país es incipiente y todavía no existen regulaciones explícitas para transacciones comerciales de tipo electrónico que permitan la protección de las partes involucradas en ellas. Lo más reciente es la aprobación de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos.

Es necesario revisar los instrumentos legales que se tienen para el control de los aspectos de seguridad para las partes (posibles defraudaciones), protección de datos personales, entre otros.

Con respecto al fomento del comercio electrónico en el país, se han desarrollado propuestas de estrategias de mercadeo para impulsar el uso de Internet para fomentar la cultura de consumo. La tesis de maestría de González y otros (2000) se refiere a estas estrategias. Estas tienen el fin de impulsar el comercio electrónico en el país. Para ellos:

> "El Comercio Electrónico es bastante nuevo para el sector empresarial en Costa Rica. El volumen de ventas por medio de Internet no ha generado utilidades para las empresas que lo están implementando en el mercado costarricense." (González et al., 2000, p. 111).

Estos investigadores concluyeron que los elementos más importantes que limitan el desarrollo del comercio electrónico de Costa Rica están: el tamaño del mercado es pequeño, son pocas las personas con acceso a Internet con poder de compra, la oferta costarricense en Internet es reducida e inseguridad en los medios de pago.

También encontramos en (Salas y Fernández, 2003) que el comercio electrónico en Costa Rica está apenas iniciando sus experiencias:

> "Los costarricenses que realizan compras por Internet adquieren principalmente libros y discos desde Amazon.com y CDNow.com. El nivel de ventas de los sitios costarricenses aún se considera bajo por los propios empresarios del comercio electrónico. Salvo de algunos sitios orientados a segmentos ubicados en el exterior, como el de Café Britt." (Salas y Fernández, 2003, p. 195).

A pesar del desarrollo que ha venido teniendo el comercio electrónico a nivel mundial, su desarrollo en Costa Rica no despegará hasta que exista el marco regulador para este tipo de transacciones, principalmente porque los usuarios no se sentirán a gusto en un medio que no les da confianza. Sin embargo, con la reciente aprobación de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, es probable que estas transacciones electrónicas aumenten.

El esfuerzo más importante en este sentido ha sido realizado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL iniciales en inglés, o CNUDMI iniciales en español), que emitió la Ley Modelo para la Regulación del Comercio Electrónico y la Ley Modelo para la Firma Electrónica junto con una guía para su aplicación en el derecho interno, sin embargo muchos países no las han aplicado, y en el caso de Costa Rica, no es hasta el 23 de agosto de 2005 cuando aprobó su ley.

La ley modelo de la UNCITRAL para el comercio electrónico establece cómo los documentos electrónicos tienen el mismo efecto jurídico que los documentos físicos. En Colombia tal situación se ha establecido por medio de la Ley 527 de 1999, la cual define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación y dicta otras disposiciones. Aunque el tema no ha sido desarrollado plenamente, esta ley es un inicio de lo que debe ser la reglamentación de los documentos informáticos en ese país.

En este mismo sentido, otros países latinoamericanos como Argentina, Perú, Chile, México y Panamá ya tienen promulgadas leyes relacionadas con el comercio

electrónico, específicamente la regulación de las firmas digitales, como en el caso de Colombia.

Según Ramírez (2002), los países decidieron entrar a realizar este tipo de transacciones electrónicas, sin todavía haberse establecido los controles necesarios para un adecuado desarrollo de éste. Es así que intervienen entonces la Organización Mundial del Comercio (OMC), la Organización para la Cooperación y el Desarrollo Económico (OCDE) y otros en un intento de regular estas transacciones.

También en Ramírez (2002), se presenta diferentes normativas existentes en la legislación costarricense actual para la protección contra posibles infracciones como consecuencia del comercio electrónico. Menciona el artículo 46 de la Constitución Política, que considera el derecho del consumidor como un aspecto del más alto nivel en nuestro ordenamiento jurídico:

> "El concepto más importante a extraer del principio constitucional es que consumidores y usuarios de bienes y servicios tienen derecho a ser tutelados en la relación de consumo, en los distintos aspectos que de ella surgen." (Ramírez, 2002, p.124).

Se refiere también a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor:

> "...Costa Rica ya cuenta con un sistema normativo en forma genérica sobre la protección de los derechos del consumidor. Falta obviamente una regulación más precisa que determine esta relación a través de Internet con la amplia gama de mecanismos diversos no contemplados aún." (Ramírez, 2002, p.125).

Asimismo Ramírez (2002) menciona el Código de Normas y Procedimientos Tributarios, la ley General de Aduanas, el Tratado sobre la Propiedad Intelectual, Ley de Derechos de Autor, Ley de Marcas y otros Signos, Ley de Protección a los Sistemas de Trazados de los Circuitos Integrados, pero en forma superficial indicando que éstas de alguna manera protegen a los usuarios de algunos delitos que se pueden cometer desde el ambiente de comercio electrónico, pero no entra a analizar en detalle cada una de ellas.

Por otro lado, se encuentran diferentes investigaciones realizadas alrededor de temas específicos en materia reguladora del comercio electrónico en la legislación actual costarricense.

Agüero y Echeverría (2002) hace un estudio de derecho comparado en relación al contrato de intercambio electrónico de datos entre empresarios; Carvajal y Jiménez (2002) se refieren a las cláusulas abusivas en contratos de adhesión en Internet y Echegaray (2001) trabaja específicamente analizando los aspectos de protección de los derechos del consumidor. Morales y Figueroa (2003) analiza la contratación electrónica y la seguridad jurídica transaccional y De Téramond y Fernández (2002) estudia con detalle la Firma digital.

De acuerdo con Carvajal y Jiménez (2002) la figura más utilizada de contratación en el comercio electrónico es la contratación por adhesión en Internet, y que esta forma de contratación tiene un nivel alto de inseguridad para el adherente como parte débil de la relación contractual,

> "...no sólo por estar expuesto a todos los abusos que el contrato por adhesión le impone, sino también por el manejo de la información personal que suministre a la hora de aceptar la oferta virtual y consumar el contrato, ya que dicha información puede ser tan privada como los números de sus tarjetas de crédito" (Carvajal y Jiménez, 2002, p.215).

En sus conclusiones Carvajal y Jiménez (2002) afirman que:

> "...no es necesario crear una rama específica para regular las situaciones contenidas de la red pues los principios generales del derecho civil y comercial pueden aplicarse a las figuras que ya conocemos y manejamos solo que dentro de un espacio virtual. El reconocimiento legal no debe ser a una rama del Derecho sino a los elementos que involucra una transacción electrónica, brindándoles la eficacia jurídica que sus análogos físicos poseen, por ejemplo el documento electrónico y la firma digital." (Carvajal y Jiménez, 2002, p.216)

Morales y Figueroa (2003) coincide con Carvajal y Jiménez (2003) y con Echegaray (2001) cuando dice que:

> "... en nuestra legislación se sigue el principio consensual, tanto en el Código Civil como en el Código de Comercio. Cuando exista manifestación de voluntad de las partes y dicho consentimiento se haya expresado libremente por medio electrónicos como Internet, dicho contrato será válido sin importar el medio por el cual se haya celebrado, un problema aparte lo será el de la autenticidad en la identidad de las partes, la determinación del momento en que se perfecciona el contrato, la posibilidad de probarlo, etc...." (Morales y Figueroa, 2003, p.268).

Es decir, que en principio todo tipo de contratos pueden celebrarse por medios electrónicos, a excepción de aquellos que requieran ciertas solemnidades, requisitos o límites expresamente estipulados por la ley, de acuerdo al artículo 411 del Código de Comercio.

> "ARTÍCULO 411.- Los contratos de comercio no están sujetos, para su validez, a formalidades especiales, cualesquiera que sean la forma, el lenguaje o idioma en que se celebren, las partes quedarán obligadas de manera y en los términos que aparezca que quisieron obligarse. Se exceptúan de esta disposición los contratos que, de acuerdo con este Código o con leyes especiales, deban otorgarse en escritura pública o requieran forma o solemnidades necesarias para su eficacia.
> *(Así reformado por el artículo 68 de la Ley No.7600 del 2 de mayo de 1996)"* (Código Comercio, 1964)

Morales y Figueroa (2003) dice que los contratos por medios electrónicos son mercantiles y nuestra legislación aunque no los regula expresamente, a ellos le son aplicables la teoría general del contrato civil y comercial, por no ser otra cosa que un contrato común y simple. Concluye de que:

> "...no existe impedimento legal para plasmar la voluntad de las partes contratantes por medio digital, lo que lo hace susceptible de ser probado en estratos judiciales mientras alguna ley no lo impida. Consecuentemente, el documento electrónico, sólo podrá ser admisible como medio de prueba, si se asegura que cumpla con los requisitos de autenticidad, integridad y verificación." (Morales y Figueroa, 2003, p.268)

Morales y Figueroa (2003) también dice que:

> "No podemos hablar de seguridad jurídica en la contratación por medios electrónicos si no sabemos lo que sucede con la información que es enviada de una computadora a otra (por ejemplo, conocimientos sobre el lenguaje que utilizan las computadoras, sobre la digitalización y las ventajas y riesgos que trae aparejada), sobre todo si no conocemos "el medio electrónico" por donde la información transita (por ejemplo, por cable-cable de cobre o fibra óptica- o satélite, y los riesgos que cada medio presenta). (Morales y Figueroa, 2003, p.270).

Ellos indican que es necesario conocer las formas y medios tecnológicos que soportan el comercio electrónico para poder dar seguridad jurídica a este tipo de transacciones.

En Costa Rica los intentos de promover el establecimiento de alguna regulación más específica al respecto, aparte de la normativa existente, se concreta con la reciente aprobación de la Ley de de Certificados, Firmas Digitales y Documentos Electrónicos. La propuesta original del Proyecto de Ley de Firma Digital y Certificados Digitales, Expediente No.14.276, se encontraba en la Comisión Especial No.13.655 de Propiedad Intelectual en el año 2001 y luego pasó a la Comisión de Asuntos Jurídicos. Se hicieron

consultas obligatorias en el 2002 de conformidad con el artículo 190 de la Constitución Política a las siguientes instituciones: Instituciones Autónomas, corte Suprema de Justicia, Consejo Nacional para Investigaciones Científicas y Tecnológicas (CONICIT), Universidades Públicas (UCR, ITCR, UNA, UNED), además se recomendó consultar el proyecto a otras instituciones públicas y privadas. Se realizaron consultas a más de 74 instituciones públicas, ministerios y universidades. Luego el 11 de febrero de 2004 se presenta una nueva redacción de este Proyecto de Ley.

En general, todas las que contestaron a la consulta realizada:

> "...manifestaron su conformidad con el proyecto, alabando su oportunidad y conveniencia. Las que presentaron observaciones, la principal recomendación fue "darle más profundidad al proyecto y más claridad a los términos, aunque casi ninguna señaló propuestas concretas en este sentido." (De Téramond y Fernández, 2002, p. 250)

De Téramond y Fernández (2002) hacen un análisis minucioso acerca de la Firma Digital. Ellos indican que las legislaciones de: Estados Unidos, Estado Utah, Colombia, Perú, Chile, Argentina, Italia, Alemania, España, Francia, Corea del Sur, India, Japón, Malasia y Singapur tienen las siguientes figuras reguladas con respecto a la firma digital:

1- El principio de neutralidad tecnológica.
2- El principio de equivalencia funcional.
3- Compatibilidad internacional.
4- Libre competencia.
5- Acreditación voluntaria.
6- Uso de la firma digital por el Estado.
7- Garantías.

De acuerdo con De Téramond y Fernández (2002):

> "...el Proyecto logra regular el tema de la firma digital, se apega al principio de neutralidad tecnológica y sus normas son compatibles a nivel internacional. Es un excelente esfuerzo por parte del Poder Ejecutivo y Legislativo." (De Téramond y Fernández,2002, p. 253)

Concluye De Téramond y Fernández (2002) que:

> "La firma digital es una realidad, es usada con regularidad, y es necesario brindarle protección jurídica. La laguna jurídica existente por falta de regulación sobre este tema, es un factor que obstaculiza el progreso del país en este ámbito." (De Téramond y Fernández, 2002, p.265).

> "...es necesario, para el pleno desarrollo del comercio electrónico, dotarlo de un entorno jurídico, es decir, emitir una normativa que sea el soporte de las transacciones, e introducir el concepto de seguridad jurídica en la era digital, así como de darle el empleo adecuado." (De Téramond y Fernández, 2002, p.266).

> "La firma digital le da seguridad a las transacciones electrónicas. Esta forma es una herramienta tecnológica, basada en sistemas complejos de encriptación, que otorgan plena seguridad al intercambio de datos en Internet y en los sistemas de comunicación. Su óptima aplicación se da cuando cuenta con el reconocimiento del ordenamiento jurídico, que para esto es necesario la intervención de terceras partes, como las autoridades de certificación que emiten certificados digitales y comprueben que el firmante es quien dice ser." (De Téramond y Fernández, 2002, p.266).

En febrero del 2004, el texto original de la propuesta de Ley de Firma Digital y Certificados Digitales fue sustituido por otro que tiene un alcance mayor y fue aprobado en segundo debate el día 23 de agosto de 2005.

Es muy reciente la aprobación del proyecto de Ley de Certificados, Firmas Digitales y Documentos Electrónicos de Costa Rica, por lo que no es posible conocer experiencias concretas a raíz de su aplicación en el país. Por tanto es necesario realizar un análisis de la legislación existente en Costa Rica acerca de las transacciones comerciales electrónicas, incluyendo la nueva Ley, con el fin de evaluar las condiciones de su legislación para promover el comercio electrónico y a la vez evitar los efectos negativos que puede traer su desarrollo.

2.2 Comercio electrónico

2.2.1 El concepto

En Bruce (2002) se encuentra varias definiciones. Entre ellas está una definición dada por la Unión Europea en su Iniciativa Europea de Comercio electrónico, señala que el comercio electrónico "consiste en realizar transacciones comerciales electrónicamente". (Bruce, 2002, p.160). También menciona una de Renato Javier Jijena, la cual indica que el

comercio electrónico "se ha definido como el intercambio telemático de información entre personas que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles o en un pedido electrónico de bienes tangibles" (Bruce, 2002, p.160).

Una definición más amplia del comercio electrónico la da Carlos de Paladella, también mencionada en (Bruce, 2002), que manifiesta que:

> "El concepto de comercio electrónico no sólo incluye la compra y venta electrónica de bienes y servicios, que es el concepto común que se tiene, sino que también incorpora el uso de las redes para actividades anteriores o posteriores a la venta, como son: la publicidad, la búsqueda de información, el aseguramiento de las posibles transacciones, el tratamiento de clientes proveedores, incluso inversores, trámites ante autoridades de control y fiscalización, la negociación de condiciones de compra, suministro, etc., la prestación de mantenimiento y servicios posventa y la colaboración entre personas".(Bruce, 2002, p.160)

Estas actividades, mencionadas en esta última definición, no necesariamente deben estar presentes en todos los escenarios de comercio electrónico. El caso más simple es realizar solo la publicidad por Internet, y el caso más completo es donde todos los pasos anteriores se hacen de forma electrónica, incluyendo el pago.

Desde el punto de vista jurídico, encontramos en Vásquez (2002) otra definición de comercio electrónico:

> "…cualquier negocio jurídico, dirigido a un intercambio económico, que se realice a través de un sistema electrónico, informático o telemático" (Vásquez, 2002, p.134).

Por otro lado, encontramos que en el comercio electrónico participan como actores principales las empresas, los consumidores y el Estado. Así se distinguen normalmente tres tipos básicos de comercio electrónico:

- entre empresas o B2B (*business to business*)
- entre empresa y consumidor o B2C (*business to consumers*)
- entre empresa y administración o B2A (*business to administrations*)

Las empresas intervienen como usuarias (compradoras o vendedoras) y como proveedoras de herramientas o servicios de soporte para el comercio electrónico: proveedores de servicios de certificación de claves públicas, instituciones financieras, etc. Por su parte, las administraciones públicas, actúan como agentes reguladores y

promotores del comercio electrónico y como usuarias del mismo (por ejemplo en los procedimientos de contratación pública o de compras por la Administración).

En un sentido amplio, los consumidores participarían en dos formas adicionales de comercio electrónico además del B2C: por una parte, el comercio electrónico directo entre consumidores (venta directa entre particulares) y, por otra, las transacciones económicas entre ciudadano y administración (pago de prestaciones sociales, pago de impuestos, etc.).

2.2.2 Evolución histórica del comercio electrónico

2.2.2.1 Introducción

Desde los tiempos más remotos el ser humano ha buscado la mejor forma de comunicarse con otros de su misma especie, aun cuando éstos se encuentren en lugares lejanos. La historia de la comunicación está marcada por los adelantos tecnológicos de cada época y lugar. En un principio, la comunicación que se establecía con otros pueblos lejanos era mediante la voz, viajeros que recorrían grandes distancias con la finalidad de llevar y traer mensajes e información. Con la aparición de la escritura se inicia una nueva era, sin embargo los mensajes seguían siendo enviados de igual manera, era un proceso lento y difícil.

Con el inicio de la era tecnológica, se dispuso de un medio con el cual fue posible establecer una comunicación a distancia y casi instantánea por medio de códigos y claves de sonido: el telégrafo; posteriormente la comunicación humana se vio beneficiada con la invención del teléfono permitiendo el uso de la voz, más adelante vino la radio, la televisión y con ello las computadoras. Estos grandes inventos son la base de los adelantos tecnológicos que disfrutamos hoy en día en cuanto a comunicación, desde el envío y recepción de un fax hasta la comunicación instantánea en cualquier lugar del mundo por medio de Internet.

Internet es hoy en día una infraestructura informática extendida ampliamente, su influencia alcanza no sólo al campo técnico de las comunicaciones entre computadoras (redes), también a toda la sociedad en la medida en que su empleo se incrementa cada vez más para llevar a cabo procesos como el comercio electrónico, la adquisición de información y la interacción entre la comunidad o comunidades remotas.

La evolución histórica del comercio electrónico necesariamente pasa por la evolución histórica de la Internet. Por tanto, se presenta primeramente el desarrollo de Internet para luego presentar propiamente el desarrollo del comercio electrónico.

2.2.2.2 Evolución de la Internet

Ya finalizando la década del 50, en pleno apogeo de la Guerra Fría entre los Estados Unidos de Norteamérica y la U.R.S.S., el Departamento e Defensa de los Estados Unidos comenzó a preocuparse por el desarrollo de tecnologías de comunicación que les permitiera mantener comunicados los distintos puntos de la fuerza armada. En 1962, Paul Baran, investigador de los Estados Unidos propuso un sistema de comunicaciones mediante computadoras conectadas en una red descentralizada, que permitía la comunicación aunque hubiere nodos destruidos. Finalmente en 1969, la Advanced Research Projects Agency (ARPA) del Pentágono, creó la primera red de computadoras que se llamó ARPAnet, que conectaba 4 computadoras a la red inicialmente: Universidad de California en Los Ángeles (UCLA), el Instituto de Investigaciones de Stanford (SRI), la Universidad de California en Santa Bárbara (UCSB) y la Universidad de UTA. En 1971 se habían agregado 11 nodos más y para 1972 había un total de 40 computadoras en la red.

En el año 1972 se presenta la necesidad de establecer un protocolo de comunicación común entre todas las computadoras, que variaban en tipo y sistemas operativos (IBM y Unisys), para que pudieran comunicarse entre sí sin inconvenientes, por lo que se crea el “InterNetworking Working Group”.

En el año 1974, dos investigadores, Vint Cerf (Stanford University) y Robert Kahn (BBN), redactan un documento titulado “A Protocol for PacketNetwork Internetworking”, donde explicaban cómo podría resolverse el problema de comunicación entre los diferentes tipos de computadoras. Pero no fue hasta 8 años después, que esta idea es implementada en su totalidad. En 1978 comenzó a utilizarse en algunas redes, y se la denominó “Transmition Control Protocol - Internet Protocol” (TCP-IP). A partir de aquí (1982) empezó a utilizarse la palabra Internet. Este protocolo, fue adoptado inmediatamente como standard por el Departamento de Defensa de Los Estados Unidos, para su red de computadoras y también, en 1982, ese organismo decidió su separación de ARPAnet y la creación de una red propia llamada MILnet.

A mediados de los años 80's, la National Science Foundation (NSF), decide que es necesaria una red de trabajo de alto desempeño para enlazar 5 centros que poseían supercomputadoras y así poder dar acceso a los investigadores que se encontraban en distintas ciudades de los Estados Unidos. En el año 1987 el NSF crea la NSFnet que conectaba 7 redes con los 5 centros de supercomputadoras antes mencionado. Con esta nueva red, la velocidad de transferencia entre los distintos nodos se incrementó a 1.5 megabits por segundos. Hasta ese momento, la velocidad de transferencia, entre nodos, era de 56 kilobits por segundos.

El protocolo TCP/IP es un sistema de comunicación muy sólido y robusto bajo el cual se integran todas las redes que conforman Internet; durante su desarrollo se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando de esta manera, origen a la red de redes más grande del mundo.

En el año 1971, Ray Tomlinson envió el primer mensaje de correo electrónico. El segundo mensaje, fue enviado a las computadoras que estaban conectadas a la red, donde él realizaba las pruebas y en el mismo anunció la creación del correo electrónico y cómo enviar los mensajes a otros usuarios de la red, utilizando el signo @ después del nombre que el usuario utilizaba para conectarse a la red.

En el año 1990 dejó de funcionar la red de trabajo que dio origen a Internet: ARPAnet. En ese mismo año, el mayor centro de Internet en Europa era el CERN (European High-Energy Particle Physics Lab). En ese organismo, en el año 1992, Tim Berners Lee (en la actualidad es el director del World Wide Web Consortium), crea la World Wide Web, utilizando tres nuevos recursos: HTML (Hypertext Markup Language), HTTP ("Hypertext Transfer Protocol") y un programa cliente, llamado "Web Browser". Todo este trabajo se basó en un escrito de Ted Nelson, en 1974, donde, por primera vez, se habló de Hypertext y links. En 1993, en el National Center for Supercomputing Aplications (NCSA), en la Universidad de Illinois, Mac Andreessen junto con un grupo de estudiantes crean un programa llamado Mosaic (Web Browser), el cual ganó fama rápidamente. Mac Andreessen, al poco tiempo, se alejó del NCSA y junto con Jim Clark fundan Netscape.

En estos momentos Netscape es uno de los programas más utilizados en Internet. La World Wide Web creció rápidamente, a mediados de 1993 solo había 100 sitios World Wide Web, en Enero del 96, ya existían 90.000. Todo este crecimiento ha sido propiciado por los fines comerciales que persiguen la mayoría de las empresas que lo forman, de esta manera entramos a la nueva era comercial de Internet.

Internet como ahora lo conocemos encierra una idea técnica clave, la de arquitectura abierta de trabajo en red, así como múltiples redes independientes, de diseño casi arbitrario. En una red de arquitectura abierta, las redes individuales pueden ser diseñadas y desarrolladas separadamente, donde cada una puede tener su propia y única interfaz. Cada red puede ser diseñada de acuerdo con su entorno específico y los requerimientos de los usuarios, no existen restricciones en los tipos de red que pueden ser incorporadas ni tampoco en su ámbito geográfico.

Así surgió y se fue desarrollando esta gran revolución llamada Internet.

2.2.2.3 Evolución del comercio electrónico

El comercio electrónico data de los años 70's cuando se utilizaba la transferencia electrónica de fondos (EFT Electrónic Fund Transfer). Las aplicaciones estaban restringidas a grandes corporaciones, instituciones financieras y unos cuantos negocios pequeños. Después aparece el Intercambio Electrónico de Datos (EDI Electronic Data Interchange) que produjo la expansión de las transacciones financieras a otros tipos de operaciones y amplió la participación de compañías financieras a compañías manufactureras, minoristas y proveedores de servicios entre otras. Le siguieron muchas otras aplicaciones como el sistema de reservaciones en la industria turística.

Con la comercialización de Internet a principio de los años 90's y su rápido crecimiento a millones de clientes potenciales se aceptó el término de comercio electrónico o "e-commerce". Sus aplicaciones se fueron expandiendo rápidamente con el desarrollo de las tecnologías de redes, softwares, protocolos y especificaciones. También se expandió por el incremento en la competencia y otras presiones de negocios.

Se puede decir que la era comercial de Internet inicia a partir de 1993. Cuando las primeras empresas se dan cuenta de la potencialidad que ofrece la red de redes para el desarrollo del comercio.

En septiembre de 1993 se inició el primer servidor Web en español. En estos momentos se aumenta la potencia de las redes troncales de E.E.U.U., y en 1994 se eliminan las restricciones de uso comercial de la red y el gobierno de E.E.U.U. deja de controlar la información de Internet. 1995 es el año de la explosión de Internet. Puede ser considerado como el nacimiento de la Internet comercial. Desde ese momento el crecimiento de la red ha superado todas las expectativas. Este hecho se produce porque es en este año cuando la WWW supera a *ftp-data* transformándose en el servicio más popular de la red, después de que el año anterior superara a *telnet*. Además de ser el servicio más popular es el que hace llegar Internet a la gente.

La explosión de Internet pasa por la entrada de servicios tradicionales como la radio, la televisión, la banca y la telefonía, que se van integrando en mayor o menor medida a la Red.

Empiezan a incrementarse de una manera casi exponencial el número de servicios que operan en la red, ya que para esta época ya operan bancos en la red *(First Virtual)*, una radio comercial de difusión exclusiva en Internet *(Radio HK)*. Gobiernos de todo el mundo se conectan a la red, y el registro de los dominios deja de ser gratuito para pagarse una cuota anual de $50. El Web continúa hoy creciendo y cambiando de maneras a veces impredecibles.

A partir de aquí el desarrollo de la tecnología es impresionante. Se desarrollan los motores de búsqueda que rápidamente añaden búsquedas inteligentes en varios idiomas. Se empieza a utilizar el lenguaje Java y se desarrollan tecnologías como entornos virtuales (VRML) o el teléfono por Internet, que permite la conexión con todo el mundo a precio de llamada local. Se desarrolla de una manera definitiva el comercio electrónico, para comprar productos y servicios a través de Internet. Se pueden ver cientos de televisiones y escuchar radios de todo el mundo en tiempo real. Los bancos se asientan en la Red y la gente empieza a ceder en su miedo inicial, confiando en la seguridad que ofrecen los servidores seguros. Aparecen los primeros virus de HTML. Son virus de macro incrustados en documentos de Word, que se transmiten por correo electrónico como archivos adjuntos y se ejecutan en las máquinas sin protección contra virus de macro.

La tecnología de telefonía móvil y la de Internet finalmente se unen para poder acceder desde los teléfonos móviles a la red de redes. Si bien es cierto que dispositivos inalámbricos ya accedían a la red, es con la definición del conjunto de protocolos WAP *(Wireless Application Protocol)* cuando los dispositivos inalámbricos, y fundamentalmente los teléfonos móviles, se conectan a Internet. WAP ha tenido un importante respaldo por parte de fabricantes de teléfonos, operadoras, compañías de software y desarrolladores, lo que ha provocado que en muy poco tiempo se convirtiera en estándar. Surgió entonces el *WAP Forum*, que hoy agrupa al 90% de los fabricantes

de teléfonos móviles y cubre unos 100 millones de teléfonos en todo el mundo. Fruto de esta entrada de la tecnología móvil en Internet es el desarrollo de páginas WML preparadas para ser leídas desde cualquier terminal WAP. Estas páginas ofrecen servicios de todo tipo, desde buscadores, guías y entretenimientos hasta aplicaciones de bolsa en tiempo real y comercio electrónico.

El futuro de Internet pasa por que la red amplíe el ancho de banda (Internet2) para permitir aplicaciones como telemedicina y videoconferencia de alta calidad, y por la telefonía sin hilos, desde donde se podrá acceder a multitud de servicios.

A finales de 1996 se reunieron 34 universidades de los Estados Unidos con el fin de acordar los pasos que deberían seguir para desarrollar una infraestructura, tanto en el plano físico (hardware), como en el lógico (definición de nuevos estándares, desarrollo del software necesario, etc.) en la que fuera posible explotar aplicaciones avanzadas. Una red de alta velocidad, que se estima entre 100 y 1.000 veces más rápida que la actual, donde la investigación y las experiencias avanzadas encuentren su espacio de cultivo ideal.

Al proyecto se le han ido sumando más universidades, más de 160 en la actualidad, el gobierno de los E.E.U.U. y diversas empresas que han aportado mucho dinero para el proyecto. En la página de Internet2 se sientan sus bases diciendo:

> "Construida sobre el tremendo éxito que en los últimos diez años ha tenido la generalizada y adaptada investigación de la tecnología de Internet para necesidades académicas, la comunidad universitaria se ha unido con el gobierno y la industria como socios para acelerar el próximo paso del desarrollo de Internet en la enseñanza. El proyecto Internet2 está dando energía y recursos para el desarrollo de una nueva familia de avanzadas aplicaciones para encontrar lo que la educación demanda en investigación, enseñanza y aprendizaje. Las universidades de Internet2 trabajando con la industria, el gobierno y otras organizaciones de investigación y de educación conectadas se están dirigiendo al mayor desafío para dar un soporte de red a la nueva generación de universidades."(Mundo-R, 2005).

De 1995 a 1999 se desarrollaron muchas aplicaciones innovadoras que iban desde publicidad a subastas y experiencias en realidad virtual utilizando todo el desarrollo tecnológico alrededor de la Internet.

2.2.3 Ventajas y Desventajas del Comercio Electrónico

2.2.3.1 Introducción

Sin duda alguna el desarrollo del comercio electrónico tiene grandes ventajas en lo que se refiere al impacto económico de las empresas, por su concepción a nivel mundial, pero también tiene su lado negativo, porque incrementa las posibilidades de comisión de delitos. En las siguientes secciones se listan las ventajas y desventajas identificadas.

2.2.3.2 Ventajas Del Comercio Electrónico

El comercio electrónico permite transacciones de compra y venta sin limitación física territorial, las empresas con un sitio Web tienen oportunidad de vender a cualquier persona ubicada en cualquier parte del mundo. Así pues, se puede encontrar muchas ventajas de este tipo de comercio, entre ellas están:

- Permite hacer más eficientes las actividades de cada empresa, así como establecer nuevas formas, más dinámicas, de cooperación entre empresas.
- Reduce las barreras de acceso a los mercados actuales, en especial para pequeñas empresas, y abre oportunidades de explotar mercados nuevos.
- Presencia de la empresa a nivel global.
- Aumento de la competitividad.
- Oferta de productos y servicios más personalizados.
- Cadenas de entrega más cortas o inexistentes.
- Reducción de costos y de precios.
- Oportunidad de nuevos negocios, productos y servicios.
- Para el consumidor, amplía su capacidad de acceder a prácticamente cualquier producto y de comparar ofertas, permitiéndole además convertirse en proveedor de información.
- Servicios de mejor calidad.
- Reduce o incluso elimina por completo los intermediarios, por ejemplo en la venta de productos en soporte electrónico (textos, imágenes, vídeos, música, programas, etc.) que se pagan y entregan directamente a través de la red.

- Superación del factor geográfico en la contratación.
- Inexistencia de horarios en la adquisición de productos y servicios.
- Aparición en el mercado de nuevos agentes y sectores: empleo.

El comercio electrónico obliga a redefinir el papel de los intermediarios entre productor y consumidor, eliminándolos en algunos casos, pero también creando la necesidad de funciones de intermediación nuevas en otros. Igualmente el comercio electrónico afecta al papel tradicional de otros actores, como las entidades financieras o los fedatarios públicos.

2.2.3.3 Desventajas Del Comercio Electrónico

El comercio electrónico plantea también problemas nuevos o agudiza algunos ya existentes en el comercio tradicional, entre ellos encontramos los siguientes mencionados por Téllez (2004):

- La validez legal de las transacciones y contratos "sin papel".
- La necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio.
- El control de las transacciones internacionales, incluido el cobro de impuestos.
- La protección de los derechos de propiedad intelectual.
- La protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales.
- La dificultad de encontrar información en Internet, comparar ofertas y evaluar la fiabilidad del vendedor (y del comprador) en una relación electrónica.
- La seguridad de las transacciones y medios de pago electrónicos.
- La falta de estándares consolidados y la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles.
- La congestión de Internet y la falta de accesos de usuario de suficiente capacidad a bajo costos.

Los problemas citados tienen, en mayor o menor medida, un componente legal o regulatorio y un componente tecnológico, por lo que su solución requiere actuaciones en ambos sentidos.
Los sistemas de comercio electrónico disponibles actualmente son en general de alto costo y reducida interoperabilidad.

2.2.4. Desarrollo de Internet y comercio electrónico en Costa Rica

En esta sección se ofrece un panorama general de la situación costarricense en relación con el desarrollo de Internet y el comercio electrónico.

2.2.4.1 Internet en Costa Rica

El proceso de interconexión de Costa Rica a las grandes redes de investigación se inicia en 1990 con el establecimiento, en la Universidad de Costa Rica (UCR), del primer nodo de la Red Bitnet en la región Centroamericana y su integración, dos años después, a la Red Internet, el 26 de enero de 1993.

Paralelamente con las conexiones pioneras de la UCR, se establece la Red Nacional de Investigación de Costa Rica (CRNet), una red digital que utiliza enlaces de fibra óptica para interconectar las instituciones académicas y de investigación más importantes del país, permitiendo amplio acceso a la información y recursos computacionales del mundo.

Estos logros importantes, no sólo permiten la conectividad instantánea de un gran número de personas con el resto del mundo, sino que introducen en el país por primera vez la tecnología inter-redes a gran escala.

Se puede decir que el servicio de Internet a nivel comercial en Costa Rica se inauguró en 1994 por medio de Radiográfica Costarricense S.A. (RACSA), que permitió expandir las posibilidades tecnológicas y de información entre empresas, facilitar el acceso y permitir el intercambio rápido de información actualizada.

Desde su inicio, el crecimiento del servicio de Internet en Costa Rica ha experimentado un crecimiento constante de más del 10% anual, según RACSA (2006).

Dentro de las fortalezas más relevantes de Internet están su cobertura mundial y su capacidad de permitir la interacción global entre diferentes computadoras a través de un lenguaje común. Esto permite al interesado establecer contacto con diferentes personas a nivel mundial, facilitando a los proveedores de información o de servicios alcanzar una inmediata penetración de mercado hacia clientes potenciales y un acceso dinámico y económico a millones de servidores de información gráficos en todo el mundo. Todo ello de forma dinámica y económica.

Según estudios realizados por la empresa CID Gallup, mencionados en RACSA (2006), especialista en estudios de opinión, se tiene los datos del siguiente cuadro:

Cuadro 1. Computadoras en hogares y uso de Internet.

	2003	2005
Acceso a Internet	24% (1 millón de personas) 48% de los hogares (unas 450.000 familias) al menos un miembro accede con cierta frecuencia Internet desde su hogar, trabajo, centro de estudios o desde los *cafés-Internet.* 600 mil personas tienen facilidades desde donde trabajan o estudian.	Aproximadamente 1.370.000 personas tienen acceso a Internet desde su hogar, el trabajo o centro de estudios. 1.070.000 tienen facilidades desde donde trabajan o estudian
Hogares con computadoras	25% (de estos 38% son del área Metropolitana y 54% fuera de él).	34%, el 50% de éstos tenían acceso a Internet.
Uso de café-Internet	300.000 personas 500 establecimientos	650.000 personas 700 establecimientos

Fuente: elaboración propia con datos de RACSA (2006).

Adicionalmente, datos del 2003 indican que cada mes se dan, en promedio, unos 50.000 accesos por medio de los servicios de RACSA, que no requieren contrato previo (900 En Línea y tarjetas prepagadas). Unas 300.000 mil personas navegan cada día por Internet en el país, circulando unos 3 millones de correos diarios.

En el país cerca de un millón de personas cuentan con dirección de correo electrónico (RACSA también administra el servicio de correo gratuito costarricense.cr, que cuenta actualmente con más de 350.000 usuarios), siendo el intercambio de comunicación y la obtención de información para los estudios los usos más utilizados del servicio Internet en Costa Rica, pero ha venido creciendo en forma sostenida e importante también el uso de Internet para realizar compras y transacciones en línea.

En conclusión, es posible afirmar que cerca de un millón de personas acceden con cierta frecuencia a la red Internet en Costa Rica, y cerca de 2 millones tienen posibilidades reales de acceder.

Por otro lado, encontramos datos del Instituto Nacional de Estadísticas y Censos, en los cuales puede verse el crecimiento que ha tenido Costa Rica en materia de uso de computadoras e Internet en los hogares. Los siguientes cuadros y figuras muestran estos datos.

Cuadro 2. Viviendas con computadoras y acceso a Internet. 2000-2005. Costa Rica.

	2000	2001	2003	2005
Total de viviendas	804.251	967.060	1.040.612	1.114.210
Viviendas con computadoras	102.334	168.050	229.166	551.362
Viviendas con Internet	28.766	51.710	104.139	213.133

Fuente: elaboración propia con datos de INEC (2000-2005).

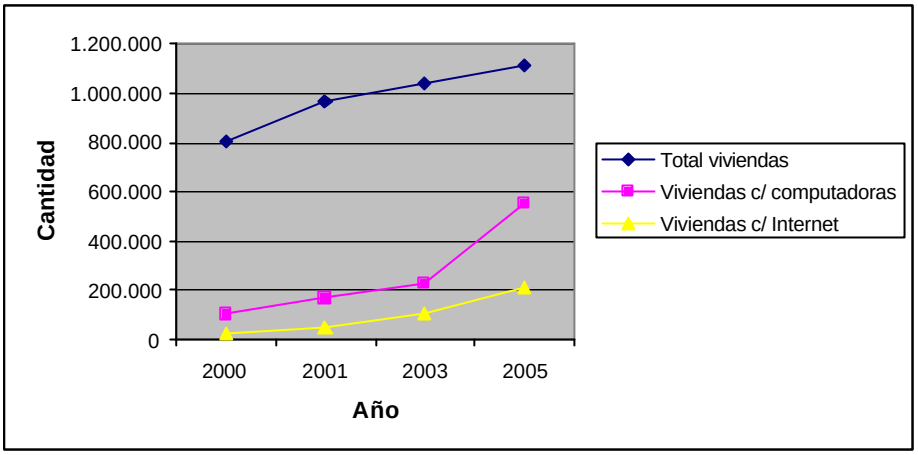


Figura 1. Viviendas con computadoras e Internet. 2000-2005. Costa Rica.
Fuente: elaboración propia con datos de INEC 2000-2005.

Se observa de los cuadros anteriores, que del año 2000 al 2003 hubo un crecimiento bastante constante, del número de computadoras en las viviendas, pero del 2003 al 2005, se observa un incremento de más del doble que los años anteriores, no así el de Internet, que aunque se refleja siempre un crecimiento, no es proporcional con el aumento de computadoras. Lo que significa que los hogares han realizado esfuerzos para dotarse de computadoras primero, y luego que también existe un esfuerzo para dotarse de Internet. Aún así, todavía hay una proporción grande de viviendas que poseen computadoras pero sin Internet, como puede verse en la siguiente figura:

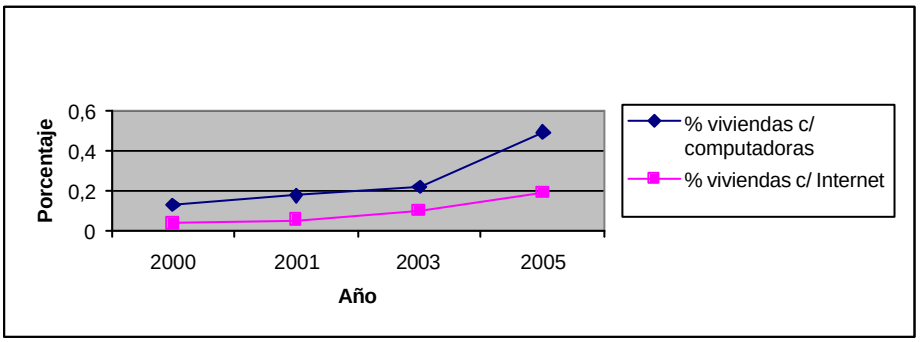


Figura 2. Porcentaje de viviendas con computadoras e Internet. 2000-2005. Costa Rica.
Fuente: elaboración propia con datos de INEC 2000-2005.

Estos datos ubican a Costa Rica entre los primeros países del mundo, en relación con el número de habitantes, con acceso a Internet.

Un informe, del 20 noviembre del 2003, preparado por la Secretaría General de la Conferencia sobre Comercio y Desarrollo de las Naciones Unidas (UNCTAD, 2003), sobre el comercio electrónico y el desarrollo, indica que Costa Rica se encuentra en el lugar #49 a nivel mundial en cuanto al Índice de Preparación de la Red (NRI - *Network Readiness Index*), definido como el grado de preparación de una nación para participar y beneficiarse del desarrollo de las tecnologías de información y comunicación.

Otro informe del mes de octubre 2004 de la Unión Internacional de Telecomunicaciones, ubica a Costa Rica en un puesto privilegiado de las naciones en el mundo mejor equipados con Internet y otras tecnologías de la información, pues coloca al país en el puesto #58, la cuarta mejor de América Latina, sólo superado por Chile (43), Uruguay (51) y Argentina (54). La situación de otros países de la región es la siguiente: México está de #64, Brasil de #65, Panamá #72, Venezuela #73, Colombia #79, Perú #83 y Ecuador #96. Los 10 países mejor ubicados son, en su orden, Suecia, Dinamarca, Islandia, Corea del Sur, Noruega, Holanda, Hong Kong, Finlandia, Taiwán y Canadá[2]. En el siguiente cuadro se muestra la posición de Costa Rica en el *ranking* mundial.

[2] Mayor información puede encontrarse en (ITU Telecom Asia, 2004).

Cuadro 3. Países mejor equipados con Internet y Tecnología de la Comunicación 2003.

País	Posción
Suecia	1
Dinamarca	2
Islandia	3
Corea del Sur	4
Noruega	5
Holanda	6
Hong Kong	7
Finlandia	8
Taiwán	9
Canadá	10
Chile	42
Costa Rica	58
México	64
Brasil	65

Fuente: Unión Internacional deTelecomunicaciones (ITU, 2004)

Como parte del plan para disminuir la brecha digital, el Ministerio de Ciencia y Tecnología (MICIT), junto con entes estatales (Bancos Estatales, Intituto Costarricense de Electricidad (ICE), Radiográfica Costarricense Sociedad Anónima (RACSA)) y empresas privadas (DHL, INTEL, DELL, LANIX, Microsoft), inauguraron en el mes de junio de 2004, un programa con el fin de dotar de computadoras, programas e Internet en condiciones accesibles y muy favorables, de forma que todos los costarricenses puedan beneficiarse de las oportunidades que brindan las nuevas tecnologías de información y comunicación (TIC 's).

Parte del plan es que los bancos estatales den crédito a personas con salarios inferiores a ¢95,000.00, para la compra de computadoras, con intereses del 20% anual a 60 meses plazo.

Con esto se prevé la venta e instalación a precios accesibles de al menos 100.000 computadoras, a fin de extender el uso de Internet en el país.

Se esperaba que al cabo de 18 meses aumentara el parque tecnológico en un 33 por ciento, calculado en 300 mil computadoras.

De acuerdo con Alejandro Urbina (2004), el impacto social de la Internet ha sido bajo porque se requiere disponibilidad de conexión dedicada de banda ancha, las veinticuatro horas del día, los siete días de la semana, él afirma que:

> "En Costa Rica el impacto ha sido menor por el mediocre acceso a Internet con que cuenta el país. El acceso residencial a Internet de banda ancha está limitado al que brindan las televisoras por cable. La solución –la Red de Internet Avanzada– propuesta hace más de dos años por el padre nacional de Internet, Guy de Téramond, sigue empantanada (intencionalmente o no) en la burocracia del ICE." (Urbina, 2004, p. 1)

También indica que es necesario que el Gobierno elimine los obstáculos para la difusión de la conexión de banda ancha.

El viernes 9 de julio del 2004, en el periódico *La Nación*, Oviedo informó que RACSA mejoró la capacidad de Internet, incrementando la capacidad del país para conectarse en un 33%, a través de uno de los dos cables submarinos que comunican al país con el resto del mundo.

En los siguientes gráficos se muestra el crecimiento que ha tenido el servicio de Internet conmutado y dedicado, tanto residencial como empresarial.

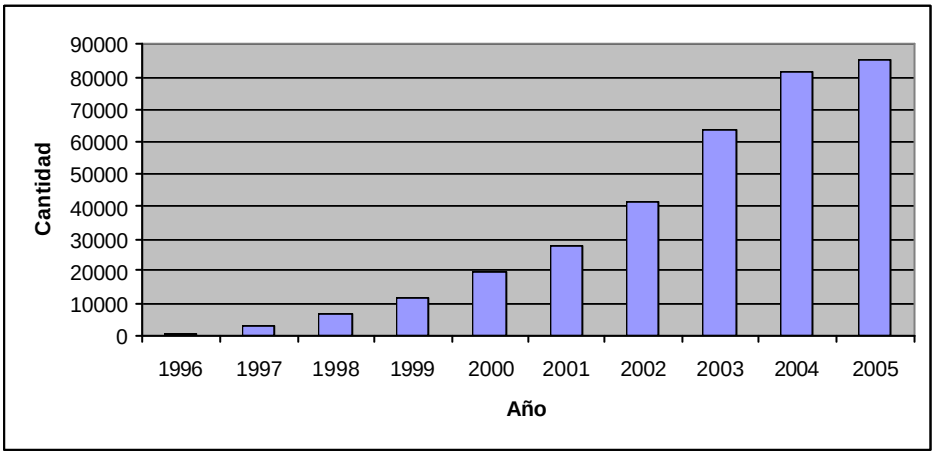


Figura 3. Clientes de Servicio de Internet conmutado (Residencial).

(Fuente: elaboración propia con datos de RACSA, 2006)

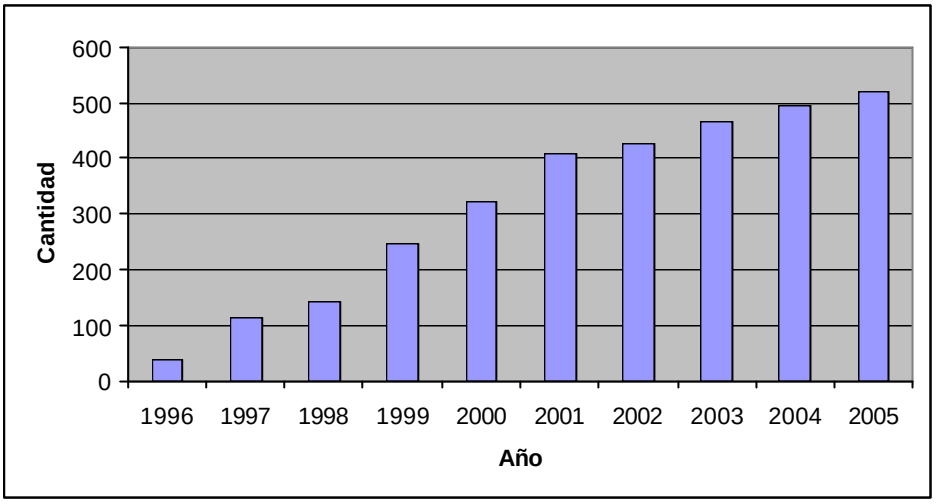


Figura 4. Clientes de Servicio de Internet dedicado (Empresarial).
(Fuente: elaboración propia con datos de RACSA, 2006)

En una noticia de La Nación del 20 de julio del 2006, se informa que las tarifas de Internet bajaron de precio, ofreciéndose desde $16 para velocidades de 128/64 hasta $169 para velocidades de 4.096/768, las tarifas disminuyeron y se aumentó las velocidades al doble.

En Leitón (2006) se informa que existen varios proyectos en marcha en el país con el fin de extender el acceso a Internet a la población de menores ingresos. Entre ellos se mencionan que:

1- El Ministerio de Ciencia y Tecnología pretende implementar en los próximos 4 años al menos 352 “centros comunales inteligentes”, estos centros tendrán 6 computadoras cada uno de “buena calidad”, y ofrecerán cursos gratuitos cada dos meses. El 25 de julio de 2006 se inauguró el primer centro en Nicoya.

2- El ICE, la Compañía de Fuerza y Luz (CNFL) y la Junta Administrativa de Servicios Eléctricos de Cartago (Jasec) realizan proyectos para ofrecer Internet por la vía eléctrica.

3- En la Asamblea Legislativa se discute un préstamo para el Proyecto de Ley Programa de ciencia y tecnología para la competitividad, el préstamo pretende dedicar $28 millones para investigación y formar recursos humanos en pequeñas y medianas empresas, incluido Internet.

4- La Fundación Omar Dengo, las universidades y las empresas también tienen proyectos para aumentar la cobertura del acceso.

En Gutiérrez (2006) se informa que se instalará una red de Internet de libre acceso en 50 puntos importantes del Valle Central, se espera que para noviembre de 2006 CR inalámbrico esté implementado. El proyecto es implementado por la Fundación Costa Rica para el Desarrollo Sostenible y la empresa Cisco Systems. Esto permitirá democratizar Internet y disminuir la brecha digital en Costa Rica. Se instalarán dispositivos de conexión (*routers*) a la red para que las personas que asisten a estos lugares puedan tener acceso gratuito al servicio de Internet. Entre los lugares donde se instalarán los *routers* están: la Biblioteca Nacional, la Plaza de la Cultura, la Municipalidad de San José, Hospital de Niños, Teatro Nacional, Edificio de Correos.

Por otro lado, la promulgación de la Ley 8454 de Certificados, firmas digitales y documentos electrónicos el 30 de agosto de 2005, y su respectivo Reglamento el 20 de marzo de 2006, es un paso más del país para dar seguridad jurídica a los documentos electrónicos y posibilitar el paso al Gobierno Digital.

El Gobierno de Costa Rica no ha dejado de promover y desarrollar proyectos en aras de aumentar el acceso y cobertura de la Internet. En Lara (2007) se informa de que el Gobierno convocó a proveedores de computadoras a presentar ofertas de equipos en el marco de un plan que facilitará a los maestros, unos 50.000 educadores, la compra de estos que les permitan acceso a Internet. El plan tiene la iniciativa de cerrar distancias sociales y económicas en la población por falta de acceso a medios electrónicos, en particular a Internet, lo cual reduciría la brecha digital.

Según el barómetro de CISCO la penetración de banda ancha en Costa Rica creció un 26% en el primer semestre del 2007 (Fonseca, 2007), contabilizando 118.853 conexiones de este tipo a junio del 2007.

Para esta fecha aún existen cuatro cantones de Puntarenas (Aguirre, Buenos Aires, Coto Brus y Osa) que no cuentan con ningún tipo de conexión a Internet. Con estos datos, el índice de penetración de banda ancha en Costa Rica se sitúa en 2,7% por cada 100 habitantes, colocando al país por encima de Colombia y Perú, pero por debajo de Chile, Brasil y Argentina (Fonseca, 2007).

Todo lo anterior muestra los esfuerzos que el país está realizando para disminuir la brecha digital y hacer la Internet accesible a todos, diminuyendo los costos con el fin de que una mayor población costarricense pueda acceder a este servicio, aumentando las velocidades y ubicando puntos de acceso gratuitos en lugares públicos. Por otro lado, el Estado realiza esfuerzos para dotar de computadoras y acceso a Internet en el Sistema de Educación Primaria y Secundaria, además de aquellos para incorporar en su propia Administración Pública esta tecnología.

2.2.4.2 Comercio electrónico en Costa Rica

El desarrollo de Internet es importante porque es la plataforma para una gran cantidad de servicios y relaciones de comunicación, entre ellos, el comercio electrónico. No es posible el desarrollo del comercio electrónico sin la plataforma básica del servicio de Internet.

El desarrollo del comercio electrónico en Costa Rica es incipiente; son pocas las empresas costarricenses que se han aventurado a utilizar el medio electrónico para sus transacciones comerciales. A pesar de ello, ya muchos usuarios costarricenses han utilizado la Internet para realizar alguna actividad comercial, por medio de páginas de empresas ubicadas en otras partes del mundo.

Las empresas consideradas en el estudio de González y otros (2000), ofrecen gran variedad de líneas de artículos y servicios por medio de comercio electrónico, entre las que se pueden mencionar: ferretería, maquinaria y herramientas, abarrotes, repostería, noticias, floristería, café, teléfonos, artesanías, lavandería, alquiler de videos, hoteles, servicios asociados al turismo y servicios bancarios.

De acuerdo con el estudio de González y otros (2000), en el año 2000, aproximadamente 300 empresas tenían presencia en la red con una página en Internet, pero que muy pocas realmente la estaban utilizando para aumentar sus ventas o reducir sus costos. Sólo aproximadamente 20 empresas sí estaban realizando comercio electrónico y sólo el 14% de los *internautas* costarricenses realizaban compras por Internet. Estas pocas empresas que han incursionado en ventas en línea por Internet notan que el aumento de su clientela es bajo.

Estos investigadores desarrollaron propuestas de estrategias de mercadeo para impulsar el uso de Internet y fomentar la cultura de consumo, con el fin de impulsar el comercio electrónico en el país. Para ellos:

> "El Comercio Electrónico es bastante nuevo para el sector empresarial en Costa Rica. El volumen de ventas por medio de Internet no ha generado utilidades para las empresas que lo están implementando en el mercado costarricense." (González, 2000, p.111).

Estos investigadores concluyeron que bs elementos más importantes que limitan el desarrollo del comercio electrónico de Costa Rica están: el tamaño del mercado es pequeño, son pocas las personas con acceso a Internet con poder de compra, la oferta costarricense en Internet es reducida e inseguridad en los medios de pago.

También encontramos en Salas y Fernández (2003) que el comercio electrónico en Costa Rica está apenas en pañales, el nivel de ventas de los sitios costarricenses aún se considera bajo por los propios empresarios del comercio electrónico, a excepción de sitios orientados a segmentos ubicados en el exterior.

Por otro lado, Salas y Fernández (2003) indican las características de las compras por Internet que realizan los costarricenses; entre lo que se destaca:

> "-Que la mayoría de los artículos que adquieren son software, hardware, música, libros y revistas. Esto se debe principalmente a las facilidades de envíos de estos productos, ya que son adquiridos en su mayoría en sitios de Estados Unidos.
> -El acceso a Internet se ha duplicado en los últimos años y la tendencia muestra que se puede esperar el mismo crecimiento anualmente.
> -Las personas que acceden la red de Internet en Costa Rica pertenecen a un nivel socioeconómico medio alto y alto, con estudios universitarios y con edades entre 18 a 40 años." (Salas y Fernández, 2003, p.195).

A pesar del desarrollo que ha tenido Internet en Costa Rica en los últimos años, todavía la mayoría de los costarricenses no la utilizan para comprar. Al respecto, Alvarado y Leitón (2003) indican que el desconocimiento del funcionamiento del sistema, las dificultades de acceso a Internet y el temor a utilizar las tarjetas de crédito para comprar son problemas que afectan el comercio electrónico.

Las siguientes es una lista no exhaustiva de las empresas en territorio nacional que realizan transacciones comerciales electrónicas:

- Ticonet
- Spoon
- Lachner & Sáenz
- Capris S. A.
- Banco de Costa Rica
- Banco Nacional de Costa Rica
- Banex
- Banco FINADESA
- Café Britt
- CRPAGE
- Teleférico del Bosque Lluvioso
- Lalibrería.com
- Crautos
- Grupo Taca
- Virtual Plaza
- Tienda Virtual Jiménez & Tanzi de Costa Rica

Una lista (actualizada al 30 mayo del 2004) de algunos de los 50 sitios más populares de Costa Rica en Internet, según un sondeo efectuado por *La Nación*, basado en el *ranking* de Alexa.com (compañía subsidiaria de Amazon.com), se presenta en el anexo 8.

Radiográfica Costarricense S.A. (RACSA) publica anualmente una Guía de *Servicios de infocomunicaciones*, en la que presenta un directorio con las direcciones y los correos electrónicos de todas las empresas que ha abierto algún sitio Web para comerciar sus

productos o servicios. Esta guía se puede adquirir, de forma gratuita, en las oficinas de RACSA en San José y de esta forma poder acceder a las diversas empresas virtuales de este país.

En el estudio de González y otros (2000), se realizaron entrevistas a 22 personas, representantes de empresas costarricenses relacionadas con el comercio electrónico. Como los principales problemas enfrentados al incursionar en este campo en Costa Rica, los entrevistados indicaron:

- "Alta inversión inicial en tecnologías de información para lograr que el sitio sea eficaz y eficiente.
- Lograr que el sitio sea conocido, por lo tanto han tenido que realizar una fuerte inversión en la estrategia de comunicación.
- Lograr que el sitio sea visitado por clientes potenciales.
- Lograr que el visitante no sólo navegue en el sitio, sino que complete una compra y que quien realice una compra vuelva al sitio y recompre en éste.
- Lograr efectividad en la logística de entrega. Atender en forma oportuna por medio del sitio, a un número creciente de clientes.
- Cambio de cultura, alcance mundial con una estrategia local.
- Utilizar una forma de pago que transmita seguridad al consumidor y no comprometa la liquidez de la empresa.
- Desconfianza y temor del consumidor ante la nueva forma de adquisición de productos y servicios.
- El costo y tiempo que representa para los consumidores conectarse a Internet para realizar sus compras.
- La tecnología imperante en el país y el monopolio en las telecomunicaciones.
- No disponer del pago en línea, al utilizar el cliente tarjetas de crédito.
- Capacidad de reacción ante volúmenes altos de demanda.
- Ser pioneros en el país, ya que la experiencia costarricense en comercio electrónico es incipiente, por lo tanto se carece de la suficiente retroalimentación.
- Las empresas que son 100% virtuales no tienen imagen de marca en el mercado, por lo que el consumidor es más desconfiado al realizar sus compras en estos sitios.
- Segmentos de consumidores con características atractivas que pudieran ser explotadas por medio del comercio electrónico (por ejemplo, personas mayores, pensionados, amas de casa), tienen todavía mucho temor de utilizar Internet.
- Empresas en Costa Rica que desarrollan sitios y portales, que ofrecen productos y servicios, que luego no entregan a las empresas, por lo que éstas se sienten defraudadas, al no ofrecer a sus clientes las facilidades que esperaban, con la consiguiente pérdida de la inversión realizada.
- Falta de legislación de comercio electrónico."(González y otros, 2000, p.43)

En ese mismo estudio, los entrevistados consideraron también que al consumidor final se le presentan ciertos problemas al momento de decidirse a realizar una compra por Internet, tales como:

- “Necesidad de ver, oler, tocar y disponer inmediatamente del producto adquirido.
- Poca cultura de compra en Internet en el mercado costarricense, el cliente prefiere seguir utilizando los medios tradicionales que estas empresas le han ofrecido para realizar sus compras.
- Desconfianza de brindar datos confidenciales por Internet.
- Dificultad para encontrar en Internet los sitios o productos de su interés, si no conoce de antemano la dirección.
- Desconfianza a la hora de pagar por adelantado.
- Inseguridad del cliente al utilizar sus tarjetas de crédito para el pago de los productos adquiridos.
- Es muy importante para el cliente que los sitios sean claros y fáciles de usar, que le permitan realizar en forma ágil las compras, ya que el tiempo de conexión tiene un costo.
- Poca oferta de productos de empresas ubicadas en el país, que le permitan reducir el tiempo y el costo en su compra.
- Desconfianza en el sistema de correo costarricense.
- Desconocimiento del cliente de los beneficios que le ofrece el comercio electrónico. Por ejemplo ahorro de tiempo, comodidad, precio, seguridad y más información, al comprar sin tener que salir de su hogar u oficina.” (González y otros, 2000, p. 45).

A pesar de los problemas anteriores, el estudio de Guerrero y Montero (2001), basado en un estudio de la compañía publicitaria Nazca Saatchi y Saatchi del año 2000, indica que:

> “se estima que por lo menos un millón de dólares fue el monto de las transacciones por concepto de comercio electrónico realizadas en Costa Rica. Por su parte la empresa Aerocasillas, calcula que en Costa Rica se traslada una tonelada diaria por compras realizadas en Internet.” (Guerrero y Montero, 2001, p. 212).

En ese mismo estudio y basados en un sondeo realizado por la Nación (publicado el 25 de junio del 2001) a nacionales que utilizan la Internet para realizar compras, se señalan las siguientes razones por la que los ticos prefieren comprar fuera del país:

> “-Porque los sitios del país no ofrecen lo que se requiere.
> -Los sitios locales no ofrecen lo que buscan los costarricenses.
> -Porque sale mejor comprar afuera.
> -No compran en Costa Rica por el precio y la falta de información” (Guerrero y Montero, 2001, p. 215).

Más recientemente, en otra noticia publicada por La Prensa Libre del 2 de marzo de 2006, se indica:

> “Costa Rica registró en 2005 un crecimiento del 32%, respecto al año anterior en cuanto a volumen de ventas de compras por Internet procesadas con productos de marca VISA; alcanzando los 43 millones de dólares.” (Acuña, 2006, p.8)

A pesar de que los beneficios de las compras virtuales realizadas por los costarricenses no sean para las empresas locales, se puede apreciar que el costarricense está perdiendo el temor de adquirir mediante esta forma de transacción comercial, aspecto que puede considerarse beneficioso para las empresas locales que tienen como meta el incursionar en el comercio electrónico.

2.2.4.3 Conclusiones

Se ha producido un crecimiento en el desarrollo de Internet en Costa Rica y en la presencia de un número cada vez mayor de empresas costarricenses en la red. También se constata un crecimiento del número de costarricenses que utilizan Internet, ya sea para buscar información, realizar comunicaciones mediante correo electrónico o para comprar.

A pesar del crecimiento que ha tenido la Internet en Costa Rica todavía muchos costarricenses no la utilizan para sus compras, lo cual obedece principalmente a la inseguridad en el medio de pago, un servicio de acceso a Internet inadecuado y costoso, además de falta de conocimiento.

Por otro lado, aunque el crecimiento de las compras por Internet por parte de los costarricenses todavía es bajo, se observa que el costarricense ha incrementado las compras por Internet y éstas se realizan principalmente a empresas fuera del territorio nacional.

Igualmente existen todavía muchas empresas que no aprovechan las ventajas que ofrece Internet para comercializar sus productos o servicios. Sin embargo, ya muchas de ellas tienen presencia en la Red para publicitar sus productos y servicios. Los Bancos y los periódicos ofrecen servicios por Internet gratuitos y otras empresas han aprovechado esta plataforma para mercadear y vender a nivel internacional.

El desarrollo del comercio electrónico ha sido gracias a la evolución que ha tenido la Internet, un tema novedoso y revolucionario en lo que se refiere al comercio

internacional, pero también trae consigo la posibilidad y facilidad de que se den una gran cantidad de problemas y de comisión de delitos.

Estas posibilidades de comisión de delitos e inseguridad que existe por el uso de la red para las transacciones comerciales, hacen que sea necesario establecer una regulación adecuada que permita proteger los derechos de los involucrados en una transacción comercial, y que no obstaculice el desarrollo del comercio.

2.3 Problemática jurídica y técnica del comercio electrónico

2.3.1 Introducción

Indica Molina (1994) que las tecnologías de la Información y la Comunicación ha provocado un volumen muy importante de intercambio de datos entre los diferentes países; y que esto también ha provocado un abierto conflicto de intereses entre los países productores y consumidores de datos informáticos. Dice que su reglamentación es uno de los problemas más urgentes del Derecho Internacional de nuestros días.

El surgimiento del comercio electrónico trae paralelamente problemas jurídicos y técnicos de gran diversidad. En algunos casos es una simple aplicación de las normas tradicionales, puesto que el comercio electrónico no es más que comercio utilizando las nuevas tecnologías de información y comunicación. Pero en otros casos exigen la implementación de nuevas reglas o un nuevo sistema basado en los nuevos conceptos.

La mayor dificultad que enfrenta la Internet para que se produzca un desarrollo definitivo del comercio electrónico, está fundamentada en problemas de índole jurídico-civil relacionados con el pago de las transacciones y la entrega de productos.

La realización de un contrato comercial requiere llevar a cabo varias etapas:

- Oferta y Publicidad.
- Compra del producto.
- Medios de pago.

- Distribución física del producto.
- Reclamo.

La primera etapa, publicidad y oferta, no plantea problemas en el comercio tradicional y en el ámbito del comercio electrónico tampoco, ya que Internet supone el mayor y más amplio espacio en el que los comerciantes pueden realizar sus ofertas.

Sin embargo, la segunda y la tercera etapa sí suponen un cúmulo de problemas para el comercio electrónico ya que dificultan la aplicación del derecho comercial tradicional a esta nueva modalidad de comercio.

El comercio electrónico se caracteriza por el desconocimiento de la localización de las partes, es decir, no se sabe dónde están situados las partes contratantes, cuál es el domicilio del cliente y del proveedor; y por su carácter mundial, son muchos los implicados, por lo que los principios o criterios implicados se incrementan.

A través de Internet se pueden realizar compras en cualquier parte del mundo. En este caso, ¿cuál legislación comercial se aplicará, la del país del consumidor o la del país del vendedor? En el comercio tradicional estos asuntos están regulados por las leyes y códigos existentes. En el caso del comercio electrónico, será posible aplicar estas regulaciones?

Para Vásquez (2002), el comercio electrónico precisa un marco esencial desde una doble perspectiva:

> "a) La seguridad del medio elegido, en este caso la de las comunicaciones para conocer el alcance del consentimiento prestado.
> b) La seguridad del contenido contractual." (Vásquez, 2002, p. 135).

Los problemas que se plantean desde el punto de vista legal vinculados a la relación contractual según Menéndez (2005) son:

a) Identificación de los contratantes.
b) La validez de la contratación por Internet en el ordenamiento jurídico vigente.

c) Lugar y tiempo de perfección de los contratos electrónicos.
d) Jurisdicción y legislación aplicable para resolver los conflictos derivados de la contratación vía Internet.

Por otro lado, se trabajará el concepto de comercio electrónico vinculados a la relación con los consumidores, debido a que en el ámbito de los consumidores, este tipo de comercio ha tenido poca penetración, y por esta misma razón este es el ámbito donde reside la importancia del comercio electrónico debido a su potencial de desarrollo, como lo indica Pinochet (2001):

> "el poco grado de penetración que ha tenido el comercio electrónico en el sector de consumidores, es en el ámbito de consumo, precisamente, en donde reside la importancia que es posible prever para el comercio electrónico en el futuro" (Pinochet, 2001, p.105).

De acuerdo con este mismo autor, el concepto de comercio electrónico se vincularía más a la relación comerciante o profesional con consumidor que a las transacciones que realizan los comerciantes o profesionales entre sí. Otros autores como Rivas (1998) y Escobar (2000) también indican que este tipo de comercio electrónico, con los consumidores, es al que normalmente se hace referencia cuando se alude al comercio electrónico.

Entre empresas ya existía desde años atrás la contratación electrónica con altos niveles de seguridad en redes cerradas como el EDI (Electronic Data Interchange).

Desde el punto de vista de los consumidores, es necesario analizar los problemas relacionados con:

a) Efectiva tutela de los consumidores y usuarios.
b) Privacidad y Protección de los datos de carácter personal.
c) Seguridad en las transacciones.

En las siguientes secciones se establece el marco teórico de la problemática jurídica planteada, alrededor del cual este trabajo de investigación realizará el análisis correspondiente. En resumen, se analizará la problemática jurídica de los siguientes aspectos del comercio electrónico: la contratación vía Internet, derechos del

consumidor, privacidad y protección de los datos personales y seguridad de las transacciones.

2.3.2 La contratación vía Internet

2.3.2.1 El concepto

El comercio electrónico supone una relación contractual que puede ser establecida desde diferentes técnicas de comunicación: página Web, chat o videoconferencia, correo electrónico y subasta electrónica. Los contratos más numerosos perfeccionados por medio de una página Web son los de compra y venta de un bien o servicio. El trabajo analizará este tipo de relación.

En los siguientes párrafos se describe el procedimiento que se sigue para llegar a concretar un compraventa a través de Internet.

La página Web presenta un catálogo de los distintos productos que pueden ser adquiridos con indicación de sus precios y características. Una vez escogido el objeto de interés, el usuario deberá pulsar un ícono que diga “comprar” o “añadir” junto al dibujo de un coche de compra. Esta operación conducirá a otra pantalla en la que mostrará los productos seleccionados hasta el momento y el precio individual de cada uno de ellos, así como el total de la selección; permitirá indicar la cantidad de unidades que se deseen de cada producto escogido; y decidir entre continuar escogiendo otros productos, que serán incluidos en la cesta, o celebrar el contrato.
La última opción resulta en la obligación del usuario de inscribirse en el registro de la propia página Web. Los datos que generalmente se exigen son: nombre, dirección, localidad, provincia, código postal y dirección de correo electrónico, así como una contraseña que será necesaria para llevar a cabo el pedido. Después de registrarse se pasará a otra pantalla en la que, para continuar con el proceso de compra, solicitará la introducción de la dirección de correo electrónico del usuario y de la contraseña previamente asignada.

Finalmente se llega a la “hoja de pedido”, “formulario de pedido” u “orden de compra” que generalmente presenta el siguiente contenido: datos del comprador, los productos, precio individual de cada uno de ellos, la cantidad correspondiente a los gastos de envío y el total a pagar. Hace referencia a la forma de pago, el comprador escogerá una de las opciones (correo o transporte contra reembolso, tarjeta de crédito, giro postal, transferencia bancaria) o simplemente indicará una modalidad de pago, normalmente mediante tarjeta de crédito. Algunas incorporan las condiciones generales de contratación.

Después de completar todos los datos y leer las condiciones generales, el usuario deberá pulsar el ícono “enviar”, “enviar pedido”, “pagar” u otro similar. Si todo está correcto se le abre una pantalla agradeciendo al usuario la compra y se le comunica el número de pedido, precio total, así como otros datos. Normalmente se le aconseja que imprima estos datos de compra y los guarde hasta recibir el pedido. Después de este proceso, al menos en dos ocasiones, el vendedor se pone en contacto por correo electrónico con el usuario. La primera vez para agradecerle haberse inscrito en su registro, y la segunda para agradecerle la compra concluida y enviarle los datos correspondiente a ésta. Puede verse aquí la interrelación entre la página Web y el correo electrónico a los efectos de perfeccionar y ejecutar un contrato.

Se define el concepto de contrato a través de Internet como:

> “aquel contrato para cuya conclusión se ha empleado este medio moderno de comunicación, sin importar la calificación de los sujetos que lo hayan empleado (profesionales, particulares o un profesional y un consumidor), ni la normativa aplicable a cada uno de ellos.” (Menéndez, 2005, p.172).

Estos tipos de contratos se basan en el documento electrónico, definido por Téllez (2004) como:

> “un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que sometidos a un adecuado proceso, permiten su traducción a lenguaje natural a través de una pantalla o una impresora.” (Téllez, 2004, p.247).

2.3.2.2 La validez de la contratación vía Internet

Menéndez (2005) indica que la admisión de este tipo de contratos a la luz del ordenamiento jurídico vigente debe analizarse desde dos aspectos:

a) La validez del empleo de Internet en la contratación actual, y la existencia y eficacia teórica del contrato concluido a través de ella.
b) La prueba de la existencia de dicho contrato.

Téllez (2004) menciona que los documentos electrónicos deben tener las siguientes características para que sean eficaces, y seguros: inalterabilidad, autenticidad, durabilidad y seguridad.

El principal obstáculo para la admisibilidad y eficacia probatoria de los nuevos soportes de información se plantea con relación al carácter de permanencia que es esencial en la definición de "documento". Para Téllez (2004), documento es:

> "Todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica". (Téllez, 2004, p. 243).

El temor sobre la posibilidad de reinscripción o reutilización de los soportes informáticos disminuye su seguridad y confiabilidad.

Un documento es auténtico cuando

> "no ha sufrido alteraciones que varíen su contenido, lo que implica decir que la autenticidad está íntimamente vinculada a la inalterabilidad. Un documento será más seguro cuando más difícil sea alterarlo y sea más fácil de verificarse la alteración que podría haberse producido o reconstruir el texto originario". (Téllez, 2004, p.248).

Durable sería

> "toda reproducción indeleble del original que importe una modificación irreversible del soporte. Se entiende por modificación irreversible del soporte la imposibilidad de reinscripción del mismo; por indeleble la inscripción o imagen estable en el tiempo y que no puede ser alterada por una intervención externa sin dejar huella." (Téllez, 2004, p.248).

Con respecto a la seguridad, se cuestiona la autenticidad de la representación.

> "Con el desarrollo de claves de cifrado y otras medidas criptográfica, el documento electrónico es al menos equivalente al instrumento escrito y firmado sobre soporte de papel en cuanto a seguridad." (Téllez, 2004, 248).

Los documentos electrónicos poseen los mismos elementos que un documento escrito en soporte de papel: constan en un soporte material (cintas, disquetes, circuitos, chips de memoria, redes) sobre el cual se grava el documento electrónico; contienen un mensaje que está escrito con el lenguaje convencional de los dígitos binarios o bits, entidades magnéticas que los sentidos humanos no pueden percibir; están escritos en un idioma o código determinado; pueden ser atribuidos a una persona determinada en calidad de autor mediante firma digital, clave o llave electrónica.

Desde la perspectiva internacional, el artículo 11 de la Ley Modelo sobre comercio de la CNUDMI (1996) reconoce la validez de los contratos perfeccionados mediante los mensajes de datos.

La contratación por vía Internet resulta perfectamente válida, y la utilización de este medio de comunicación está permitida siempre y cuando las partes no hayan prohibido expresamente su uso.

2.3.2.3 Identificación de las partes

En una relación de compra y venta por Internet, se identifica dos partes y que se caracteriza de que entre éstas no existe un contacto físico previo. Por un lado se encuentra el proveedor o prestador de servicios definido como

> "cualquier persona física o jurídica que manifiesta a través de la red, y desde su propia página Web, un conjunto de ofertas contractuales, ya sean de productos o servicios, cumpliendo todos los requisitos para poder ser calificadas como tales y no de simple publicidad." (Menéndez, 2005, p.249).

Por el otro lado se encuentra el usuario o consumidor que es cualquier persona física o jurídica que utilice la página Web del proveedor para comprar bienes o servicios, o simplemente para obtener información de las ofertas publicadas en la página.

La identificación de ambas partes es fundamental para dar por terminado el contrato o para conocer la condición de consumidor, profesional, empresa o particular que les corresponda en la relación, principalmente por la posibilidad que brinda el sistema para cometer estafas, fraudes y abusos encubiertos, o para exigir reclamos posteriores por parte de los usuarios o consumidores.

2.3.2.4 Tiempo y lugar de perfección del contrato

El uso de instrumentos de comunicación entre partes físicamente distantes, hace necesario determinar en qué instante exacto se entiende perfeccionado el contrato, y cuál es el lugar en el que se considera concluido el contrato. La importancia de la determinación de estos dos aspectos se debe a las siguientes razones indicadas por Menéndez (2005):

- Conocer el momento que entra en vigor el contrato que une las partes para exigir las obligaciones instituidas por él.
- Ineficacia de los intentos extemporáneos de revocación y retirada de la oferta o retirada de la aceptación por parte de los autores.
- Ineficacia de determinadas causas de extinción de las declaraciones contractuales (ejemplo: incapacidad sobrevenida o muerte del autor de la declaración, caducidad, etc.)
- Transmisión de los riesgos de la cosa al adquirente, en aquellos casos en que el contrato que se perfeccione conlleve la transmisión de la propiedad u otro derecho real.
- Determinación exacta de la ley o norma aplicable en el tiempo a la relación contractual creada; es decir, los problemas típicos asociados a la aplicación temporal de las normas jurídicas.
- Momento determinante del inicio del cómputo de determinados plazos para el correcto ejercicio de algunos derechos o acciones.

Asimismo, resulta fundamental localizar el lugar exacto en que se entiende concluido el contrato, pues con ello se determina:

- La ley o norma aplicable especialmente a la relación contractual originada, así como los usos interpretativos relevantes para subsanar las ambigüedades de los contratos.
- El fuero jurisdiccional competente para la resolución de futuras controversias derivadas de la ejecución del contrato perfeccionado.

De acuerdo con Pinochet (2001), los requisitos básicos de la oferta son:

- Propósito del oferente de vincularse contractualmente con carácter definitivo.
- La oferta debe ser completa, es decir, debe contener todos los elementos esenciales del futuro contrato, de modo que con la simple aceptación del comprador el contrato sea perfecto.
- La oferta debe exteriorizarse. La exteriorización de la voluntad puede ser efectuada de forma expresa, tácita e incluso presunta, pero lo importante es que sea concluyente, en el sentido inequívoco.

La aceptación por su parte debe tener los siguientes requisitos de acuerdo con Pinochet (2001):

- Que se exteriorice. La exteriorización puede ser de cualquier manera, por el principio de libertad de forma, pero en lo que se refiere al comercio electrónico, debe producirse electrónicamente.
- Que sea pura y simple.

Entonces, la aceptación perfecciona el contrato. Para Pinochet (2001), una contratación vía Internet, el perfeccionamiento del contrato será en el momento en que el comprador pulse el botón “aceptar”, puesto que en segundos la aceptación habrá llegado a conocimiento del oferente o a su ordenador.

2.3.2.5 Jurisdicción y legislación aplicable

En una relación comercial a través de Internet, es posible que las partes se encuentren en diferentes países. También puede ocurrir que el sitio virtual se encuentre alojado en un servidor localizado en un país distinto del proveedor físico y es posible todas las

combinaciones de localización del proveedor, sitio Web y consumidor. Surge, por lo tanto, incertidumbre no sólo respecto al lugar en que se realizan las actividades comerciales, sino que las propias actividades pueden tener consecuencias previstas o imprevistas en todo el mundo, lo que provoca incertidumbre cuando hay que localizar la controversia, determinar el derecho aplicable y los aspectos prácticos de seguir adelante con el cumplimiento o buscar alternativas adecuadas de solución de controversias.

Relacionado a esto, Vásquez (2002) indica lo siguiente:

a) "En la contratación electrónica si no hay una previa aceptación de foro, resulta prácticamente imposible llevar a cabo una conexión mínima con algún tipo de norma que haga asumible una jurisdicción adecuada y ponderada.
b) Las partes pueden escoger libremente la ley aplicable a un contrato transnacional, los más frecuentes en la Web." (Vásquez, 2002, p. 140).

En el ámbito internacional, las cuestiones relativas a la jurisdicción, el Derecho aplicable, reconocimiento y cumplimiento de decisiones judiciales extranjeras se han resuelto remitiéndose al Derecho Internacional Privado. En principio, cada país determina sus propias normas de Derecho Internacional Privado; aunque en ciertas regiones del mundo, algunas de esas reglas se han uniformado mediante tratados, el panorama general aún es complejo.

2.3.3 Derecho de los consumidores

También el derecho de los consumidores requiere un examen profundo para indagar si las leyes actuales podrán prevenir fraudes o incumplimiento de contratos celebrados por medio del computador. Es necesaria la protección al consumidor en cuanto a devolución de bienes y servicios por no cumplir con las expectativas acordadas.

La Constitución Política de Costa Rica, consagra en su artículo 46, el derecho de los consumidores y usuarios "a la protección de su salud, ambiente, seguridad e intereses económicos, a recibir información adecuada y veraz; a la libertad de elección, a un trato equitativo. El Estado apoyará los organismos que ellos constituyan para la defensa de sus derechos. La ley regulará esas materias" (Rivera, 2003, p.21).

De acuerdo con Salas y Barrantes (1997), la protección del consumidor tiene tutela constitucional, no es irrestricto pero limita horizontalmente la libertad contractual y el mismo tiene sentido toda vez que sin consumidores el mercado no existe y por ende, la libertad de competencia.

Esto resulta importante porque sin seguridad y protección, el comercio electrónico no será atractivo para los consumidores. Y es en este ámbito donde las empresas se preparan para ofrecer sus productos y servicios a la gran masa consumidora a través de los medios electrónicos que la tecnología hoy pone al alcance de los empresarios, es decir, comerciar electrónicamente, actividad que, debido a su grado de complejidad técnica y a una cierta desconfianza por parte de la gran masa consumidora ha tenido una penetración algo lenta, en relación a los volúmenes que se producen en el comercio tradicional.

Por otro lado, la gran cantidad de publicidad "en línea" plantea la necesidad de implementar métodos para el control de la publicidad engañosa, fraudulenta o no deseada, ofrecida a través de Internet.

También, la mayoría de las ventas por Internet solicitan información de los consumidores, es necesario entonces la protección de estos datos contra la utilización indebida por parte de la empresa o terceros que puedan acceder a ellos.

Indica Rivero (1997), que la libertad de competencia conduce al establecimiento de prácticas de competencia desleal, así como a la invención de prácticas de desleales de mercadeo; el principio de igualdad de derechos y deberes se transforma en una ilusión y el de responsabilidad por culpa se convierte en la principal causa de exoneración de la responsabilidad de los productores, dado que la prueba de la culpabilidad supone un conocimiento adecuado del proceso de producción a fin de demostrar, cuál fue el deber de cuidado que se violó, y a quién resulta imputable la violación de ese deber.

Según Salas y Barrantes (1997), el derecho de protección al consumidor se entiende, en consecuencia, como una reacción ante el déficit de las codificaciones tradicionales,

donde la falta de experiencia, de conocimiento y de organización del consumidor, así como la necesidad de racionalizar las decisiones de consumo, son algunas de las principales situaciones que mueven al legislador a actuar en este campo.

Pinochet (2001) menciona los aspectos que más preocupa a los consumidores, mencionados en la Resolución del Consejo de 19 de enero de 1999 sobre la Dimensión Relativa a los Consumidores en la Sociedad de la Información (norma fundante del estatuto jurídico de protección al consumidor europeo en el ámbito de las nuevas tecnologías):

> "a) La accesibilidad y la asequibilidad a las nuevas tecnologías.
> b) La facilidad de uso de equipos y aplicaciones y las competencias necesarias para utilizarlos.
> c) La transparencia, la cantidad y la calidad de la información.
> d) La equidad de las prácticas comerciales, las ofertas y las condiciones contractuales.
> e) La protección de los niños frente al contenido inadecuado.
> f) La seguridad de los sistemas de pago, incluida la firma electrónica.
> g) El régimen jurídico aplicable a las transacciones que los consumidores efectúen en el nuevo entorno con respecto tanto a la elección del régimen jurídico como a la viabilidad de las disposiciones existentes.
> h) La atribución de responsabilidades.
> i) La intimidad y la protección de los datos personales.
> j) El acceso a unos sistemas eficaces de recurso resolución de litigios.
> k) La tecnología de la información como instrumento informático y educativo." (Pinochet, 2001, p. 108).

En esa misma Resolución, mencionada por Pinochet (2001) se propone las siguientes medidas o acciones en beneficio del consumidor:

> "a) El logro de la transparencia y el derecho a recibir, antes de la transacción y en su caso después de ella, información suficiente y fiable que contenga, en particular la identidad comprobada del proveedor y la información necesaria para probar la autenticidad de cada uno de los elementos de una transacción.
> b) La no discriminación en el acceso a productos y servicios, con atención a las necesidades de los consumidores vulnerables.
> c) La protección de los consumidores frente a las prácticas de comercialización no solicitadas, engañosas y desleales, incluida la publicidad, y el apoyo a que se pongan a disposición del consumidor medios fiables para filtrar el contenido de los sistemas de comunicación.
> d) La protección de los intereses económicos de los consumidores, con una distribución equitativa de riesgos y responsabilidades que refleje en especial la responsabilidad del proveedor al optar por medios electrónicos de comercio y con inclusión, en particular, de las condiciones necesarias para que el consumidor pueda tomar decisiones ponderadas.

e) La protección de la salud, seguridad e intimidad de los consumidores, incluida la protección contra la utilización abusiva de datos personales.
f) La información y educación del consumidor, a fin de posibilitar la adquisición de las competencias adecuadas.
g) La consulta de los consumidores a la hora de desarrollar nuevas políticas o mecanismos reglamentarios.
h) La representación de bs intereses de los consumidores en los órganos de control y vigilancia pertinentes." (Pinochet, 2001, p.110).

La presente investigación tomará como base, para el análisis de los derechos de los consumidores, estos aspectos mencionados por Pinochet (2001).

2.3.4 Privacidad y Protección de datos

2.3.4.1 El concepto

Se reconoce las beneficiosas posibilidades que brinda la Internet y el comercio electrónico para mejorar la calidad de vida de las personas, al mismo tiempo se advierte la necesidad de crear mecanismos de protección de derechos fundamentales del individuo, que podrían resultar perjudicados por el uso de las nuevas tecnologías.

Los derechos fundamentales que pueden estar en riesgo a raíz del comercio electrónico son, de acuerdo con Balarini (2003):

> "…los derechos de la libertad de información como garantía, el derecho al honor, el derecho a la intimidad, el derecho a la propia imagen, el derecho a la reputación, los comúnmente llamados derechos de la personalidad, el derecho a la correspondencia, y también, en cuanto tienen reconocimiento en nuestra Constitución como la Declaración Universal, los derechos morales del autor o inventor." (Balarini, 2003, p. 99).

Uno de los nuevos problemas que surge con el comercio electrónico se encuentra constituido por la gran cantidad de información que puede almacenarse de una persona y por el tratamiento que puede darse a ésta, gracias a los archivos digitales de datos y a los programas informáticos desarrollados para tales efectos.

Hoy en día es posible consultar múltiple información sobre una persona a una velocidad altísima, y además es factible cruzar la información que sobre ella existe en diferentes registros, pudiendo crear perfiles completos sobre ingresos, consumo, preferencias,

etc., lográndose resultados que superan largamente los objetivos previstos por las diferentes leyes que han dispuesto la creación de los mencionados archivos o registros.

Por tanto, y recogiendo el análisis que hace Del Peso y Ramos (1994), se define el derecho a la intimidad al derecho a que los demás no conozcan nuestros datos personales, y que estos datos personales esté protegida con una serie de garantías jurídicas frente a la intromisión de los demás. Para la presente investigación, se considera lo mismo el término de derecho a la intimidad con el término de derecho a la privacidad, aunque para algunos autores sean diferentes. Esto es, la privacidad abarca una esfera más amplia de las facetas de la personalidad del individuo que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. En tanto que la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, el domicilio, las comunicaciones en las que se expresa sus sentimientos, por ejemplo.

2.3.4.2 El problema de la tutela del derecho a la intimidad

El desarrollo tecnológico ha complicado el problema de la tutela del derecho a la intimidad. Por un lado, las sociedades modernas deben proteger este derecho pero al mismo tiempo deben crear condiciones para mejorar la comunicación de los ciudadanos, así como su autodeterminación.

De acuerdo con Chirino y Carvajal (2003), el derecho a la intimidad debe ser considerada en una nueva dimensión, el de la tutela de las posibilidades de participación reales del ciudadano en una sociedad que se informatiza. Esta nueva dimensión de la intimidad debe considerar la autodeterminación y las facultades de control que un ciudadano debe tener sobre el flujo de informaciones que circulan sobre sí mismo.

Para Del Peso (1994), esa intimidad se puede preservar mediante la autodeterminación informativa, que es el derecho que tienen las personas a decidir por sí mismas cuándo y

dentro de qué límites procede revelar secretos referentes a su propia vida. Este derecho, no solo se vincula con la intimidad, sino también con derechos constitucionales como: la dignidad humana, la libertad individual, la autodeterminación y el principio democrático.

Surge también la preocupación por determinar si las bases de datos pueden ser transferidas con propósitos comerciales, y si no existe un deber de custodiarlas a cargo de quienes las confeccionan.

Las aplicaciones que se le pueden dar a estos datos pueden ser para una gran variedad de fines: publicitarios, comerciales, fiscales, policíacos, etc., convirtiéndose de esta manera en un instrumento de opresión y mercantilismo. La variedad de los supuestos posibles de indefensión frente al problema provoca que los individuos estén a merced de un sinnúmero de situaciones que alteren sus derechos fundamentales en sociedad provocados por discriminaciones, manipulaciones, persecuciones, presiones y asedios; todo ello al margen de un control jurídico adecuado.

Para Balarini (2003), los proveedores de acceso son responsables de la confidencialidad de los datos que les son transmitidos por los abonados; los editores, del contenido de lo que editen, y los usuarios no deben violar la ley.

En el ambiente de comercio electrónico donde la plataforma básica es la Internet, los datos de los usuarios se transmiten a través de la red, y muy posible traspasando fronteras entre países. Surge aquí también el problema del derecho aplicable. Sarra (2000) indica que tanto para las empresas transnacionales como para las nacionales, las legislaciones deben contener especificaciones para que en países donde existen normativas menos elaboradas o en donde, directamente, no haya previsiones legales al respecto, esta condición no genere vulneraciones no deseadas a los derechos de las personas.

En el tema de la protección de la información personal se reconoce la existencia de una serie de principios generales, garantías y excepciones, que están condicionados por el

principio de equilibrio o balance. Los principios generales subyacen a toda la problemática y son esenciales para garantizar, en forma directa, la adecuada protección de la información personal (y, en algunos casos, los intereses legítimos de personas jurídicas), e indirectamente, para salvaguardar los derechos de la privacidad, al honor, a la reputación, a la libertad de expresión (incluyendo la libertad de prensa), etc., mediante la generación de un adecuado marco jurídico en donde puedan hacerse efectivos todos y cada uno de estos derechos y garantías fundamentales del hombre.

2.3.4.3 Principios generales, garantías y excepciones

De acuerdo con Sarra (2001), los principios generales responden a la siguiente enunciación y fundamentación:

> "a) Legitimidad y buena fe. Es fundamental que toda información relativa a las personas sea procesada en forma legítima y no pueda ser utilizada con fines contrarios a la buena fe." (Sarra, 2000, p. 197)."
>
> "b) Especificación de la finalidad, racionalidad y duración. Bajo este concepto hemos incorporado la noción de que el tratamiento de la información debe realizarse con fines determinados, los cuales además de ser explícitos y legítimos, deben poder asegurar que la utilización o divulgación posterior no sea incompatible con los fines originarios especificados y, si lo fueren, debe mediar consentimiento del interesado que así lo autorice. Así mismo, la racionalidad de su utilización implica que los datos deben ser utilizados sólo cuando lo justifique la finalidad para los cuales fueron recolectados y no en otras circunstancias que, aunque igualmente legítimas, no fueran razonables para esos fines…..la información no podrá ser conservada por un período de tiempo que exceda el razonablemente necesario para la consecución de los fines para los cuales fue recolectada." (Sarra, 2000, p.198).
>
> "c) Pertinencia y exactitud….La información referida a las personas que esté sometida a procesamiento debe ser adecuada, pertinente y no excesiva con relación al ámbito y los fines." (Sarra, 2000, p. 199).
>
> "d) No discriminación….El objetivo de este principio es evitar que el tratamiento de los datos relativos a las personas pueda converger en actos ilegítimos o discriminatorios…..Con miras a la consecución de este objetivo se ha establecido, como pauta genérica, la prohibición de compilar datos sensibles, es decir, aquellos que incluyan información sobre el origen racial o étnico, vida sexual, opiniones políticas, religiosas, filosóficas o cualquier otra creencia y la pertenencia a asociaciones, sindicatos, etc.; en suma, cualquier tipo de información que pudiera ser utilizada para la comisión de actos discriminatorios sobre las personas." (Sarra, 2000, p. 200).
>
> "e) Confidencialidad y seguridad de la información….Es fundamental que pueda garantizarse al interesado que la información que le concierne sólo será tratada por las personas autorizadas….Asimismo, debe garantizarse que la información estará debidamente protegida, para lo cual deberán adoptarse las medidas técnicas de seguridad y de organización necesarias para garantizar un adecuado resguardo de los datos. Es decir que la información debe estar debidamente protegida contra destrucción, pérdida, alteración o difusión (accidentales o ilícitas), accesos no autorizados (remotos o no), utilización fraudulenta de los datos, contaminación por virus de computadora, etc." (Sarra, 2000, p. 201).

Las garantías son la condición de operatividad de los principios. Sarra (2000) y Téllez (2004) mencionan los siguientes:

> a) "Derecho de acceso: es aquel que permite a los interesados conocer las instituciones y el tipo de información que dispongan sobre su persona, (quien, cómo, cuándo, para qué). (Téllez, 2004, p. 62).
> b) "Derecho de rectificación: complementario al anterior, dicho derecho permite solicitar al interesado una modificación en los términos de alteración o ampliación, o una supresión o cancelación de aquellos datos que, referidos a su persona, considere como inexactos o irrelevantes o que requieran actualizarse." (Téllez, 2004, 62).
> c) "Derecho de oposición. El interesado tiene derecho a oponerse -en cualquier momento y siempre que poseyera un interés legítimo basado en su situación particular- al tratamiento de datos en los dos supuestos que se mencionan a continuación: 1) ….Cuando la oposición del interesado está basada en una causa justificada, el tratamiento que efectúe el responsable ya no podrá referirse a esos datos. 2) ….cuando el responsable fuera a utilizarlos con fines de prospección." (Sarra, 2000, p. 204).
> d) "Derecho al consentimiento y a fijar el nivel de protección. En todo procesamiento de datos se requiere que el interesado preste su consentimiento al respecto en forma inequívoca, salvo cuando exista una disposición en contrario…Mediante el derecho de autodeterminación se otorga a la persona la posibilidad de determinar el nivel de protección que desea que se otorgue a los datos que le conciernen." (Sarra, 2000, p. 205).
> e) "Derecho de uso conforme al fin: consiste en que el interesado pueda exigir que su información nominativa sea destinada para los objetivos específicos por los cuales se proveyó." (Téllez, 2004, p.62).
> f) "Derecho para la prohibición de interconexión de archivos: Que las distintas bases de datos, no puedan consultarse y/o vincularse indistintamente." (Téllez, 2004, p. 62)
> g) "Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente. Por medio de este derecho pretende asegurarse al interesado que no será sometido a una decisión que pudiera tener efectos jurídicos significativos sobre él, cuando ésta hubiere sido adoptada sobre la única base de un tratamiento automatizado de datos y fuera destinada a evaluar determinados aspectos de su personalidad, conducta, fiabilidad, rendimiento laboral, etc. Con este objetivo, se otorga al interesado la posibilidad de impugnar los actos administrativos o cualquier decisión privada que implique una valoración de su comportamiento en las circunstancias aludidas." (Sarra, 2000, p. 206).

En relación a las excepciones a dichos derechos fundamentales en el equilibrio del Estado y su poder coercitivo y los integrantes de la sociedad, se tienen a aquellas derivadas con motivo de la seguridad del Estado tanto en lo interno como en lo externo, así como las relativas a intereses monetarios, persecución de delitos, motivos de salud, protección del propio interesado o de los derechos y libertades de terceros, entre otros.

La presente investigación tomará como base para la discusión del tema de la privacidad los principios generales, garantías y excepciones mencionadas en este apartado.

2.3.4.4 Protección de datos: sistema norteamericano, europeo y latinoamericano

Encontramos en Chirino y Carvajal (2003), un resumen de estos tres sistemas de protección de datos que a continuación se expone.

Indica Chirino y Carvajal (2003) que la Unión Europea ha avanzado hasta poner en vigencia una reglamentación sobre protección de datos. Esta reglamentación tiene por objetivo proteger a las personas objeto de tratamiento de datos por parte de órganos e instituciones de la Unión Europea. También se anunció el día 7 de diciembre de 2000 en Niza, la Carta de Derechos Fundamentales de la Unión Europea, que incluye un artículo 8, el cual regula detalladamente aspectos relacionados con la protección de datos:

> "Toda persona tiene derecho a la tutela de sus datos personales.
> Estos datos solo deben ser procesados de buena fe para el fin preestablecido con el consentimiento de la persona afectada o para cumplir con los fines establecidos con un adecuado fundamento legal. Toda persona tiene el derecho a recibir información sobre los datos referidos a su persona que hayan sido recogidos y a lograr su rectificación.
> El cumplimiento de estas reglas será vigilada por un centro independiente". (Chirino y Carvajal, 2003, p. 213).

El sistema norteamericano de protección de datos es completamente opuesto al modelo europeo. Los norteamericanos no han dictado leyes específicas en la materia, sino que han preferido un sistema de autorregulación, especialmente desde el punto de vista del consumidor, indicando que los proveedores deben divulgar sus políticas de privacidad con el fin de que los consumidores puedan escoger el que ofrezca un mejor nivel de tutela.

La posición de autorregulación de Estados Unidos ha representado un gran problema para establecer acuerdos de libre comercio con la Unión Europea. Los europeos necesitan algo más que la promesa de la autorregulación.

Por otro lado, Latinoamérica ha recurrido al hábeas data como forma de tutela de los ciudadanos frente al tratamiento de sus datos personales.

> "...el hábeas data pretende hacer referencia a la posibilidad jurídica de proteger el derecho de los ciudadano a acceder a las informaciones personales que se encuentren disponibles en registros magnéticos y manuales con el fin de ser revisados, y si representan para la persona un perjuicio, también el de ser corregidos o eliminados". (Chirino y Carvajal, 2003, p.230)
>
> "...es una garantía para acudir a una determinada vía y ahí solicitar los datos o las informaciones que se entiende son lesivas a los derechos protegidos, y como pretensión solicitar la anulación, borrado, obstrucción o corrección de los datos que afectan a la persona". (Chirino y Carvajal, 2003, p.230)

De acuerdo con estos autores, se trata de un derecho reactivo y no de uno preventivo. Funciona cuando ya ha sucedido un daño, que puede ser, en algunos casos de incalculables proporciones, por la afectación que puede recibir una persona al producirse interconexiones automáticas de los bancos de datos.

2.3.5 Seguridad de la información

2.3.5.1 Introducción

Cada día las entidades basan en mayor medida su gestión en una información exacta, completa y obtenida a tiempo, por lo que es creciente la importancia de su seguridad y de su confidencialidad.

El concepto de seguridad aplicada a la información se asocia con la disponibilidad, la seguridad física, la integridad y la confidencialidad.

Los aspectos de seguridad física y disponibilidad están relacionados a vulneraciones al medio utilizado para almacenar la información o al lugar en donde se encuentra. Por ejemplo, se debe asegurar la información contra incendios o inundaciones, evitar la apropiación indebida de soportes magnéticos, que se pueda seguir trabajando cuando no hay energía eléctrica o si falla el equipo o línea de comunicación; para esto deben existir alternativas.

La integridad de la información se pierde cuando se producen variaciones no autorizadas, que pueden consistir en información añadida, borrada o modificada. Para Del Peso (1994), la integridad se cumple si éstos son exactos, completos y fiables.

La confidencialidad se cumple si los datos son sólo conocidos por las personas autorizadas. Esto es un concepto relacionado con la privacidad, como derecho de las personas a determinar qué datos suyos pueden ser conocidos, por parte de quiénes y durante cuánto tiempo.

La confidencialidad puede verse afectada, según Del Peso (1994), por falta de políticas generales y de una clasificación de la información (qué es de uso restringido, departamental, confidencial); ausencia de procedimientos que ayuden a cumplir las políticas; controles de acceso (físico y lógico) inadecuados, que permitan accesos no autorizados a ficheros o a datos transmitidos.

Los entornos de procesamiento de la información son cada vez más sofisticados, a la vez que más distribuidos gracias a los avances en comunicaciones y redes, resultando a veces difícil poder garantizar razonablemente la seguridad de la información, y de forma especial su confidencialidad.

2.3.5.2 La problemática de la privacidad y seguridad del comercio electrónico desde la perspectiva penal

El problema de la privacidad o protección de la información personal está estrechamente relacionado con el tema de la seguridad en las redes y la promoción de la actividad en ellas. A escala internacional se realiza el abordaje de la temática debido a los innumerables inconvenientes surgidos con relación a la inseguridad jurídica de las redes abiertas.

Por otro lado, la Internet ha potenciado la capacidad de generar y acumular una gran cantidad de información obtenida de las transacciones que se realizan en ella. Siempre que se accede a Internet se deja una señal de ello, que conforme aumente el número de actividades que se realicen a través de la red, irá configurándose el perfil de las preferencias de sus usuarios, gustos, ocupaciones, etc.

> "... existen software especialmente diseñado para recopilar en Internet la mayor cantidad de datos posibles respecto de una persona especificada, tales como, lugar de trabajo, preferencias con respecto a bebidas, comidas o vestimenta, opiniones acerca de temas de actualidad, política o cultura, escuela donde se graduó, si padece adicción a las drogas o al alcohol, …" (Sarra, 2000, p.193)

Lo que es grave es que esta información puede ser comercializada en Internet, surgiendo entonces el tema de la responsabilidad derivada de la violación de secretos o a la privacidad. Se debe poder asegurar a los usuarios de Internet que su información será usada para:

> "…fines legítimos, que la cantidad de información requerida sea sólo la necesaria en relación a los propósitos, que sólo se mantenga por el límite de tiempo adecuado, que sea utilizada exclusivamente para los fines determinados, etc." (Sarra, 2000, p.194).

Muy relacionado con esto, se tiene que la transmisión de información por medio de la Internet hace vulnerable la información en tránsito. Es necesario establecer responsabilidades por el acceso no autorizado a esta información, así como buscar mecanismos tecnológicos para asegurar la información que viaja por la red.

De acuerdo con Mata (2001), los avances de la informática sitúan al Derecho Penal ante problemas nuevos, o ante problemas que debe abordar con una nueva visión de los mismos.

Las enormes potencialidades que se abren para el tratamiento automatizado de datos, tienen un reverso que son los riesgos que se introducen para facilitar la realización de hechos que afecten a los intereses fundamentales de las personas. Es decir, la informática, o en general, el tratamiento automatizado de datos se presenta como factor criminógeno, pues permite el acceso y el manejo de bases de datos, programas de cualquier género, en ocasiones en forma lesiva para intereses básicos de las personas y de la sociedad.

La preocupación fundamental de las instituciones, en la actualidad, según Sarra (2000), es brindar la mayor seguridad a sus sistemas automatizados de información. La tecnología ha permitido mayor agilidad y dinamismo en las actividades y procesos que realizan, pero se ha expuesto a los riesgos de violación a sus sistemas de información.

Los principales perjuicios sufridos suelen ser violación de los secretos comerciales, la destrucción de información y de los sistemas de información y el robo de información crítica en general.

Los ataques pueden venir de personas externas (hackers o crackers), pero también puede provenir de personas relacionadas a la institución (empleados o proveedores).

Por otro lado, también resulta extremadamente difícil poder probar la comisión del hecho ilícito en este ambiente electrónico.

Los actos de violación a los sistemas de información, directamente traen como consecuencia el acceso y usos no autorizados de la información, y en lo que nos interesa, de la información relativa a las personas o datos personales.

La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

El estudio de los distintos métodos de destrucción o violación del *hardware* y el *software* es necesario para determinar la dirección que debe seguir la protección jurídica de los sistemas informáticos, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos. De este modo se pueden conocer los problemas que es necesario resolver para conseguir una protección jurídica eficaz.

En consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, con base a las peculiaridades del objeto de protección, sea imprescindible.

Surge entonces nuevas posibilidades de delitos, los llamados delitos informáticos, que se han desarrollado gracias a la evolución de la Informática y las redes de comunicación. Se puede identificar los siguientes como aquellos cuya comisión ha sido facilitada por el comercio electrónico:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
b) Lectura, sustracción o copiado de información confidencial.
c) Modificación de datos tanto en la entrada como en la salida.
d) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria.
e) Intervención en las líneas de comunicación de datos o teleproceso.
f) Interceptación de *e-mail*: lectura de un mensaje electrónico ajeno.
g) Estafas electrónicas: por medio de compras realizadas haciendo uso de la red.
h) Transferencias de fondos: engaños en la realización de este tipo de transacciones.
i) Uso indebido de información confidencial para beneficio propio: la red facilita la obtención de datos que pueden ser mal utilizados por el proveedor.

j) Pornografía y proxenetismo: La red facilita este tipo de comercio y hace más difícil la ubicación e identificación del proveedor.

Todos estos delitos se reducen a la problemática de la privacidad y seguridad de las transacciones electrónicas, a excepción del último, pornografía y proxenetismo, que más bien ha encontrado en la red un medio que ha facilitado su comercio.

También cabe resaltar que el problema de la privacidad al fin y al cabo también se reduce a un problema de seguridad de la información. Por tanto, no es posible abordar sólo del aspecto de la privacidad sin analizar al mismo tiempo los asuntos de seguridad de las transacciones.

2.3.5.3 Seguridad de las transacciones electrónicas y firma digital

Los riesgos e incertidumbres que plantea la comunicación telemática son los siguientes, de acuerdo con Bauzá (2003):

a) Identificación correcta de los interlocutores en la transacción.
b) Evitar fraudes, posibles suplantaciones.
c) Evitar negativas de esos interlocutores en cuanto a asumir autorías y recepciones de mensajes.
d) Asegurar que no haya alteraciones accidentales o dolosas.
e) Asegurar que los negocios que se plasman no lleguen a conocimiento de personas no autorizadas.

> "Con estos riesgos a la vista, si no existieran mecanismos garantistas, técnicos y jurídicos, no se podría nunca estar seguro de que un mensaje electrónico es fidedigno, es auténtico. Y esto a su vez estaría poniendo en jaque toda la estructura jurídica, el edificio jurídico de la validez y la eficacia de las transacciones electrónicas." (Bauzá, 2003, p. 77).

Para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida Internet básicamente se trata de garantizar cuatro principios:

> "Confidencialidad. Debe garantizarse que la información enviada sólo puede ser leída por personas debidamente autorizadas.

> Integridad. Debe garantizarse que la información no puede ser alterada en el transcurso hacia su destino.
> Autenticación. Debe garantizarse que los participantes en el intercambio de información o transacción comercial son realmente quienes dicen ser.
> No repudio. Debe garantizarse que ninguna de las personas involucradas en la transacción puedan negar posteriormente el hecho de haber participado en la misma." (Alonso, 2004, p. 30).

Los sistemas de seguridad y acceso actuales se basan en las claves, que son sumamente sencillas de suplantar por un pirata informático "no muy experto".

También surgen, dudas naturales en torno al reconocimiento legal de la igualdad que puedan tener las transacciones en papel, en relación a las electrónicas; cuando se emplean sistemas de identificación basados en clave, ya que no existe una legislación específica sobre este tema.

Ante dichas disyuntivas diversos organismos a nivel mundial han planteado la utilización de un sistema que proporcione suficiente seguridad al Comercio Electrónico, dándole validez jurídica y cobertura legal, ante una utilización fraudulenta o incorrecta. El sistema que más se ha adecuado a los parámetros estipulados, al garantizar la culminación y realización satisfactoria de negocios electrónicos seguros es el Sistema de la Firma Digital, más adelante se explica en detalle este sistema.

La seguridad de la información es un aspecto crítico. El desarrollo de un comercio electrónico seguro requiere contar con normas de seguridad que permitan proteger la información almacenada en computadoras conectadas a la red, así como la que viaja en ella; y garantizar que el uso que se de a la información no viole los derechos fundamentales del individuo. También es necesario reformar las normas penales para tutelar bienes jurídicos amenazados por los nuevos delitos de tipo informático, que a raíz del desarrollo de Internet, nacen también una gran cantidad y variedad de formas de comisión de delitos.

La firma digital, basada en la criptografía de clave pública, constituye el elemento tecnológico y legal que posibilita la realización de transacciones comerciales seguras mediante Internet y requiere ser regulada. Su implementación permite firmar contratos

por medio de la red, adquirir bienes y servicios, realizar pagos, votar o cualquier otra actividad donde se requiera identificación de autoría.

Actualmente existe un amplio movimiento legislativo que está implementando normas sobre firmas digitales y electrónicas para su uso con fines privados o comerciales. Estas leyes establecen el uso de claves públicas y privadas, y autorizan la existencia de autoridades certificadoras (también llamadas "terceras partes confiables"), que funcionan como una especie de notario que autentica *"on line"* la firma digital del usuario. En varios países ya se han aprobado leyes para la firma digital, entre ellos están: México, El Salvador, Chile, Colombia, Perú, Uruguay, Panamá y República Dominicana. En el caso de Costa Rica, recientemente, en el mes de setiembre de 2005, se publicó en La Gaceta Oficial la nueva Ley 8454, de Certificados, Firmas Digitales y Documentos Electrónicos.

En Estados Unidos, todos los Estados han promulgado normas que de alguna manera implementan el uso de firmas digitales en el sector público o en el privado.

En Europa, Alemania e Italia ya cuentan desde el año 1999 con leyes especiales que regulan el uso de estos reemplazos de la firma tradicional. Malasia, Japón y Corea han implementado proyectos o legislaciones sobre la firma por medios electrónicos.

Una vez que se otorga valor legal a la firma digital, es posible realizar contratos por medio de Internet, y allí surge la problemática jurídica de determinar su validez, la existencia del consentimiento válido, y su valor probatorio posterior en caso de discrepancias.

Es importante también que los países no pongan limitaciones a la circulación y exportación de programas para cifrar la información. Este es el caso de Francia o Estados Unidos, que prohíben la exportación de programas para cifrado de mensajes electrónicos, porque los consideran armas estratégicas en razón del nivel de seguridad que otorgan. Estas políticas han sido criticadas por la Organización de Cooperación y Desarrollo Económico (OCDE) quienes proponen la liberación de esas prohibiciones

para este mercado. También se ha opuesto la Unión Europea, que ha adoptado una postura similar.

A su vez, la infraestructura de firma digital que se constituya en un determinado ordenamiento jurídico deberá respetar la privacidad de los individuos. En tal sentido no puede obligarse a depositar la clave privada, medio por el cual se firma digitalmente, ante organismos estatales o fuerzas de seguridad, como medio de acceder a una eventual comunicación del usuario de la red.

2.3.6 Necesidad de una reacción jurídico-penal para proteger el comercio electrónico de los delitos informáticos

En los Estados Unidos existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos por medio de las computadoras. Esta entidad es el Instituto de Seguridad de Computadoras (CSI), el cual publicó en el año 2000 un documento denominado *Estudio de Seguridad y Delitos Informáticos*, que se realizó a un total de 273 instituciones principalmente grandes Corporaciones y Agencias del Gobierno. Este estudio es dirigido por CSI con la participación de la Agencia Federal de Investigación (FBI) de San Francisco, División de delitos informáticos. El objetivo de ese esfuerzo es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los delitos informáticos en los Estados Unidos de Norteamérica.

Entre lo más destacable del *Estudio de seguridad y delitos informáticos* se puede incluir lo siguiente:

Violaciones a la seguridad

- El 90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.
- El 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los

empleados -por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

Pérdidas financieras

- El 74% reconocieron pérdidas financieras debido a las violaciones de las computadoras. Las pérdidas financieras ascendieron a $265,589,940 (el promedio total anual durante los últimos tres años era $120,240,180).
- De los encuestados 61 cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27.148.000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendió a sólo $10.848.850.

Como en años anteriores, las pérdidas financieras más serias ocurrieron por medio del robo de información (66 encuestados reportaron $66.708.000) y el fraude financiero (53 encuestados informaron $55.996.000).

Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados, dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

Accesos no autorizados

El 71% de los encuestados descubrieron acceso no autorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque.

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del *Estudio de Seguridad y Delitos Informáticos 2000* confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo. El gráfico siguiente muestra los principales abusos y ataques informáticos.

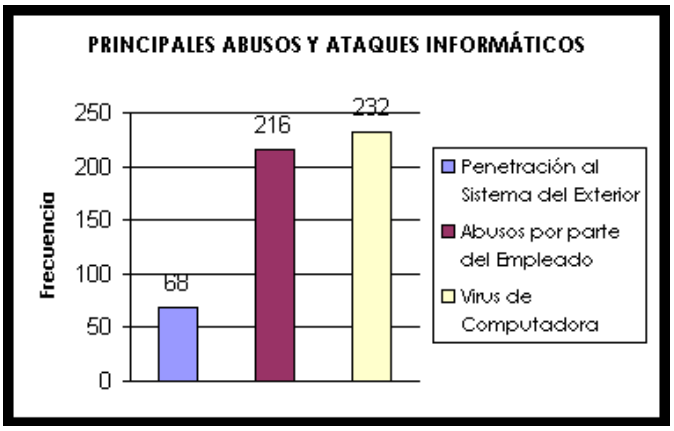


Figura 5. Principales abusos y ataques informáticos.
Fuente: (CSI, 2000)

El estudio concluye que la tendencia creciente de los delitos es alarmante. Los crímenes en Internet y otros delitos de seguridad de información se han extendido y diversificado. Además, tales incidentes pueden producir serios daños. Las 273 organizaciones que pudieron cuantificar sus pérdidas, informaron un total de $265.589.940. Claramente, la mayoría fue en condiciones que se apegan a prácticas legítimas, con un despliegue de tecnologías sofisticadas, y lo más importante, por personal adecuado y entrenado, practicantes de seguridad de información en el sector privado y en el gobierno.

Aunque los datos anteriores se refieren en forma general a violaciones a la seguridad, no específicamente relacionada con el comercio electrónico, no puede obviarse las inmensas posibilidades de violación a la seguridad que permite la red en el ambiente de comercio electrónico.

Otras estadísticas:

La *"línea caliente"* de la *Internet Watch Foundation (IWF)*, (mencionado en CSI, 2000), abierta en diciembre de 1996, ha recibido, principalmente por medio del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la *línea caliente* (un

85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.

Según datos recientes del Servicio Secreto de los Estados Unidos (citado en CSI, 2000), se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas *online* sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjeras bancarias y de crédito.

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo con el libro de Barbara Jenson *Acecho cibernético: delito, represión y responsabilidad personal en el mundo online*, publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año (indicado en CSI, 2000).

En Singapur el número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año 1999; la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999.

En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.

En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas *(software)* que utilizan. Esta proporción tan alta ha ocasionado que organismos Internacionales reaccionen ante este tipo de delitos, tal es el caso de *BSA (Bussines Software Alliance).*

Los datos anteriores reflejan que hay un gran impacto real en la seguridad y privacidad de la comunicación e intercambio de información en Internet, aspecto que tiende a

profundizarse conforme más usuarios acceden a los servicios en línea y aumenta la velocidad de conexión.

En Costa Rica se abrió la Unidad de Delitos Informáticos del Organismo de Investigación Judicial en el año 1996, a partir del cual y hasta el año 2001, habían recibido alrededor de 300 casos, un promedio de 60 ilícitos cada año, según informa Solano en un artículo publicado en el periódico La Nación del 1 de junio de 2001.

Por otro lado, de los archivos de esta Unidad, se obtuvo las siguientes estadísticas de casos de delitos informáticos:

Cuadro 4. Delitos Informáticos en Costa Rica. 2004-2005.

AÑO 2004		
DELITO	**CANTIDAD**	**TOTAL CASOS INGRESADOS**
Estafa	19	134
Fraude Informático	8	
Infracción Ley Derechos de Autor	8	
Tráfico de Drogas	7	
Defraudación Fiscal	7	
Producción y Difusión de pornografía	5	
Total	54	
AÑO 2005		
DELITO	**CANTIDAD**	**TOTAL CASOS INGRESADO**
Fraude Informático	15	142
Infracción Ley Derechos de Autor	7	
Amenazas	7	
Difusión y Producción de Pornografía	7	
Peculado	7	
Defraudación Fiscal	6	
Falsedad Ideológica	6	
Proxenetismo	6	
Administración Fraudulenta	5	
Estafa	4	
Total	70	

Fuente: (Lewis, 2005).

La columna de total de casos ingresados representa la totalidad de las denuncias que recibió la Unidad de Delitos Informáticos, de éstos, no todos fueron tipificados como delitos informáticos.

A partir de la creación de esta Unidad, todos los años se reciben denuncias, y puede esperarse que el desarrollo del comercio electrónico en el país traerá como consecuencia un aumento de este tipo de delitos.

Además, se debe considerar la cantidad de hechos ilícitos que no llegan a concretarse en denuncias explícitas ante las autoridades judiciales. Puede mencionarse entre estos, la propagación de virus informáticos que fueron alertados en varias ocasiones por la prensa nacional; los accesos no autorizados y robos de palabras claves que ocurren en los lugares de trabajo, que ni siquiera se concretan en denuncias.

Esto indica que cada vez se hacen más frecuentes actividades criminales de tipo informático como: alteración de información, creación de sitios falsos, propagación de virus, accesos no autorizados, fraudes, entre otros, que ya afectan a otros países.

La propuesta de atención legal sobre firmas digitales y certificados digitales, la Ley 8454, que entró en vigencia en el mes de setiembre del 2005, llega a solventar una parte de la problemática de la seguridad de las transacciones electrónicas. Pero todavía se hace necesario analizar lo que queda al descubierto y sin protección jurídica, que permita a la ciudadanía tener mayor confianza para que el comercio electrónico pueda desarrollarse.

2.3.7 Experiencias internacionales relacionadas con el problema del tratamiento penal de los delitos informáticos relacionados al comercio electrónico

Esta sección presenta el problema del tratamiento penal de los delitos informáticos y algunas experiencias internacionales al respecto.

2.3.7.1 Captura de delincuentes cibernéticos

A pesar de los grandes esfuerzos que han realizado muchos de los países desarrollados, todavía las autoridades enfrentan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo

que la investigación, enjuiciamiento y condena de los transgresores se convierte en un dolor de cabeza jurisdiccional y jurídico en general. Además, una vez capturados, se debe escoger entre extraditarlos para que se les siga juicio en otro lugar o transferir las pruebas, y a veces también a los testigos, al lugar donde se cometieron los delitos. Por otro lado, puede ocurrir, que los países no hayan firmado acuerdos de extradición por delitos de informática y que por lo tanto se dificulte la penalización del delito.

Cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Una serie de problemas rodean a la cooperación internacional en el área de los delitos informáticos, que se pueden resumir en los siguientes:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

2.3.7.2 Destrucción u ocultación de pruebas

Otro grave obstáculo al enjuiciamiento por delitos cibernéticos es el hecho de que los delincuentes pueden destruir fácilmente las pruebas cambiándolas, borrándolas o trasladándolas. O puede ser que los datos estén cifrados, una forma cada vez más

popular de proteger tanto a los particulares como a las empresas en las redes de computadoras.

Es posible que la criptografía dificulte las investigaciones penales, pero los derechos humanos podrían ser vulnerados si los encargados de hacer cumplir la ley adquieren demasiado poder técnico. Las empresas electrónicas sostienen que el derecho a la intimidad es esencial para fomentar la confianza del consumidor en el mercado de la Internet, y los grupos defensores de los derechos humanos desean que se proteja el cúmulo de datos personales archivados actualmente en ficheros electrónicos.

Por otro lado, los países con problemas de corrupción, el manejo de la información en forma segura es un elemento primordial para evitar la tentación a la comisión de delitos.

2.3.7.3 Identificación de delitos a nivel mundial

Las dificultades que enfrentan las autoridades en todo el mundo ponen de manifiesto la necesidad apremiante de una cooperación mundial para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición para poder alcanzar a los delincuentes.

Ya se han iniciado algunos esfuerzos al respecto, encontramos en Landaverde y otros (2000) la siguiente información sobre esfuerzos realizados al respecto por diferentes organismos internacionales:

- En el Manual de las Naciones Unidas de 1977 se insta a los Estados a que coordinen sus leyes y cooperen en la solución de ese problema.
- El Grupo de Trabajo Europeo sobre delitos en la tecnología de la informática ha publicado un Manual sobre el delito por computadora, en el que se enumeran las leyes pertinentes en los diversos países y se exponen técnicas de investigación, al igual que las formas de buscar y guardar el material electrónico en condiciones de seguridad.
- El Instituto Europeo de Investigación Antivirus colabora con las universidades, la industria y los medios de comunicación y con expertos técnicos en seguridad y

asesores jurídicos de los gobiernos, agentes del orden y organizaciones encargadas de proteger la intimidad a fin de combatir los virus de las computadoras o "caballos de Troya". También se ocupa de luchar contra el fraude electrónico y la explotación de datos personales.

- En 1997, los países del Grupo de los Ocho (o G-8, son los 8 países más poderosos: Alemania, Canadá, Estados Unidos, Francia, Gran Bretaña, Italia, Japón y Rusia) aprobaron una estrategia innovadora en la guerra contra el delito de "tecnología de punta". El Grupo acordó que establecería modos de determinar rápidamente la proveniencia de los ataques por computadora e identificar a los piratas, usar enlaces por vídeo para entrevistar a los testigos a través de las fronteras y ayudarse mutuamente con capacitación y equipo. También decidió que se uniría a las fuerzas de la industria con miras a crear instituciones para resguardar las tecnologías de computadoras, desarrollar sistema de información para identificar casos de uso indebido de las redes, perseguir a los infractores y recabar pruebas. El Grupo de los Ocho ha dispuesto ahora centros de coordinación abiertos 24 horas al día, siete días a la semana para los encargados de hacer cumplir la ley. Estos centros apoyan las investigaciones de otros Estados mediante el suministro de información vital o ayuda en asuntos jurídicos, tales como entrevistas a testigos o recolección de pruebas consistentes en datos electrónicos.

Un obstáculo mayor opuesto a la adopción de una estrategia del tipo Grupo de los Ocho a nivel internacional es que algunos países no tienen la experiencia técnica ni las leyes que permitirían a los agentes actuar con rapidez en la búsqueda de pruebas en sitios electrónicos, antes de que se pierdan, o transferirlas al lugar donde se esté enjuiciando a los infractores.

2.3.7.4 Algunas acciones tomadas

A medida que aumenta la delincuencia electrónica, numerosos países han promulgado leyes declarando ilegales nuevas prácticas como la piratería informática, o han

actualizado leyes obsoletas para que delitos tradicionales, incluidos el fraude, el vandalismo o el sabotaje, se consideren ilegales en el mundo virtual.

En el trabajo de Landaverde y otros (2000) menciona las siguientes acciones tomadas por diferentes países:

Singapur, por ejemplo, enmendó recientemente su Ley sobre el Uso Indebido de las Computadoras. Ahora son más severos los castigos impuestos a todo el que interfiera con las "computadoras protegidas", es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia, así como a los transgresores por entrada, modificación, uso o intercepción de material computarizado sin autorización.

Hay países que cuentan con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Oficina de Investigaciones Especiales de la Fuerza Aérea de los Estados Unidos, creada en 1978. Otro es el de Investigadores de la Internet, de Australia, integrado por oficiales de la ley y peritos con avanzados conocimientos de informática. El grupo australiano recoge pruebas y las pasa a las agencias gubernamentales de represión pertinentes en el Estado donde se originó el delito.

En Estados Unidos se han aprobado leyes que establecen castigos tomando en cuenta el valor económico del crimen. La nueva ley considera la Seguridad Nacional y los motivos por los que el delincuente cometió el crimen y con base a: los perjuicios económicos, la posibilidad de lastimar gente, y la sensibilidad de los datos modificados se establecen sanciones más duras que pueden incluir cadena perpetua. En materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En Alemania, se sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

Espionaje de datos.

Estafa informática.

Alteración de datos.

Sabotaje informático.

En Austria, La Ley de reforma del Código Penal, sancionada el 22 de Diciembre de 1987, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión de especialistas en sistemas.

En Holanda, el 1º de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- El hacking.
- El prehacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).
- La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).
- La distribución de virus.

En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:

- La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. El nuevo Código Penal de España sanciona en forma detallada esta categoría delictiva (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa.

- En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

En el caso de Costa Rica, en el año 2001 se crearon algunos tipos penales informáticos, por medio de la promulgación de la Ley No. 8148 del 2001; tales delitos son: violación a las comunicaciones electrónicas, fraude y sabotaje informático.

En síntesis, la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países en desarrollo, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los investigadores y expertos de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

2.4 Promoción del comercio electrónico

El problema de la seguridad en las redes es un tema que, por la magnitud de sus consecuencias y las proyecciones que se prevén en el futuro desarrollo de ellas, se ha tornado estratégico para los gobiernos en todo el mundo.

> "Estas proyecciones pronostican que el crecimiento y evolución de la sociedad de la información globalizada tendrá características exponenciales, en virtud del sostenido abaratamiento de los costos del hardware y software y del desarrollo de Internet II (que posibilita la conexión a cien veces mayor velocidad que en la actualidad) todo lo cual significará un aumento desmedido en la cantidad de usuarios conectados a la red." (Sarra, 2000, p. 148)

A esto se debe sumar los esfuerzos internacionales para promover el crecimiento del comercio electrónico y sus derivaciones (firma digital, contratos instrumentados digitalmente, moneda digital).

Con este último objetivo, los Estados han tomado decisiones estratégicas para otorgar mayor seguridad a las redes, fundamentalmente tratando de delinear un marco normativo adecuado que brinde seguridad jurídica, con el fin de fomentar el desarrollo de actividades a través de la red.

Encontramos en Sarra (2000) el proceso que lleva la promoción del comercio electrónico:

1. "Decisión estratégica: La tendencia evidenciada es que los Estados han decidido promover el comercio electrónico.
2. Seguridad en las redes: Para lograr esa promoción se fomenta la seguridad tecnológica y la creación de un adecuado marco jurídico.
3. Confianza en entornos digitales: Esa situación provoca confianza en los particulares e instituciones, lo cual posibilita la utilización fiable de las redes con fines comerciales.
4. Utilización masiva del comercio electrónico: La confianza generalizada en las redes origina su utilización habitual.
5. Crecimiento económico: El efectivo desarrollo del comercio electrónico contribuye al crecimiento económico de las naciones." (Sarra, 2000, p. 149).

Todas las acciones que se lleven a cabo en el desarrollo de seguridad y de normativas específicas para regular la administración, acceso y control de los sistemas informáticos, se traducirán tanto en la promoción del comercio electrónico como en la seguridad de las naciones.

2.5 Aspectos técnicos para la seguridad del comercio electrónico

2.5.1 Introducción

Existen todavía numerosas barreras a la implantación del comercio electrónico: costos de investigación, difícil acceso a los clientes, mayor competencia, falta de experiencia, incipiente regulación legal. Sin embargo, el obstáculo fundamental viene determinado por la consecución de una seguridad efectiva en las transacciones, tanto para el vendedor como para el comprador. Se requiere el desarrollo de mecanismos de protección, confianza y seguridad, que garanticen que ambos sean quienes dicen ser, que los mecanismos de pago sean eficientes o que simplemente se garantice que el objeto o servicio deseado sea entregado a la persona que realmente lo ha adquirido, tal y como se muestra en el siguiente cuadro.

Cuadro 5. Paradigmas de la seguridad electrónica.

	Vendedor	Comprador
Autenticación	Conocer la identidad del comprador antes de que se realice la compra.	Confirmar la identidad del vendedor antes de que se realice la compra.
Certificación	Probar que el comprador está capacitado para realizar la compra.	
Confirmación	Posibilidad de probar ante cualquier persona que el comprador autorizó la compra y el pago.	Obtención de un recibo que garantice la compra y el pago efectuado.
No repudio	Protección frente al comprador de que niegue la compra efectuada.	Protección frente al vendedor por incumplimiento de las condiciones de la transacción.
Pago	Seguro frente al comprador de que pagará lo acordado.	Seguro frente a pagos no autorizados.
Privacidad		Interés en no manifestar su identidad.

Fuente: (Fernández, 2002)

En el comercio tradicional todas estas circunstancias han sido solucionadas mediante elementos físicos, en el mundo electrónico se han tenido que desarrollar sistemas virtuales que realicen las mismas funciones que sus homólogos en el mundo real, tal y como se muestra en el siguiente cuadro.

Cuadro 6. Medidas de seguridad electrónicas.

Problema	Medida material	Concepto electrónico	Solución electrónica
¿Quién tiene acceso a …?	Tarjeta de identidad	Identidad	Certificados digitales
¿Cómo puedo garantizar que soy quien digo ser?	Tarjeta de identidad y firma	Autenticación	Firma digital
¿Cómo garantizo que sólo tienen acceso a la información aquellos que he autorizado?	Entrega en mano. Firma del destinatario a la recepción	Confidencialidad	Encriptación
¿Cómo puedo asegurarme que la información no ha sido manipulada?	Sobres y paquetes sellados.	Integridad	Firmas digitales
¿Cómo me aseguro que no nieguen su participación en la transacción?	Notarios, testigos, certificados.	No repudio	Firmas digitales

Fuente: (Fernández, 2002)

La siguiente sección describe las soluciones técnicas existentes para dar seguridad al comercio electrónico.

2.5.2 Seguridad en la comunicación

Las condiciones que debe reunir una comunicación segura a través de Internet (o de otras redes) son en general las siguientes, como se comentó anteriormente:

- Confidencialidad: evita que un tercero pueda acceder a la información enviada.
- Integridad: evita que un tercero pueda modificar la información enviada sin que lo advierta el destinatario.
- Autenticación: permite a cada lado de la comunicación asegurarse de que el otro lado es realmente quien dice ser.
- No repudio: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación. En el caso de no repudio de origen, el remitente del mensaje no puede negar haberlo enviado. En el caso de no repudio de destino, el destinatario del mensaje no puede negar haberlo recibido.

La herramienta básica para cumplir las condiciones anteriores son las técnicas criptográficas, en particular los métodos de cifrado simétrico (usan una misma clave secreta para cifrar y descifrar) o asimétrico (cada usuario tiene una pareja de claves, una pública y otra privada, con la propiedad de que lo que se cifra con una de las claves sólo se puede descifrar con la otra). La siguiente sección resume brevemente los aspectos técnicos básicos de estos métodos de cifrado.

2.5.2.1 Cifrado simétrico

Los métodos de cifrado simétrico se caracteriza por usar una misma clave para cifrar y descifrar. Suponiendo que dos interlocutores comparten una clave secreta y de longitud suficientemente grande, el cifrado simétrico permite garantizar la confidencialidad de la comunicación entre ellos.

Los algoritmos de encriptación simétricos tienen la ventaja de ser muy rápidos. Sin embargo, éstos son pocos adecuados cuando una parte establece comunicaciones ocasionales con muchas otras con las que no tenía una relación previa, como ocurre frecuentemente en el comercio electrónico, ya que antes de poder establecer cada comunicación sería necesario intercambiar previamente por algún procedimiento seguro la clave que se va a utilizar para cifrar y descifrar en esa comunicación. El emisor debe dar a conocer al receptor la clave para que éste sea capaz de descifrar el mensaje.

El principal inconveniente viene dado por la necesidad de distribuir la clave, además del mensaje. Por ejemplo, un consumidor que quisiera comprar a través de Internet necesitaría intercambiar una clave secreta diferente con cada uno de los vendedores a los que quisiera acceder. Si una tercera persona consigue interceptar la clave enviada, podrá descifrar cualquier mensaje que utilice dicha clave, rompiendo así la seguridad de este mecanismo.

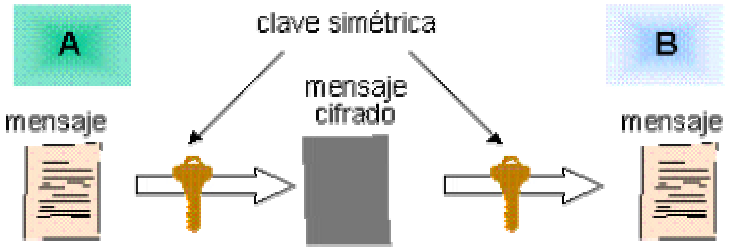


Figura 6. Cifrado/descifrado simétrico

Fuente: (Urtza e Ibon, 2003)

Los principales algoritmos de encriptación de clave simétrica utilizados en la actualidad son las siguientes, de acuerdo con Alonso (2004):

- DES (Data Encryption Estándar): El algoritmo DES toma como entrada bloques de 64 bits del mensaje original y cada uno de éstos se somete a 16 interacciones usando una clave de 56 bits más 8 de paridad (para chequeo de errores). Tiene

la ventaja de que es muy rápido, su implementación es muy simple, está muy extendido a nivel mundial y, hasta la fecha, no ha sido posible romperlo, es decir, no se ha conseguido desarrollar un método para obtener la clave simétrica a partir del mensaje cifrado. La principal desventaja del este algoritmo es que la clave es relativamente corta (sólo 56 bits) y por tanto, con un computador suficientemente potente es posible aplicar un mecanismo de “fuerza bruta” para descifrar la clave en un tiempo relativamente corto, es decir, probar todas las posibles combinaciones de 56 bits (aproximadamente 72.000 billones de combinaciones) hasta dar con la clave empleada.

- Triple DES (TDES): Se ideó para evitar el problema de la longitud de la clave de DES. El funcionamiento TDES consiste en aplicar tres veces DES de la siguiente manera: se utilizan dos claves distintas de 64 bits cada una (K1 y K2). El texto original se cifra con la clave K1, luego se descifra con la clave K2, dando lugar a un texto distinto del original y finalmente éste se vuelve a cifrar con K1.

- IDEA (International Data Encryption Algorithm): su estructura es muy similar a DES, aunque utiliza una clave de mayor longitud (128 bits) que mejora notablemente su seguridad.

- Rijndael: Ante las limitaciones de seguridad de los algoritmos de clave simétrica existentes, en el año 1997, el instituto NIST (National Institute of Standard Technology, sucesor del NBS) convocó un nuevo concurso para seleccionar un sistema criptográfico de clave simétrica que pudiese utilizarse como estándar durante, al menos, los siguientes 20 años. En agosto de 1999 el NIST publicó la lista de los cinco algoritmos que pasaron la primera fase de pruebas (MARS, RC6, Rijndael, Serpent y Twofish) y en agosto de 2000 se publicó como ganador el algoritmo Rijndael, desarrollado por J. Daemen y V. Rijmen.

2.5.2.2 Cifrado asimétrico

Los métodos de cifrado asimétrico, usan parejas de claves con la propiedad de que lo que se cifra con cualquiera de las claves de una pareja sólo se puede descifrar con la otra clave de la pareja. En el caso más simple, con este sistema un interlocutor sólo necesita tener una pareja de claves que puede utilizar para comunicarse de forma segura con cualquier otro interlocutor que disponga a su vez de otra pareja de claves. Cada interlocutor hace pública una de sus claves (será su clave pública) y mantiene en secreto la otra (su clave privada). Por ello, el cifrado asimétrico se denomina también cifrado de clave pública. La clave privada (o las claves privadas si el usuario utiliza varias parejas de claves para diferentes propósitos) puede guardarse en el ordenador del usuario o en una tarjeta inteligente.

Por la propiedad de las parejas de claves citada antes, para enviar un mensaje de forma confidencial a un destinatario basta cifrarlo con la clave pública de ese destinatario. Así sólo él podrá descifrarlo mediante la clave privada que mantiene en secreto. No es necesario que el remitente y el destinatario intercambien previamente ninguna clave secreta. El remitente sólo necesita averiguar la clave pública del destinatario. Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación. Vea la siguiente figura.

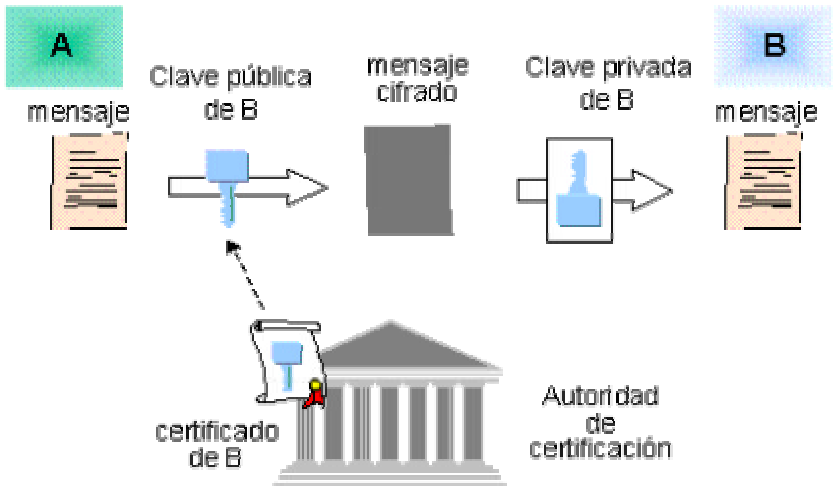


Figura 7. Cifrado asimétrico con consulta de clave pública a autoridad de certificación y descifrado con clave privada del destinatario.

Fuente: (Urtza e Ibon, 2003)

Las claves pública y privada están relacionadas matemáticamente de forma que la clave pública se obtiene a partir de la privada. Sin embargo es computacionalmente muy complejo obtener la clave privada a partir de la pública.

El mecanismo de encriptación por clave pública funciona de la siguiente forma, suponga que A quiere enviar un mensaje a B:

1. A cifra el mensaje con la clave pública de B.
2. A envía el mensaje cifrado.
3. B descifra el mensaje con su clave privada.

El usuario A debe conocer la clave pública de B (y viceversa), por tanto, la primera vez que estos usuarios quieren establecer una comunicación deben intercambiar sus respectivas claves públicas. De esta forma, cada usuario puede coleccionar varias claves públicas correspondientes a cada uno de los usuarios con los que ha establecido una comunicación previa, formando lo que se conoce como un “llavero” de claves públicas.

La ventaja fundamental de la encriptación por clave pública es su elevada seguridad: solamente el propietario de la clave privada puede descifrar un mensaje cifrado con su clave pública. Puesto que la clave privada nunca se transmite por la red, es imposible que alguien la conozca, aparte de su propietario. El principal inconveniente de este mecanismo es que el cifrado y el descifrado puede llevar un tiempo excesivo (varios minutos).

Los principales algoritmos de encriptación de clave pública empleados en la actualidad de acuerdo con Alonso (2004) son:

- RSA: Se basa en la dificultad matemática que supone la factorización de números grandes (mayores a 512 bits). Se toman 2 números primos, p y q, cuyo producto es un número N muy elevado (mayor de 10^{150}), de manera que a partir de N es computacionalmente imposible obtener p y q. El número N forma la clave pública, que se utiliza para cifrar el mensaje. Los números p y q, forman la clave privada, que se utilizan para descifrar el mensaje.

- Diffie-Hellman: este algoritmo fue el primero de encriptación basado en clave pública. Este algoritmo se emplea únicamente para el intercambio eficiente y seguro de claves simétricas, denominada clave secreta compartida.

2.5.2.3 Firmas digitales

Los sistemas de clave pública permiten además cumplir los requisitos de integridad del mensaje, autenticación y no repudio del remitente utilizando firmas digitales.

El procedimiento de firma digital de un mensaje consiste en extraer un "resumen" (o “hash” en inglés) del mensaje, cifrar este resumen con la clave privada del remitente y añadir el resumen cifrado (firma) al final del mensaje. A continuación, el mensaje más la firma (el resumen cifrado) se envía cifrados con la clave pública del destinatario. El algoritmo que se utiliza para obtener el resumen del mensaje debe cumplir la propiedad de que cualquier modificación del mensaje original, por pequeña que sea, dé lugar a un

resumen diferente. (Note que la firma digital de un usuario no es siempre la misma secuencia de bits, sino que depende del mensaje firmado). Vea la figura siguiente .

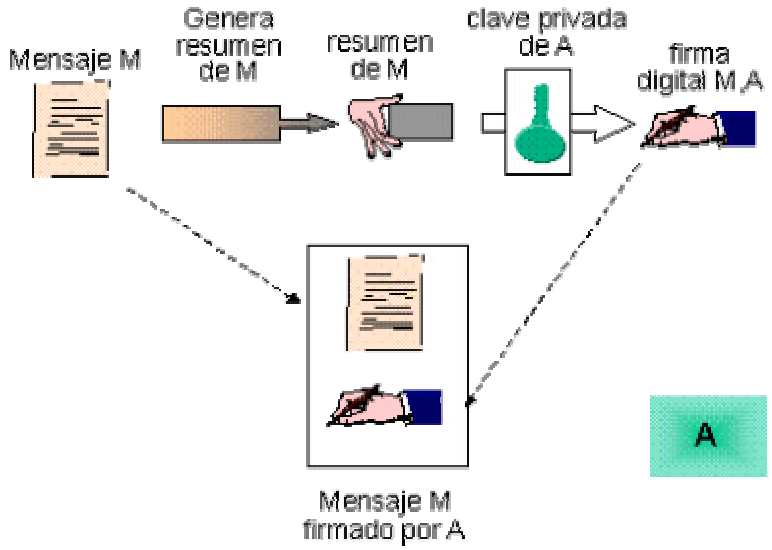


Figura 8. Generación de la firma digital de un mensaje.

Fuente: (Urtza e Ibon, 2003)

Cuando el destinatario recibe el mensaje, lo descifra con su clave privada y pasa a comprobar la firma. Para ello, hace dos operaciones: por un lado averigua la clave pública del remitente y descifra con ella el resumen que calculó y cifró el remitente. Por otro lado, el destinatario calcula el resumen del mensaje recibido repitiendo el procedimiento que usó el remitente. Si los dos resúmenes (el del remitente descifrado y el calculado ahora por el destinatario) coinciden, la firma se considera válida y el destinatario puede estar seguro de la integridad del mensaje: si el mensaje hubiera sido alterado a su paso por la red, el resumen calculado por el destinatario no coincidiría con el original calculado por el remitente.

Además, el hecho de que el resumen original se ha descifrado con la clave pública del remitente prueba que sólo él pudo cifrarlo con su clave privada. Así el destinatario está seguro de la procedencia del mensaje (autenticación del origen) y, llegado el caso, el

remitente no podría negar haberlo enviado (no repudio) ya que sólo él conoce su clave secreta. Vea figura siguiente.

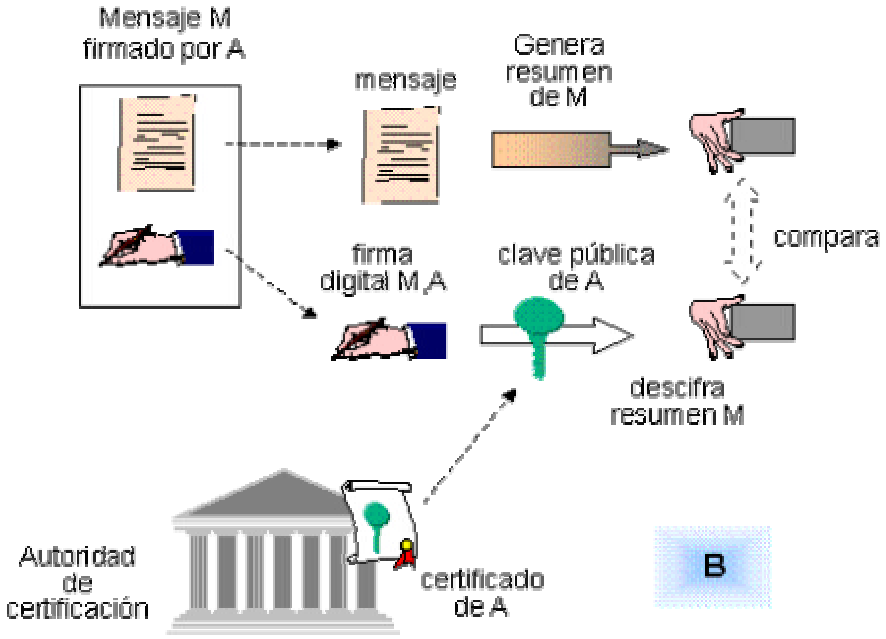


Figura 9. Comprobación de una firma digital.

Fuente: (Urtza e Ibon, 2003)

El mensaje enviado puede, a su vez, descifrarse con alguna de las técnicas de la clave simétrica o pública. De esta forma tenemos cuatro posibles combinaciones, que se resumen en el siguiente cuadro:

Cuadro 7. Nivel de seguridad y requerimiento de cifrado y firmado.

Nivel de seguridad	No cifrado, no firmado	Cifrado, No firmado	No cifrado, firmado	Cifrado Firmado
Confidencialidad	NO	SI	NO	SI
Integridad	NO	NO	SI	SI
Autenticación y no repudio	NO	NO	SI	SI

Fuente: (Fernández, 2002)

La función hash debe cumplir determinados requisitos para que pueda ser considerada segura. Estos son los siguientes:

- Debe transformar un texto longitud variable en un bloque de longitud fija, que generalmente es pequeña (algunas son de 16 bits).
- Debe ser sencilla de implementar.
- Debe ser irreversible, es decir, no se puede obtener el texto original del resumen hash.
- Debe ser imposible encontrar dos mensajes diferentes cuyo resumen, después de aplicar la función hash, sea el mismo.

Los inconvenientes de este sistema son la lentitud de los algoritmos de clave asimétrica (típicamente varias veces más lentos que los de clave simétrica) y la necesidad de las autoridades de certificación ya mencionadas. Un certificado digital emitido por una de estas autoridades contiene la identidad de un usuario, su clave pública y otros datos adicionales (por ejemplo, el período de validez del certificado), todo ello firmado digitalmente con la clave privada de la autoridad de certificación, con el fin de que el certificado no se pueda falsificar. Pueden existir varios tipos de certificados, válidos para diferentes usos, según la información y garantías que la autoridad de certificación (directamente o a través de una autoridad de registro) pide al usuario antes de emitir el certificado.

Como en la práctica no es viable que todos los usuarios estén certificados por la misma autoridad, surge la necesidad de que unas autoridades de certificación certifique a su vez a otras, bien de forma jerárquica (las autoridades de un nivel jerárquico son certificadas por otras de nivel superior hasta llegar a una autoridad raíz) o mediante certificaciones cruzadas entre autoridades del mismo nivel (de forma que cada una acepta como fiables los certificados emitidos por la otra). La infraestructura necesaria para el uso de los sistemas de clave pública, incluyendo las autoridades de certificación, se llama Infraestructura de Clave Pública (PKI: Public Key Infrastructure).

Hay muchos detalles no incluidos en este resumen, por ejemplo el uso de varias parejas de claves, diferentes tipos de certificados, la combinación de algoritmos de clave simétrica y asimétrica, los estándares existentes para cifrado, firmas, certificados, etc.

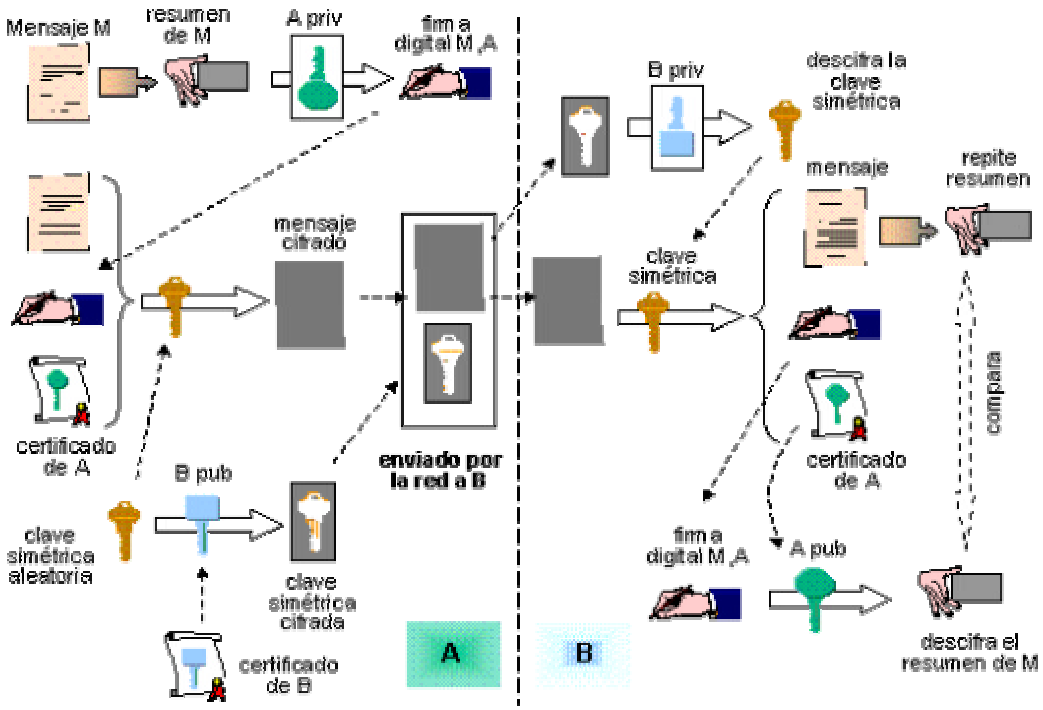
2.5.3 Mecanismos de seguridad en el pago electrónico

Actualmente existe una amplia diversidad de mecanismos de pago electrónico. La interoperabilidad entre estos mecanismos sería deseable, aunque en algunos casos este requisito puede introducir un costo adicional apreciable en las transacciones. Tanto la Unión Europea como Estados Unidos favorecen los acuerdos de la industria como mejor forma de incrementar la interoperabilidad, aunque sin descartar la necesidad de introducir normas generales.

En general, los vendedores a través de Internet tratarán de soportar el mayor número posible de sistemas de pago con el fin de atraer más clientes (como ocurre ahora en el comercio tradicional).

2.5.3.1 Pagos con tarjeta de crédito a través de Internet

Un ejemplo de un método de pago electrónico es el protocolo SET (Secure Electronic Transaction) definido por MasterCard y Visa con la colaboración de otras importantes compañías como IBM, Microsoft y Netscape. SET permite hacer transacciones seguras con tarjeta de crédito a través de Internet. Para ello utiliza procedimientos de cifrado simétrico y asimétrico, firmas digitales y certificados como los descritos anteriormente (ver detalles en la siguiente Figura).



Apub, Apriv: claves pública y privada de A; Bpub, Bpriv: claves pública y privada de B

Figura 10. Esquema de cifrado en SET.

Fuente: (SETS, 1997)

SET es un protocolo aplicable al comercio electrónico de empresa a consumidor, que básicamente reproduce en el entorno electrónico el procedimiento de pago con tarjeta de crédito utilizado hoy en día. La versión 1.0 de SET se publicó en 1997. Aunque hasta la fecha se ha utilizado relativamente poco (por ejemplo en países del norte de Europa como Dinamarca o Finlandia), esta situación puede cambiar si hay un apoyo decidido de las entidades financieras a este sistema. En el caso de España, la Agencia de Certificación Electrónica, en la que participan Telefónica, CECA, SERMEPA y Sistema 4B, emite ya certificados SET. Para los usuarios estos certificados se ofrecerán como un servicio más de los bancos y cajas, con la consiguiente imagen de seguridad dada por estas entidades y, en principio, buenas perspectivas de aceptación por los consumidores.

Otros sistemas de pago electrónico basados en tarjetas son CyberCash y First Virtual.

2.5.3.2 Cheques y órdenes de pago electrónicas

En el caso del comercio entre empresas el pago mediante tarjeta de crédito es mucho menos usual, por lo que un sistema como SET parece claramente menos adecuado que en el escenario anterior. Entre empresas, en particular PYMEs, es frecuente el pago mediante cheques. Los sistemas de pago basados en cheques electrónicos pueden reducir considerablemente el costo de procesar los cheques y minimizar el fraude (firma digital en lugar de firma tradicional).

Un ejemplo de sistema de cheque electrónico es el eCheck definido por el FSTC (Financial Service Technology Consortium), un consorcio de más de 90 miembros, principalmente bancos, que colaboran de forma no competitiva en el desarrollo de proyectos técnicos. El sistema FSTC utiliza una tarjeta inteligente para implementar un "talonario de cheques electrónicos" seguro. La Tesorería estadounidense firmó en junio de 1998 su primer cheque electrónico usando este sistema, marcando el inicio de un período de pruebas del sistema antes de su comercialización. Otro ejemplo es el sistema NetCheque, desarrollado por la Universidad del Sur de California, que básicamente reproduce en la Red el sistema usual de emisión de cheques y compensación entre bancos.

2.5.3.3 Dinero electrónico

Los sistemas de pago citados en los párrafos anteriores sirven para realizar transacciones electrónicas (cargo en una tarjeta de crédito, orden de pago) sobre dinero no electrónico. Existe otro grupo de sistemas en los que se maneja directamente dinero electrónico, por ejemplo almacenado en una tarjeta inteligente que hace de monedero electrónico.

Estos sistemas se basan en el prepago, es decir la conversión previa de dinero real en dinero electrónico. Por comparación, los sistemas de cheque electrónico serían sistemas de tipo “pague ahora” y los de pago electrónico con tarjeta serían de tipo “pague más tarde”. Los sistemas de dinero electrónico suelen caracterizarse por un bajo

costo de cada operación de pago, lo que los hace apropiados para realizar micropagos. Por micropagos se entiende cantidades (muy) pequeñas, por ejemplo unos pocos dólares o colones, y que en ocasiones pueden llegar a ser del orden de $0.02 o incluso menores. Los micropagos son muy importantes para hacer posible el comercio electrónico de fotografías, imágenes, noticias, pequeños programas y otros elementos que pueden tener un valor unitario bajo, así como para poner en práctica esquemas de pagar por ver páginas Web, pagar por jugar a un juego a través de la red, etc.

En general, los sistemas de dinero electrónico se basan en “tokens”, esto es, secuencias de bits que representan un cierto valor en sí mismas y que se almacenan en un dispositivo específico como una tarjeta inteligente (denominadas normalmente tarjetas de valor almacenado o monederos electrónicos) o simplemente como ficheros en el disco de un ordenador. Los “tokens” se obtienen a cambio de una cantidad de dinero real (es decir, son sistemas de prepago). Para certificar su valor, el banco emisor firma los “tokens” con su firma digital, se los entrega al usuario que los ha pedido y carga en la cuenta de este usuario la cantidad de dinero real correspondiente al dinero digital generado. Una vez creados y firmados, los “tokens” pueden almacenarse como se ha dicho, transferirse a través de la red a cambio de un producto o un servicio y, eventualmente, volverse a convertir en dinero real.

Los “tokens” se convierten así en el equivalente digital de los billetes y monedas y, de hecho, comparten con ellos muchas características, por ejemplo: el pago es rápido, sin autorización previa y (relativamente) anónimo, debe evitarse la posibilidad de falsificar o duplicar “tokens” (para evitar que se pueda gastar el mismo dinero digital varias veces), si se pierde el dinero electrónico o éste es robado no hay posibilidad de impedir que otra persona lo gaste.

Algunos sistemas de dinero electrónico son:

- ecash (de Digicash, compañía de origen holandés)
- Millicent (de Digital Equipment Corporation)

Y de monedero electrónico:

- EMV (sistema de Europay, Mastercard y Visa)
- European Electronic Purse (EEP), iniciativa del European Committee for Banking Standards (ECBS)
- Conditional Access for Europe (CAFE), proyecto ESPRIT 7023.
- MONDEX

2.5.4 Seguridad de los Servidores

A nivel global, el protocolo SET (Secure Electronic Transaction) proporciona toda la seguridad en las transacciones de comercio electrónico. Los servidores seguros que utilizan el protocolo SSL (Secure Sockets Layer) ofrecen las medidas suficientes para disfrutar con toda comodidad de las compras realizadas desde la casa.

A continuación se describen los aspectos básicos del Protocolo SSL (Secure Sockets Layer) .

Servidor Seguro - Protocolo SSL (Secure Sockets Layer)
Un servidor seguro garantiza la confidencialidad de los datos personales que viajan por la red. El protocolo que se encarga de asegurar la privacidad de la información es el SSL.

El protocolo SSL cifra los datos que se envían a través de Internet, mediante el sistema RSA. Los principales softwares para navegar Netscape y Explorer, actúan en colaboración con el servidor seguro. De tal forma que, cuando detectan que se encuentran en un servidor seguro, cifra los datos de manera que resulta imposible que una persona ajena al circuito pueda acceder a su lectura.

Un servidor seguro se identifica mediante el símbolo de una Llave entera o un Candado cerrado, visible en los márgenes de la pantalla de la computadora. También se identifica un servidor seguro con un pequeño cambio en la descripción de la URL o dirección de la página. Por ejemplo la típica http se transforma en https.

Hoy día existe una certificación de seguridad del servidor mediante la expedición de un documento que certifica que la empresa titular del servidor seguro cumple una serie de condiciones en el proceso de encriptación de los datos (SSL). La empresa certificadora es una entidad externa independiente que controla, verifica y comprueba la configuración del servidor y los datos de la empresa solicitante.

Los compradores, los comerciantes, los intermediarios financieros y los bancos tendrán la confianza de que cada transacción está protegida por un protocolo de validación aceptado.

En Costa Rica, el acceso a la red Internet utiliza los protocolos de autenticación PAP/CHAP (Password Authentication Protocol/Challenge Handshake Authentication Protocol). Son protocolos de autenticación que se encargan de realizar la validación de los usuarios.

Para garantizar a los compradores transacciones seguras varias empresas financieras, como Credomatic, están ofreciendo el protocolo SSL, que debería ser asumido por todas las empresas para proteger la información de sus clientes.

2.6 Leyes Modelos de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional (CNUDMI)

2.6.1 Antecedentes

A partir de los años 60, las Naciones Unidas, se ha dedicado a facilitar los procedimientos del comercio internacional, agilizando trámites y reduciendo requisitos excesivos. A principios de los años 90 se ha preocupado por el Intercambio Electrónico de Datos, conocido como "EDI" por sus iniciales en inglés. La Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional (CNUDMI), mejor conocida por sus iniciales en inglés UNCITRAL, constituyó un Grupo de Trabajo en Comercio Electrónico a fin de elaborar leyes modelos que den soporte legal a los mensajes electrónicos. Este esfuerzo produjo la reciente Ley Modelo de la CNUDMI sobre el Comercio Electrónico.

Este proyecto de Ley Modelo consideró la falta de uniformidad internacional con respecto a la regulación de los conocimientos de embarque negociables, y se trabajó para dar una solución que cubriera todos los tipos de conocimientos de embarque.

El Grupo de Trabajo EDI recomendó que la falta de uniformidad necesitaba ser considerada por otro grupo de trabajo, al que se le encomendara estudiar y analizar y trabajar con otras organizaciones interesadas acerca de los problemas relacionados con el transporte de mercancías por agua.

Posteriormente, el Proyecto de la Ley Modelo se remitió, para el examen de la Comisión, con todos los artículos generales completos y renombrado el mismo como Proyecto de Ley Modelo sobre "COMERCIO ELECTRÓNICO", con el fin de ampliar su ámbito de aplicación, no solo a los EDI sino a todas las formas de transmisión de mensajes electrónicos comerciales. El nombre del grupo trabajo fue consecuentemente cambiado para reflejar esta decisión.

Se hicieron reformas a los artículos para ampliar su aplicabilidad para todo tipo de transporte.

Al completarse los primeros 17 artículos de la Ley Modelo, la Secretaría de la CNUDMI, emitió un informe sobre el tema de firmas digitales, para ser considerado por el Grupo de Trabajo. El informe indica que este tema tiene serias dificultades para su tratamiento jurídico desde que el mismo depende todavía más de la tecnología que de la ley. Por ello, los borradores preliminares han sido preparados con el entendimiento de que un nuevo trabajo y discusión serían necesarios.

Las firmas digitales han sido desarrolladas por más de seis años por varios grupos comerciales. La inexistencia de un patrón uniforme de tratamiento de las firmas ha afectado su desarrollo. El problema es debido a que cada diseñador de programas de computación puede adoptar su propio patrón, y esto hace que cada comerciante tenga que pagar e instalar programas diferentes para cada una de las partes con las cuales desearía negociar.

Con la gran cantidad de patrones competitivos e irreconciliables, la "Internacional Standards Organization" (ISO) se ha encontrado incapacitada para lograr un consenso sobre los mismos. Esto ha dado lugar, a que los diseñadores de firmas digitales hayan estado presionando a la CNUDMI, a través de sus Estados miembros, para que redacte y apruebe reglas de naturaleza legal, las cuales son en realidad en muchos aspectos, patrones técnicos. El Grupo de Trabajo ha resistido la tentación de involucrarse en la controversias de los patrones, dejando la discusión de ese tema sólo a las autoridades de certificación, y manteniendo una actitud neutral en este asunto.

En las siguientes secciones se presentan un resumen de las leyes modelos propuestos por la CNUDMI sobre comercio electrónico y para las firmas electrónicas, el texto completo de ambas leyes modelos se encuentran en el anexo 7.

2.6.2 Resumen de la Ley Modelo de la CNUDMI sobre Comercio Electrónico

En la primera parte de la Ley Modelo, compuesta de quince artículos, se establecen principios generales con el fin de dar el soporte legal al comercio electrónico en aquellos países que promulguen las leyes modelos. Estas serían extremadamente útiles en suministrar el necesario apoyo legal a las Reglas de 1990 del Comercio Marítimo Internacional (CMI) sobre Conocimientos de Embarques Electrónicos. Sin embargo, tales artículos no tienen aplicación directa al comercio marítimo, pero son esenciales si el comercio marítimo se realiza en un ambiente electrónico.

En la segunda parte del proyecto de ley, compuesto de dos artículos (16 y 17) referidos a los contratos de transporte de mercancías, se provee la base legal para que los documentos de transporte electrónicos sean negociables, redactados de forma tal que sean aplicables a cualquier tipo de transporte.

El Capítulo I, contiene las provisiones generales: ámbito de aplicación (artículo 1), definiciones (artículo 2), interpretación (artículo 3) y modificación mediante acuerdo (artículo 4).

La característica única de este capítulo es la creación del término "mensaje de datos" usado para diferenciar el cruce de comunicación con las otras formas de aviso, información y mensajes tradicionales. El grupo de trabajo se esforzó con el término apropiado a lo largo de los años para el desarrollo de la Ley Modelo. En realidad, virtualmente cualquier nombre hubiera podido ser usado desde que no hay un precedente para tal concepto. La más fácil solución, podría haber sido simplemente denominar el concepto "mensaje" o "aviso", pero estos términos son algo genéricos y tienden a causar confusión por su uso común. Por ello, el término "mensaje de datos", no tiene otro significado especial que el de darle sustancia a un concepto.

La modificación mediante acuerdo (artículo 4) está diseñada para facilitar la libertad del contrato. La Interpretación (artículo 3), incita a los eventuales usuarios e intérpretes de la Ley Modelo para que tengan una mente amplia en su aplicación e interpretación dado su origen internacional.

El Capítulo II, se refiere a la aplicación de los requisitos legales de los "mensajes de datos", comenzando con su reconocimiento jurídico (artículo 5), al señalar que no se le negará efectos jurídicos, validez o fuerza probatoria por la sola razón de que esté en forma de mensaje de datos. Este reconocimiento es necesario, esencial y de sentido común, por la razón de que el comercio electrónico es un concepto nuevo, lo que probablemente causará resistencia a su aceptación en lugar de las formas tradicionales, siendo de invalorable ayuda para la implementación de los conocimientos de embarque electrónicos.

Los artículos 6 al 8, sobre escrito, firma y original, respectivamente, proporcionan la llamada "equivalencia funcional". Si hay un requerimiento legal para una de esas categorías, esos requerimientos pueden ser satisfechos por el equivalente funcional del mensaje de datos.

El problema de la admisibilidad y la fuerza probatoria de los "mensajes de datos" (artículo 9), está solucionado en aquellas jurisdicciones donde se ha adoptado la llamada "regla de la mejor prueba" (best evidence rule), conforme a la cual no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de

un mensaje de datos por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

Es importante, sin embargo, señalar que, tal como se mencionara durante las deliberaciones del Grupo de Trabajo, probablemente habrán casos, especialmente en los países de derecho continental o civil, en donde su derecho procesal no ha admitido esa regla de prueba, por lo que sus tribunales se encontrarán en dificultad en admitir el valor probatorio de los mensajes de datos generados por computadoras, en lugar de los documentos escritos en papel, tradicionalmente admitidos.

El artículo restante en este capítulo, señala los requisitos para la conservación o el archivo de los mensajes de datos (artículo 10). Para que el mensaje de datos sea confiable, es esencial que sean conservados o archivados sin que se le pueda hacer modificación alguna durante largos períodos de tiempo. Igualmente, es importante que, durante ese largo período de tiempo, puedan ser accesibles. Esos requisitos parecieran fáciles de cumplir, pero ello no es así dada la velocidad de los cambios tecnológicos, ocasionando la obsolescencia tanto de las máquinas (hardware) como de los programas (software) de computación. Es claro, que muchos cambios pueden tener lugar en pocos años, de modo tal que el mensaje de datos generado años atrás, posiblemente no pueda leerse e imprimirse por un equipo actual. Por ello, no es suficiente poder conservar o archivar mensajes de datos en discos, sino también poder tener una computadora operativa, capaz de leer e imprimir el mensaje de datos requerido.

El Capítulo III prevé los protocolos de comunicación de los mensajes de datos; esto es la formación y validez de los contratos a través de los "mensajes de datos" (artículo 11), su reconocimiento por las partes (artículo 12), su atribución (artículo 13), su acuse de recibo (artículo 14) y su tiempo y lugar del envío y recepción (artículo 15). Mientras que estos artículos no establecen normas directa y necesariamente aplicables a los conocimientos de embarque electrónico, podrían ser útiles para definir los derechos y responsabilidades que nacen de los mensajes de datos, a los efectos de la aplicación voluntaria de las Reglas de París del CMI.

La segunda parte de la Ley Modelo, está dirigido a la regulación del comercio electrónico en áreas específicas, la primera de las cuales es el transporte de mercancías. En el artículo 16, (Actos relacionados con el Transporte de Mercancías), se describen y especifican los diversos actos regulados por dicho capítulo, que pudieran haber sido registrados en fragmentos separados de documentos escritos a medida que la mercancía es procesada para su transporte. Esto es necesario para asegurar un tratamiento similar a todos los mensajes de datos relacionados con el transporte, en lugar de sólo darle aceptación a los mensajes de actos importantes, teniendo que acudir a documentos escritos para los actos circunstanciales. Los actos se entienden aplicables a cualquier modo de transporte, y no sólo al marítimo.

El Artículo 17, (Documentos de Transporte), establece la singularidad del mensaje de datos, al señalar que cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o la utilización, de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos (artículo 17, inciso 3)).

Con sujeción a ese requisito de la singularidad, en los casos que la ley requiera que alguno de los actos enunciados en el artículo 16 se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos (artículo 17, inciso 1)).

En consecuencia, el requisito de la singularidad del mensaje de datos, es esencial para la transferabilidad de derechos a través de mensajes de datos, sin lo cual, las Reglas de París del CMI, o cualquier otro esquema voluntario para transferir derechos sobre las mercaderías no podría funcionar. Por ello, la adopción de la Ley Modelo, conteniendo tales provisiones, podría servir para validar esas reglas voluntarias, siendo un elemento importante para su desarrollo.

El párrafo 17 inciso 4), hace referencia a la manera de valorar del nivel de fiabilidad requerido para el reconocimiento de tales mensajes de datos, mientras el párrafo 17 inciso 5) reconoce que, mientras existen instancias donde las partes tienen que volver a los conocimientos de embarque por escrito o que consten en un papel, ambos sistemas no pueden ser usados al mismo tiempo, de lo contrario la singularidad podría ser destruida. Consecuentemente, antes de que un conocimiento de embarque por escrito o que consten de papel pueda ser emitido, el uso de los mensajes de datos debe ser terminado y tal hecho registrado en el conocimiento de embarque escrito en papel que se emita.

El párrafo 17 inciso 6), asegura que si una convención sobre responsabilidad del transportista de mercaderías por agua, rige obligatoriamente un conocimiento de embarque por escrito o que consten de papel, al contrato de transporte creado por el mensaje de datos, no dejará de aplicarse dicha convención.

2.6.3 Resumen de la Ley Modelo de la CNUDMI para las Firmas Electrónicas

La nueva Ley Modelo fue preparada partiendo del supuesto de que debería derivarse directamente del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y considerarse como una forma de proporcionar información detallada sobre el concepto del “método fiable para identificar” a una persona y “para indicar que esa persona aprueba” la información que figura en el mensaje de datos”.

Los artículos 1 y 2 se refieren al ámbito de aplicación y a definiciones de conceptos. Se trata de abarcar todas las situaciones de hecho en que se utilizan firmas electrónicas, independientemente del tipo de firma electrónica o de técnica de autenticación que se aplique. Establece el ámbito de aplicación de la ley a las actividades comerciales, incluyendo una lista de estas actividades. Y define los conceptos de: firma electrónica, certificado, mensaje de datos, firmante, prestador de servicios de certificación, parte que confía.

El artículo 3 da igualdad de tratamiento a las diferentes tecnologías para la creación de la firma electrónica, enuncia el principio fundamental de que ningún método de firma

electrónica puede ser objeto de discriminación, es decir, que debe darse a todas las tecnologías la misma oportunidad de satisfacer los requisitos del artículo 6 sobre cumplimiento de la firma. En consecuencia, no debe haber diferencias de tratamiento entre los mensajes firmados electrónicamente y los documentos de papel con firmas manuscritas, ni entre diversos mensajes firmados electrónicamente, siempre y cuando cumplan los requisitos básicos enunciados en el párrafo 1) del artículo 6 de la Ley Modelo o cualquier otro requisito enunciado en el derecho aplicable.

El artículo 4 indica que esta Ley debe interpretarse tomando en cuenta su naturaleza de origen internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe. Lo que no se encuentre expresamente será dirimidas de conformidad con los principios generales en que se inspira. Este artículo tiene la finalidad de dar orientación a los tribunales arbitrales y ordinarios y a otras autoridades administrativas nacionales o locales en la interpretación de la Ley Modelo. Entre los principios generales están: 1) facilitar el comercio electrónico entre los países y en los países; 2) validar operaciones concertadas mediante nuevas tecnologías de información; 3) promover y alentar de forma neutral respecto de la tecnología la aplicación de nuevas tecnologías de información en general y de las firmas electrónicas en particular; 4) promover la uniformidad del derecho; y 5) apoyar la práctica comercial.

El artículo 5 sobre modificación mediante acuerdo permite hacer excepciones a la presente Ley o modificar sus efectos mediante acuerdo. Esto con el fin de apoyar el principio de la autonomía de la voluntad de las partes. No debe interpretarse este artículo en el sentido de que permita a las partes apartarse de las reglas imperativas, como por ejemplo las reglas adoptadas por razones de orden público.

Los artículos 6, 7 y 8 se refieren al cumplimiento del requisito de firma y la responsabilidad del proceder del firmante. Estos artículos dan orientación sobre el modo en que puede satisfacerse el criterio de fiabilidad de la firma electrónica, y el que esta firma tenga las mismas consecuencias jurídicas que la firma manuscrita. Describe que el Estado promulgante puede designar un órgano o una autoridad confiriéndole la facultad para determinar qué tecnologías específicas pueden beneficiarse de las presunciones o de la regla de fondo que establece el artículo 6, al establecer o

reconocer la entidad que puede validar el uso de firmas electrónicas o certificar su calidad. Por último, se establece un código de conducta mínimo para el firmante. Las consecuencias del incumplimiento de ese código de conducta se dejan en manos del derecho aplicable al margen de la Ley Modelo.

Los artículos 9 y 10 se refieren a las responsabilidades del prestador de servicios de certificación y los elementos para que se consideren fiables estos servicios. Establece el código de conducta mínimo para el prestador de servicios de certificación. Presenta una lista no exhaustiva de factores que deben tenerse en cuenta para determinar la fiabilidad de los sistemas, procedimientos y recursos humanos.

El artículo 11 se refiere al proceder de la parte que confía en el certificado. Establece las medidas que debe tomar la parte que confía en el certificado, como verificar la fiabilidad de la firma electrónica, verificar la validez del certificado. Conviene recordar que la Ley Modelo no deroga ninguna norma que rija la protección del consumidor.

Sin embargo, la Ley Modelo puede ser de utilidad al informar a todas las partes interesadas, incluidas las partes que confían en firmas, sobre la norma de la conducta razonable que debe observarse con respecto a las firmas electrónicas.

Artículo 12 reconoce los certificados y firmas electrónicas provenientes del extranjero. La determinación de si un certificado o una firma electrónica es jurídicamente eficaz, o en qué medida lo es, no debe depender del lugar en el que se expidió el certificado o la firma. Se establece un umbral de equivalencia técnica de los certificados y firmas electrónicas extranjeros basado en contrastar su fiabilidad con los requisitos de fiabilidad establecidos por el Estado promulgante de conformidad con la Ley Modelo.

Capítulo 3. Marco Metodológico

3.1 Tipo de investigación

La investigación es de tipo cualitativa, puesto que se pretende analizar la legislación costarricense con el fin de identificar sus debilidades para regular las transacciones comerciales electrónicas. Es también de tipo comparativa porque plantea analizar las experiencias latinoamericanas en esta materia y las exigencias a nivel internacional con el fin de establecer semejanzas y diferencias entre ellas y con la legislación costarricense. El método comparativo es posible para el análisis de un número reducido de casos (Lijphart, 1971) para confrontar una cosa con otra, con el fin de poner de manifiesto sus diferencias recíprocas; de ese modo se prepara el esquema para interpretar lo que se analizará (Sartori y Morlino, 1994). Siguiendo a Sartori y Morlino (1994), para realizar comparaciones se deben tener atributos compartidos; por lo tanto, una vez establecidos los atributos de los asuntos a comparar, se adopta una estrategia comparativa: la búsqueda de diferencias o similitudes entre sí. Es decir, es necesario construir variables comparativas que sean aplicables a más de un país que permitan el uso de indicadores similares en las unidades escogidas.
En este sentido, la investigación realizará la comparación de las legislaciones de los países Chile, Colombia, Perú, Ecuador, México y Costa Rica. Además los contrastará con las disposiciones establecidas por los organismos internacionales para identificar vacíos jurídicos con relación al comercio electrónico.

La investigación que se propone utilizaría también el método hermenéutico debido a sus características. La hermenéutica tiene como propósito básico proveer los medios para alcanzar la interpretación del objeto o escritura. De acuerdo con Telmo (2007), es aquella capacidad de las personas de brindar o captar significados, y en el caso de los documentos escritos, se requiere de normas para que faciliten la labor de interpretación. De acuerdo con Telmo (2007), el hermeneuta interpreta el sentido de las leyes aplicando algunos principios de esta, como son: las condiciones que rodearon la

creación de la norma, intención del legislador, el significado de las palabras en el texto legal entre otros.

La investigación es hermenéutica pues requiere de la comprensión e interpretación de los datos y documentos en su dimensión conceptual, contextual e histórica:

- Conceptual: Es importante conocer los conceptos en los cuales se basan los datos o documentos que se investigarán, puesto que un significado puede tener conceptos diferentes según el individuo que las interpreta. En este caso, se debe comprender los conceptos que están plasmados detrás de los datos o documentos para poder tener una comprensión e interpretación lo más exacta posible de la realidad que representan.
- contextual: los datos pertenecen a personas y las acciones humanas tienen una explicación en la vida social, así como en la historia personal de cada ser humano. Las personas tienen su postura ideológica y del rol que desempeñaron cuando plasmaron el texto de los documentos que se investigarán.
- Histórica: El papel de la cultura, costumbres, la situación histórica del país en el momento en que se escribieron los documentos o se obtuvieron los datos es importante, puesto que todas estas características cambian con el tiempo, deben comprenderse los datos en su dimensión histórica.

“La investigación teórica es la construcción de una teoría o parte de la misma; pero también lo es el reconstruirla, reestructurarla, reformularla, remodelarla, fundamentarla, integrarla, ampliarla o desarrollarla.” (UNED, 2004).

Es una investigación teórica cualitativa y comparativa de tipo mayormente hermenéutico. La investigación que se propone tratará de analizar y comparar las experiencias, de tipo legislativo y documental, existentes en otros países latinoamericanos en materia de regulación del comercio electrónico, se tratará de comprender e interpretar lo que esas experiencias intentaron regular, y de analizar y comprender la situación actual, los requerimientos a nivel internacional que se están exigiendo en esta materia, y conceptualizar, contextualizar y proponer lineamientos para una adecuada regulación para Costa Rica que permita promover el comercio electrónico. Es posible que para una mejor interpretación y comprensión de los

documentos escritos se tenga que recurrir a las entrevistas en profundidad con expertos en la materia a nivel costarricense, y no se descarta también a expertos de otros países latinoamericanos, como se indicó anteriormente. Se toma las experiencias a nivel latinoamericano debido a su similitud en las condiciones sociales, culturales y económicas con nuestro país.

El trabajo tratará de analizar lo que ya existe y a partir del conocimiento previo de otros países, de la situación propia de nuestro país y del mundo actual, determinar las lagunas de la legislación costarricense para regular el comercio electrónico.

También es importante observar aquí, el hecho de utilizar como base del conocimiento las experiencias de otros países, esto enriquece aún más la investigación, puesto que ya se tiene resultados de esas experiencias que pueden ser aprovechadas para el análisis de la situación de Costa Rica. En este sentido, puede hablarse del círculo hermenéutico, es decir, se presume que "... no puede darse algún desarrollo de conocimiento sin algún conocimiento previo, nuestro conocimiento del todo es corregido continuamente y profundizado por el crecimiento en nuestro conocimiento de los componentes". (UNED, 2004)

Esta investigación aprovechará entonces los principios de la hermenéutica para obtener una clara y precisa comprensión de las legislaciones existentes en otros países, y para comprender la situación del país acerca de las transacciones comerciales electrónicas. Tratará de comprender el texto escrito de las leyes existentes en otros países y se interpretará y adaptará para la situación costarricense y según las exigencias internacionales al respecto.

Por lo tanto, la hermenéutica tiene la ventaja de reunir las características necesarias para realizar el trabajo propuesto, puesto que se tratará de comprender e interpretar los conceptos, el contexto y la situación histórica de lo que existe en materia de regulación de transacciones comerciales electrónicas en Costa Rica, en otros países, y cuáles son las exigencias actuales mundiales en esta materia.

Como puede verse, claramente tendrá la limitación basada principalmente en el nivel de interpretación que se lleve a cabo así como la amplitud de los delitos que se abarquen.

La interpretación se realizará con base al conocimiento que la investigadora tiene acerca del comercio electrónico y el vacío existente en la legislación costarricense para regular este tipo de transacciones, así como el conocimiento que pueda adquirirse del análisis de las legislaciones de otros países.

La amplitud de los delitos que pueden llevarse a cabo con la apertura comercial electrónica es enorme, por tal motivo, ésta estará limitada a clarificar los relacionados con la contratación vía Internet, la privacidad, seguridad, y los derechos de los consumidores.

3.2 Sujetos y fuentes de información

El único participante de esta investigación es quien suscribe.

Utilizará fuentes secundarias principalmente, dada su naturaleza principalmente documental.

Se hará una búsqueda de información en fuentes secundarias con el fin de conocer la situación actual del comercio electrónico de Costa Rica.

También se hará una revisión de las leyes existentes que regulan las transacciones comerciales electrónicas en Costa Rica.

Y por último se hará una revisión de otras experiencias latinoamericanas en esta materia, al igual que los requerimientos que se están exigiendo a nivel internacional.

No se descarta la posibilidad de realizar entrevistas en profundidad a expertos en la materia a nivel nacional e internacional.

3.3. Análisis de la información

Para llevar a cabo el trabajo se propone realizar las actividades que a continuación se detallan.

3.3.1 Actividades

En primer término, se efectuará un análisis exhaustivo de la legislación comparada estableciendo un criterio clasificatorio de la misma en atención a la problemática planteada, e identificar las tendencias legislativas, los aciertos, las necesidades, los elementos técnicos y lo pendiente.

Se clasificará la totalidad de la normativa en atención a la procedencia de organizaciones supranacionales. En este sentido se analizarán las Leyes Modelos de la UNCITRAL, la Directiva de la Unión Europea sobre Comercio Electrónico, las Disposiciones de la Organización Mundial de Comercio (OMC) y, las Recomendaciones de la Organización de Cooperación y Desarrollo Económico (OCDE). No se descarta la posibilidad de entrevistas a profundidad con expertos en la materia.

También se verificará si los textos normativos configuran la categoría de “sancionados” o “proyectos”. Conjugando entonces ambos criterios de análisis se revisará los cuerpos normativos extranjeros, de países latinoamericanos: Chile, México, Ecuador, Perú, Colombia. Estos países se han escogido por cuanto han iniciado cambios legislativos conducentes a promover el comercio electrónico en América Latina, además de que ofrecen estándares de desarrollo económico y de competitividad que son de interés para esta investigación.

Se estudiarán los aportes de los doctrinistas nacionales e internacionales y se revisarán las indicaciones de la jurisprudencia.

Por último, se realizará un estudio de la legislación costarricense teniendo en cuenta las áreas legisladas para detectar posteriormente los núcleos “débiles” tales como

inconsistencias, redundancias y lagunas normativas y, con idéntico criterio se analizará los proyectos en discusión en la Asamblea Legislativa, si los hubiere. Para esto se considerará la problemática jurídica planteada en el Marco Teórico.

Se desarrollará una matriz comparativa con los aspectos de una legislación modelo y la legislación vigente o proyectada en Costa Rica.

Como esfuerzo metodológico dentro de la ciencia del derecho, resulta interesante acotar que este trabajo inicia con una revisión legislativa internacional y nacional, compara esas legislaciones y deduce aportes dogmáticos a la regulación del comercio electrónico. Gracias a ello será posible trabajar las lagunas normativas y definir las tendencias de desarrollo en la temática.

Junto a ello, debe tenerse en cuenta el cambiante horizonte de la legislación y la doctrina, lo que obligaría a construir una matriz comparativa que refleje los cambios y las tendencias actuales y futuras.

Las conclusiones de estas observaciones serán por supuesto traducidas de nuevo en un modelo de legislación que permita el equilibrio entre los aportes de las TIC's y los cánones jurídicos.

En síntesis, el criterio metodológico consiste en el análisis cualitativo, comparativo y hermenéutico, de las recomendaciones emergentes de la legislación comparada y el estudio de las necesidades reales, a fin de valorar las condiciones legislativas costarricense para promover el comercio electrónico, esto permitirá identificar los vacíos jurídicos normativos y un conjunto de medidas o líneas de acción oportunas y estratégicas para el desarrollo de las nuevas tecnologías.

Se trata de lograr un equilibrio entre el grado de seguridad (técnica y jurídica) exigible y la flexibilidad que demanda la nueva realidad de comunicación con desarrollos tecnológicamente variables y, la adopción de patrones y estándares universales.

En el análisis de la información no se aplicarán medios estadísticos.

3.3.2 Principales modelos en atención a la legislación comparada

Los principales “modelos” de legislación comparada son los que a continuación se mencionan: la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL en sus siglas en inglés), aprobada en Nueva York en 1996.

La Directiva de la Unión Europea sobre Comercio Electrónico, elaborada en 1997 por la Comisión Europea y presentada a los organismos comunitarios competentes a través de una comunicación dirigida a promover un sistema europeo de comercio electrónico. Esta directiva se complementa con otra que establece la prohibición de transferencia de datos personales a países que no tengan un nivel adecuado de protección de la privacidad.

Asimismo, las leyes y directivas mencionadas se complementan con las Disposiciones de la Organización Mundial de Comercio (OMC) y las Recomendaciones de la Organización de Cooperación y Desarrollo Económico (OCDE), entre otros organismos internacionales, en el tratamiento específico de la temática de referencia.

3.4 Diseño de instrumentos

En la investigación cualitativa se dispone de otra fuente muy importante de información, además de los propios sujetos o individuos; esta es la que aporta los documentos escritos, que abarcan gran variedad de modalidades como: documentos oficiales y personales, comunicaciones, libros, artículos, documentos de trabajo, actas, documentos de organizaciones, cartas, etc.

El análisis de documentos es una fuente de gran utilidad para obtener información retrospectiva acerca de un fenómeno, situación o programa y, en ocasiones, la única fuente para acceder a una determinada información. Para el presente trabajo, los

principales documentos que se utilizarán son los textos de las leyes, normas y directivas comunitarias.

A continuación se diseñan algunos instrumentos para organizar la información que permitan facilitar el análisis del contenido de los documentos.

3.4.1 Cuadro comparativo de la situación legislativa latinoamericana

Se diseña el siguiente cuadro para concentrar la información sobre la situación legislativa acerca del comercio electrónico de los distintos países a analizar. Se trata de dar un panorama general de la situación latinoamericana a través de este cuadro.

País	**Síntesis situación general del país sobre la regulación del comercio electrónico**	**Comentarios**
País 1		
País 2		
País 3		

3.4.2 Cuadro comparativo de la situación legislativa costarricense acerca del comercio electrónico y los requerimientos a nivel internacional (establecidos por la UNCITRAL)

El siguiente cuadro permitirá comparar la legislación costarricense contra los requerimientos establecidos por organismos internacionales. Esto permitirá conocer si la legislación costarricense cumple con las recomendaciones dictadas por los organismos internacionales.

Costa Rica	**UNCITRAL**	**OMC**	**OCDE**	**UE**

3.4.3 Cuadro para el análisis de la problemática jurídica planteada y la legislación actual costarricense

Para analizar la cobertura que tiene la legislación actual costarricense para atender los problemas planteados de las transacciones comerciales electrónicas, se propone el siguiente instrumento.

Problema	Ley	Artículo	Análisis y comentarios

3.4.4 Cuadro para el análisis de la problemática jurídica planteada y otras legislaciones latinoamericanas

Con el fin de analizar cómo otros países han resuelto los problemas planteados del comercio electrónico, se propone el siguiente instrumento. Esto permitirá también conocer las tendencias legislativas en la materia, así como necesidades y oportunidades que pueden ser aprovechadas para Costa Rica:

Problema	País 1	País 2	País 3

3.4.5 Cuadro para el análisis de la problemática jurídica planteada y las propuestas de organismos internacionales, jurisprudencia, aportes de doctrinistas

Similarmente, para analizar las propuestas de organismos internacionales para solucionar la problemática planteada se propone el siguiente instrumento:

Problema	ORGANISMO INTERNACIONAL 1	ORGANISMO INTERNACIONAL 2

Para analizar la jurisprudencia y aportes de doctrinistas en relación a la problemática planteada se propone el siguiente instrumento:

Problema	jurisprudencica	Aportes de doctrinistas

Todos los instrumentos propuestos tienen como fin ayudar al investigador a ordenar los datos para su interpretación y análisis posterior.

Es importante revisar la situación del país de acuerdo con los nuevos escenarios, más específicamente lo relacionado con el Tratado de Libre Comercio, nuevos mercados, competencia, entre otros. En este sentido, se plantea el siguiente instrumento para identificar la problemática que se plantea en este tema:

Problema	Necesidad	Solución

3.4.6 Entrevistas a profundidad

Se diseñará las entrevistas a expertos en la materia, con el fin de validar la información obtenida en los documentos y experiencias latinoamericanas. La idea es lograr mantener una conversación con el experto que le permita desarrollar el tema sin limitaciones de tiempo ni de temática. Sin embargo, la conversación debe ser dirigida para obtener la información que se busca. Por lo tanto, se propone que las entrevistas contengan al menos los siguientes elementos:

Nombre del experto entrevistado.
Currículum del experto.
Nacionalidad.
Comentarios de su experiencia en el campo de la regulación del comercio electrónico.
Comentarios sobre las leyes modelos u otras propuestas internacionales.
Elementos que considera que hace falta cubrir en las regulaciones existentes.

Elementos necesarios que considera que la legislación costarricense debe tomar en cuenta.
Problemas no resueltos y su propuesta de solución.
Otros aspectos importantes que el experto considere pertinentes.

3.5 Alcances y limitaciones

La investigación tendrá como ámbito de estudio la situación legal del comercio electrónico en Costa Rica y los requerimientos internacionales al respecto. El análisis se centrará en los núcleos jurídicos problemáticos relacionados con el comercio electrónico desarrollados en el marco teórico, se analizará la problemática jurídica de los siguientes aspectos: la contratación vía Internet, derechos del consumidor, privacidad y seguridad de las transacciones. Se analiza sólo las compras y ventas establecidas por un consumidor con una empresa (B2C) y a través de página Web.

En lo referente al tratamiento de los delitos informáticos, se delimita el trabajo a analizar únicamente los delitos relacionados con la privacidad y seguridad en el comercio electrónico y con relación al consumidor.

Los instrumentos de recolección de datos son ayudas para organizar la información y poder lograr un orden de análisis de ésta. No se descarta la posibilidad de que se requiera otros instrumentos, según se avance en la investigación, o la modificación de los instrumentos propuestos.

3.6 Proyecciones

Los resultados de este estudio servirán de base para que posteriores estudios amplíen los aspectos que se detecten y que requieran un tratamiento legislativo más comprensivo en relación con la regulación del comercio electrónico en el país.

Capítulo 4. Seguridad jurídica y tecnológica del comercio electrónico

En un principio el desarrollo de Internet se produjo en forma libre y sin regulación alguna, la aparición del comercio como elemento principal de las operaciones en la red ha hecho necesaria una regulación que permita otorgar ciertas seguridades en relación a una serie de elementos que deben encontrarse presentes en la actividad económica electrónica para evitar abusos y conflictos que puedan darse en este tipo de transacciones.

Esta parte de la investigación se centrará en el análisis de la situación de la seguridad del comercio electrónico desde dos aspectos: la seguridad jurídica y la seguridad tecnológica.

La primera parte analiza el aspecto de seguridad jurídica relacionado con los documentos electrónicos o mensajes de datos, certificados y firmas digitales. Presenta el trabajo de los Organismos Internacionales y hace un análisis comparativo de las legislaciones de: Chile, Colombia, Costa Rica, Ecuador, México y Perú.

La segunda parte hace una breve reseña de los aspectos tecnológicos relacionados con el sistema de seguridad utilizado: criptografía asimétrica, certificados y firmas digitales; y se refiere al aspecto de la prueba documental electrónica.

4.1 Seguridad jurídica del comercio electrónico

Este apartado analiza la situación del comercio electrónico desde los elementos de seguridad jurídica necesarios para permitir que el usuario utilice este tipo de transacciones con toda confianza.

Un principio fundamental sobre el que descansa el comercio es la confianza entre las partes. Esto es uno de los motivos que lleva a las personas a celebrar un negocio. En el comercio electrónico este principio se mantiene, ya que mientras mayor sea la confianza en las transacciones electrónicas, mayor será la utilización de esta forma de comercio.

Moreno (2002) indica que:

> "la seguridad jurídica en el comercio electrónico es el tema que más ha preocupado desde su comienzo. La falta de presencia física simultánea de los contratantes es una circunstancia que no genera la confianza necesaria en las partes, sobre todo si una de ellas -el consumidor- está en posición teórica desigual respecto a la otra. Por este motivo han sido muchos los esfuerzos normativos tanto de organizaciones supranacionales como nacionales para conseguir un entorno o un medio electrónico seguro que genere la suficiente confianza para un desarrollo óptimo en el futuro del comercio electrónico, pues es fundamental garantizar la seguridad jurídica de los destinatarios, consumidores o usuarios mediante el establecimiento de un marco jurídico claro y de carácter general para determinados aspectos de las transacciones electrónicas." (Moreno, 2002, p.131).

El contrato electrónico se caracteriza por la forma en que se produce la concurrencia de la oferta y de la aceptación, la confianza necesaria y la seguridad jurídica se concretan en la prueba de la forma de exteriorizar la voluntad, en la acreditación de las partes o autoría y en el contenido contractual. La prueba de todas estas circunstancias se logra mediante el documento y la firma, en este caso, mediante el documento y la firma "electrónica" (Moreno, 2002).

En este sentido, y con relación al aspecto de seguridad jurídica, los distintos países han venido discutiendo a nivel interno e internacional la creación de normas mínimas lo más homogéneas posibles que permitan asegurar que no se negará la existencia ni la validez de un documento encriptado o firmado digitalmente con el fin de dar la seguridad jurídica necesaria a todas las actividades en la red.

La primera parte de este capítulo revisa el trabajo de Organismos Internacionales con relación a la temática de comercio electrónico y firmas digitales, después se hace un análisis comparativo de la normativa de los países: Chile, Colombia, Costa Rica, Ecuador, México y Perú, con el fin de identificar semejanzas y diferencias. Y por último se analiza la Ley 8454 de Certificados, Firmas digitales y Documentos Electrónicos de Costa Rica, para determinar vacíos y necesidades.

4.1.1 Propuestas de Organismos Internacionales y Estados Unidos

A partir de 1995 diversos organismos ligados al derecho y a las Tecnologías de la Información (TI) empezaron a discutir el marco jurídico que permitiera contar con

tecnologías seguras para garantizar el desarrollo del comercio electrónico. Este tema ha sido tratado ampliamente a nivel internacional por varios organismos internacionales preocupados por su desarrollo. En el anexo 10 puede encontrar un resumen de los aspectos establecidos por estos organismos.

4.1.1.1 CNUDMI

Dentro de los organismos internacionales, se puede nombrar a la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI por sus siglas en español, o UNCITRAL por sus siglas en inglés).

Dicho organismo ha desarrollado una estructura legal modelo para que los países la adopten en sus legislaciones internas, de manera que el documento electrónico pase a ser considerado como un "equivalente" al documento tradicional en papel, partiendo de la base de que el documento electrónico puede ofrecer un grado de seguridad superior a la consignada en el soporte tradicional.

Los principios generales de la Ley Modelo de la CNUDMI incluyen aspectos mínimos que debe contemplar una legislación sobre el tema, a continuación se resume estos aspectos:

a- Definiciones técnicas: se establece definiciones de lo que se entiende por firma electrónica, certificado, mensaje de datos, firmante, prestador de servicios de certificación y parte que confía, en el artículo 2 de la Ley Modelo sobre Firmas Electrónicas.

b- Neutralidad Tecnológica: se refiere a que las legislaciones no estén atadas a una tecnología específica, establecida en el artículo 3 de la Ley Modelo sobre Firma Electrónica del 2001.

c- Equivalencia Funcional: se refiere a que se les asigne el mismo valor a los documentos y firmas electrónicas que a los equivalentes en papel, indicado en los

artículos 6, 7 y 8 de la ley modelo de Comercio Electrónico de las Naciones Unidas, CNUDMI de 1996.

d- Autonomía de la Voluntad: que las partes son soberanas para determinar las formas de actuar y de contratar electrónicamente, establecido en el artículo 4 de la Ley Modelo de Comercio Electrónico de 1996.

e- Condiciones de fiabilidad: La Ley Modelo sobre Firmas Electrónicas establece en el artículo 6 que la firma electrónica se considerará fiable si cumple las siguiente condiciones: 1) Datos de creación de la firma correspondientes al firmante en forma exclusiva, 2) Datos de creación de la firma estaba bajo control exclusivo del firmante en el momento de la firma, 3) Posibilidad de detectar cualquier alteración a la firma posterior al momento de la firma, 4) Posibilidad cierta de detectar cualquier alteración a la información posterior al momento de la firma. Se deja a salvo, tanto la posibilidad de demostrar, por otros medios, dicha fiabilidad, como la prueba en contrario de ella, e incluso la inaplicabilidad de todo el artículo a hipótesis a determinar en cada legislación.

f- Proceder del prestador de servicios de certificación: el artículo 9 de la Ley Modelo sobre Firmas Electrónicas establece una serie de cargas y obligaciones para estos sujetos que intervienen en la creación de las firmas electrónicas: actuar conforme declaraciones de normas y prácticas que haga; actuar con diligencia razonable para asegurar la veracidad y exactitud de las declaraciones que más importan al ciclo vital del certificado; dar medios razonablemente accesibles al tomador del certificado, para que determine, mediante el propio certificado, una serie de elementos esenciales (identidad del prestador del servicio, existencia de un control de datos de creación de firma por parte del firmante en el momento en que se expidiera el certificado, validez de dichos datos, etc.)

g- Reconocimiento de certificados y firmas electrónicas extranjeros: El artículo 12 de la Ley Modelo sobre Firmas Electrónicas establece la previsión de que todo certificado y firma electrónica, expedidos, creados o utilizados fuera del Estado, tengan los mismos

efectos que los expedidos, creados o utilizados dentro del Estado, siempre y cuando se observe un grado de fiabilidad sustancialmente equivalente de unos con otros.

4.1.1.2 Unión Europea

La Unión Europea ha dictado una directiva en la que establece un Marco Comunitario para la Firma Electrónica, la Directiva 1999/93/CE, del 13 de diciembre de 1999, sobre un Sistema Común para las Firmas Electrónicas. Esta normativa viene a regular la actividad de certificación y firma electrónica al interior de la comunidad.

Las disposiciones más importantes de la Directiva Europea se resumen en las siguientes líneas:

a- Constituye un marco jurídico homogéneo y adecuado para el uso de las firmas dentro de la comunidad.

b- La libertad contractual regula toda aplicación en entornos cerrados o redes locales.

c- Los prestatarios de servicios de certificación podrán ofrecer sus servicios sin la obligación de autorización previa.

d- Consagra un marco jurídico para todos los certificados y servicios que preste la entidad certificadora.

e- Validez e igualdad de la firma electrónica a la firma tradicional.

f- Permite a los prestatarios de servicios de certificación avalar los certificados de terceros países de la misma forma que garantizan a sus propios certificados.

g- Prohíbe limitar el número de entidades certificadoras.

h- Limita la utilización de los datos obtenidos. La difusión de datos personales debe ser autorizada por el titular de los mismos. Queda prohibido que los datos puedan obtenerse o tratarse con fines distintos sin el consentimiento de su titular.

i- Establece los requisitos de los certificados reconocidos y los requisitos de los proveedores de los servicios de certificación.

j- Consagra el principio de la buena fe: Los estados miembros deben velar por que el proveedor de los servicios de certificación, que emita un certificado reconocido, sea responsable ante cualquier persona que de buena fe confíe en el certificado, en relación a:

1) La exactitud de toda la información contenida en el certificado.
2) La conformidad de todos los requisitos que exige la ley.
3) La garantía de que, en el momento de la emisión del certificado reconocido, obra en poder del titular identificado en el mismo el dispositivo de creación de firma correspondiente al dispositivo de verificación dado o identificado en el certificado.

La principal disposición de la Directiva establece que la firma electrónica avanzada basada en un certificado reconocido equivale a una firma manuscrita y es admisible como prueba en procedimientos judiciales.

Sin embargo, se reconoce eficacia jurídica y probatoria a la firma electrónica aunque no sea avanzada, es decir, siempre que se base: en un certificado (aunque no sea reconocido), expedido por un prestador de servicios de certificación (aunque no sea acreditado), esté creada por un dispositivo de creación de firma (clave privada, aunque no sea seguro).

De esta forma, a la firma en su forma electrónica que no reúna todos los requisitos (existencia de un certificado reconocido emitido por un prestador de servicios de certificación acreditado y creada por un dispositivo seguro de creación de firma) no se le negarán efectos jurídicos ni será excluida como prueba en juicio (art. 5.2 de la Directiva 1999/93/CE, Unión Europea). Pero se recomienda a los Estados que procuren que la firma electrónica sea “avanzada”, basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma (art. 5.1 de la Directiva 1999/93/CE, Unión Europea).

También establece que los Estados miembros velarán por que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan lo establecido en las Directivas 95/46/CE y 97/66/CE sobre la protección de datos personales.

La Directiva Europea 2000/31/CE del 8 de Junio de 2000 sobre el comercio electrónico prevé que los Estados deben de vigilar que su sistema jurídico pueda hacer posible la

existencia de los contratos por vía electrónica. Esta recomendación va dirigida a que se reconozca el proceso contractual y que los contratos concluidos electrónicamente no sean privados de validez por este motivo. Además en su artículo 16 establece que los Estados miembros fomentarán la elaboración de códigos de conducta.

4.1.1.3 Estados Unidos

La primera ley en materia de Firma Digital en el mundo fue la denominada “Utah Digital Signature Act”, publicada en mayo de 1995 en el Estado de UTAH, en Estados Unidos.
Su objetivo es facilitar mediante mensajes electrónicos y firmas digitales las transacciones, procurar las transacciones seguras y la eliminación de fraudes y establecer normas uniformes relativas a la autenticación y confiabilidad de los mensajes de datos, en coordinación con otros Estados.
Su ámbito de aplicación son las transacciones mediante mensajes electrónicos, su confiabilidad, así como las firmas digitales.
Esta ley, define a la Firma Digital como la transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación.
Define el Criptosistema Asimétrico como aquel algoritmo o serie de algoritmos que brindan un par de claves confiables relacionadas matemáticamente, y con característica que el mensaje cifrado con una clave solo puede ser descifrado con la otra clave.
Define al Certificado, como aquel registro basado en la computadora que identifica a la autoridad certificante que lo emite; nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite.
En cuanto a la Supervisión y al control, estos recaen sobre la División, quien actúa como autoridad certificadora. También formula políticas para la adopción de las tecnologías de firma digital y realiza una labor de supervisión.
La emisión de los certificados corre a cargo de la autoridad certificadora que ha sido acreditada.

Se equipara el valor probatorio de un mensaje de datos con el de papel siempre y cuando contenga una firma digital confirmada mediante la clave pública contenida en un certificado que haya sido emitida por una autoridad certificadora.
No se contempla el reconocimiento de certificados extranjeros, solo se menciona que la División puede reconocer la autorización emitida por Autoridades Certificadoras de otros Estados.
Esta Ley no contempla sanciones**.**
El Comité de Seguridad de la Información, de la División de Comercio Electrónico, de la American Bar Association (ABA), emitió, en agosto de 1996, la "Guía de Firmas Digitales". En la redacción de esta Normativa participaron casi ochenta profesionales de las disciplinas del derecho, la informática y la criptografía de los sectores público y privado, en la que específica un mecanismo de firma digital a base de criptografía asimétrica, los certificados de clave pública y los certificadores de clave pública.

El 15 de agosto de 1997, la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme (NCCSL), elaboró la "Uniform Electronic Transactions Act" (UETA), la cual se aprobó el 30 de julio de 1999.

El 4 de agosto del 2000 se aprobó la "Uniform Computer Information Transactions Act" (UCITA), la cual se encuentra en proceso de adopción por los diversos Estados de la Unión Americana.

El 24 de enero de 2000 el Congreso de los Estados Unidos aprobó la "Electronic Signatures in Global and National Commerce Act" (Ley de Comercio Electrónico y Firma Electrónica para el Comercio Nacional e Internacional). El 30 de junio el 2000 la presidencia emite la "Electronic Signatures in Global and National Commerce Act" (E-Sign Act.) vigente a partir del 1 de octubre del 2000 (otorgando a la firma y documento electrónico un estatus legal equivalente a la firma autógrafa y al documento en papel).

Es una norma federal que regula las actividades comerciales entre los estados y a nivel internacional y establece principios generales. Cada estado debe dictar sus propias normas particulares específicas.

Lo más importante es que establece una regla de validez para todos los actos o transacciones celebrados por medios electrónicos, igualando los documentos en formato papel a los documentos en formato digital.

La norma general consagrada establece que ningún estatuto, regulación o principio de derecho que afecte o sea aplicable al comercio entre estados o internacional podrá negar efecto legal, validez o fuerza legal a alguna transacción o contrato por el solo hecho de que éste tenga forma electrónica.

4.1.1.4 OCDE

En marzo de 1997, la Organización para la Cooperación y el Desarrollo Económico publicó su recomendación para el establecimiento de políticas sobre Criptografía, sin embargo solo establece una serie de lineamientos que se sugiere a los gobiernos adoptar al momento de legislar en materia de firma digital y de Entidades Prestadoras de Servicios de Certificación: promover el uso de la criptografía para favorecer la confianza en las redes y sistemas de información y garantizar la seguridad de los datos y la protección a la vida privada; promover el uso de la criptografía sin poner el riesgo a la seguridad pública, a la seguridad nacional y a las leyes; concienciar sobre la necesidad de contar con una política y una legislación en materia de criptografía; ayudar a los responsables de la toma de decisiones de los sectores público y privado a elaborar e implementar políticas, métodos y procedimientos coherentes; promover la cooperación internacional para lograr un uso concertado de los métodos criptográficos (DCSSI, 2004).

Luego en el 2002 la OCDE adoptó directrices para la seguridad de los sistemas y redes de información. Estas Directrices constituyen una base de trabajo fundamental hacia una cultura de seguridad para toda la sociedad. Ello permitirá que los participantes consideren la seguridad en el diseño y uso de los sistemas y de las redes de información. Asimismo, estas directrices proponen que todos los participantes adopten y

promuevan una cultura de seguridad como modo de pensar, así como de evaluar y actuar en los sistemas y redes de información.

Estas directrices se presentan como nueve principios complementarios entre sí (DCSSI, 2004):

- Concienciación: Las partes involucradas deben ser concientes de la necesidad de garantizar la seguridad de los sistemas y redes de información y de las acciones que pueden emprenderse para reforzar la seguridad.
- Responsabilidad: Las partes son responsables de la seguridad de los sistemas y redes de información.
- Reacción: Las partes involucradas deben actuar rápidamente y con espíritu de colaboración para prevenir, detectar y dar respuesta a los incidentes de seguridad.
- Ética: Cada una de las partes involucradas deben respetar los intereses legítimos de las demás partes involucradas.
- Democracia: La seguridad de los sistemas y redes de información deben ser compatibles con los valores fundamentales de una sociedad democrática.
- Evaluación de los riesgos: Las partes involucradas deben hacer evaluaciones de los riesgos.
- Diseño e implementación de la seguridad: Las partes involucradas deben integrar la seguridad como un elemento esencial de los sistemas y redes de información.
- Gestión de la seguridad: Las partes involucradas deben adoptar un enfoque global de la gestión de la seguridad.
- Reevaluación: Las partes involucradas debe examinar y reevaluar la seguridad de los sistemas y redes de información e introducir las modificaciones apropiadas en sus políticas, prácticas, medidas y procedimientos de seguridad.

4.1.2 Análisis de legislación comparada sobre comercio electrónico y firma digital: Chile, Colombia, Costa Rica, Ecuador, México y Perú.

En Latinoamérica, casi todos los países se encuentran discutiendo o han promulgado normas legales que regulan estas materias. Todas estas normas pretenden dar regulación a los nuevos servicios que se generan a raíz de la instauración de la Firma

electrónica, y en mayor o menor medida recoge las disposiciones al respecto emanadas de la CNUDMI, de la directiva de la Unión Europea y de la Ley de Utah de Estados Unidos. El anexo 4 se muestra un resumen de la normativa de comercio electrónico de los países analizados en esta investigación: Chile, Colombia, Costa Rica, Ecuador, México y Perú.

Esta parte del trabajo realiza una comparación de las disposiciones de la normativa vigente sobre comercio electrónico de los países en estudio. Se identifica cuáles son las semejanzas y diferencias entre las mismas y se hace mención de las normas legales adoptadas de acuerdo con los lineamientos de las leyes modelo sobre comercio electrónico y firma electrónica de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL), con el fin de identificar aspectos de la normativa que tienen los otros países y determinar las necesidades en relación con el marco jurídico actual.

Se identifica los siguientes aspectos regulados en las legislaciones, los cuales serán un marco para realizar el análisis, en el anexo 5 se encuentra los artículos de las normativas de los países analizados:

1. Objeto y Ámbito de aplicación
2. Reconocimiento jurídico. Validez.
   a. Definición de mensajes de datos
   b. Definición de firma electrónica o digital
3. Fuerza probatoria.
4. Equivalencia funcional.
5. Neutralidad tecnológica.
6. Autonomía de la voluntad.
7. Compatibilidad internacional.
8. Disposiciones supletorias.
9. Otros asuntos.

4.1.2.1 Objeto y Ámbito de aplicación

Ley Modelo CNUDMI sobre Comercio Electrónico: art. 1.

> "La presente Ley** será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto*** de actividades comerciales ****.
> *La Comisión sugiere el siguiente texto para los Estados que deseen limitar el ámbito de aplicación de la presente Ley a los mensajes de datos internacionales:
> La presente Ley será aplicable a todo mensaje de datos que sea conforme a la definición del párrafo 1) del artículo 2 y que se refiera al comercio internacional.
> **La presente ley no deroga ninguna norma jurídica destinada a la protección del consumidor.
> ***La Comisión sugiere el siguiente texto para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:
> La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en las situaciones siguientes: [...].
> ****El término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de facturaje *(factoring);* de arrendamiento de bienes de equipo con opción de compra *(leasing);* de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera." (CNUDMI, 1999, p.3)

Ley Modelo CNUDMI para Firma Electrónica:

> "Artículo 1. Ámbito de aplicación
> La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No derogará ninguna norma jurídica destinada a la protección del consumidor." (CNUDMI, 2002, p.10)

Análisis

Solo Colombia sigue el texto de la Ley Modelo sobre Comercio Electrónico, adicionando la inclusión de algunas excepciones. La Ley 527 de Colombia no indica nada con respecto a las firmas electrónicas dentro de su ámbito de aplicación (articulo 1 Ley 527).

La Ley 67 de Ecuador incluye en el ámbito de aplicación, además de los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos y la protección a los usuarios (Artículo 1 Ley 67).

Perú del todo no tiene una Ley o Proyecto que incluya el concepto de mensajes de datos, pero en el Reglamento de la Ley, sí hace referencia a este término. El Reglamento regula la utilización de firmas electrónicas en mensajes de datos y documentos electrónicos, además establece reglas en materia probatoria para los mensajes firmados electrónicamente.

La Ley 19799 de Chile se refiere a documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso (artículo 1 Ley 19799).

México indica que las disposiciones del Decreto sobre Firma Electrónica regirán para todos los asuntos de orden comercial de la República Mexicana (Artículo 89 del Decreto sobre Firma Electrónica de México).

Costa Rica incluye dentro del ámbito de la Ley toda clase de transacciones y actos jurídicos, públicos y privados (Artículo 1 Ley 8454). No hace referencia al término de mensaje de datos.

Es importante recalcar que la CNUDMI ha hecho un enorme esfuerzo y ha trabajado durante muchos años para ofrecer una Ley Modelo sobre Comercio Electrónico, con el fin de dar una guía a los países que les permita promulgar sus propias leyes en esta materia.

La propuesta de la CNUDMI solo ha sido acogida por Colombia, los otros países tomaron algunos elementos e hicieron su propia redacción de la normativa.

Es importante analizar la conveniencia de tener la misma normativa que regule los asuntos de comercio electrónico, para estandarizar todos los elementos involucrados en las legislaciones de los países, facilitar y dar confianza a los usuarios de usar el medio electrónico para sus transacciones comerciales.

Una diversidad de normas, no permite dar confianza y seguridad jurídica a las partes involucradas en una transacción, precisamente porque no permite estandarizar el tratamiento que pueda darse a una misma situación en distintos países, debido que al tener una diversidad de redacción promueve diferentes interpretaciones jurídicas con respecto a una misma situación que no es conveniente para el usuario o consumidor.

4.1.2.2 Reconocimiento jurídico

Este principio permite reconocer jurídicamente a los mensajes de datos y la firma electrónica dándoles el mismo valor como los documentos y firmas tradicionales.

Ley Modelo CNUDMI sobre Comercio Electrónico:

> "Artículo 5. — Reconocimiento jurídico de los mensajes de datos
> No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos." (CNUDMI, 1999, p.5)

Ley Modelo CNUDMI para Firma Electrónica:

Artículo 6. Cumplimiento del requisito de firma

> "1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje." (CNUDMI, 2002, p.11)

Análisis

Colombia (artículo 5 de la Ley 527) y México (artículo 89 bis del Decreto sobre firma electrónica) tiene el mismo texto donde expresamente se reconoce jurídicamente a los mensajes de datos y basado completamente en la Ley Modelo de la CNUDMI. Relacionado con la firma, el texto de Colombia (artículos 10 y 28 de la Ley 527) y México (artículo 97 del Decreto sobre firma electrónica) es similar con una diferencia mínima pero que al final se interpreta el mismo significado.

Chile expresa el reconocimiento jurídico de los actos y contratos celebrados por personas naturales o jurídicas suscritos por firma electrónica, igual que los celebrados

por escrito en soporte de papel (artículos 3, 5 de la Ley 19799). Su redacción difiere a la de la Ley Modelo.

Ecuador reconoce la validez y eficacia jurídica de los mensajes de datos y de la firma electrónica separándolo en dos articulados. Lo referente al reconocimiento jurídico de los mensajes de datos, el texto es igual al de la Ley Modelo de la CNUDMI, lo relacionado a la firma electrónica es diferente al texto de la Ley Modelo (artículo 2 y 14 de la Ley 67).

Perú reconoce la validez y eficacia de la firma electrónica, agrega el concepto de Infraestructura Oficial de la Firma Electrónica, y reconoce otras firmas electrónicas, siempre que estén acreditadas por una autoridad administrativa competente. No tiene el concepto de mensajes de datos. Utiliza para esto varios artículos cuya redacción difiere a la de la Ley Modelo (artículo 1 de la Ley 27269 del 2000, artículos 5, 6, 7 del Reglamento de la Ley 27269).

Costa Rica se refiere al concepto de documento electrónico privado y público, indicando que se les reconocerá fuerza probatoria igual que los documentos físicos. Su redacción difiere completamente a la de la Ley Modelo (artículos 4, 9 de Ley 8454).

Como se ha dicho anteriormente, es importante tener una sola redacción en materia de reconocimiento jurídico de los mensajes de datos y firmas electrónicas con el fin de proteger a los todos los usuarios del comercio electrónico de manera igualitaria y con la misma interpretación.

4.1.2.3 Definición de Mensajes de Datos

Ley Modelo CNUDMI sobre Comercio Electrónico:

> **"**Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;" (CNUDMI, 1999, p. 4).

Análisis

Es satisfactorio notar que al menos cuatro de los seis países analizados adoptaron la misma definición de mensajes de datos (con algunas variantes) consagrada en ambas Leyes Modelo de la CNUDMI.

La Ley colombiana incluyó como parte de los mensajes de datos, la información generada, enviada, recibida, almacenada o comunicada por medio de Internet (artículo 2 Ley 527); mientras que la Ley ecuatoriana consideró los documentos y registros electrónicos y los servicios Web como mensajes de datos (párrafo 10 de las Disposiciones Generales de la Ley 67). Se interpreta que, la Internet y los Servicios Web podrían ser considerados como sinónimos o elementos equivalentes.

Chile (artículo 2 Ley 19799) no define el concepto de mensaje de datos, sino más bien el de documento electrónico al igual que Costa Rica (artículo 3 Ley 8454).

Se considera que una definición única y uniforme de mensaje de datos debería estar en armonía con lo dispuesto en la Ley Modelo de la CNUDMI y los países: Colombia, Ecuador, Perú y México.

4.1.2.4 Definición de Firma Electrónica o Digital

Ley Modelo CNUDMI para Firma Electrónica:

> "Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos;" (CNUDMI, 2002, p. 10).

Análisis

La firma electrónica ha sido definida dentro de las disposiciones originadas en Ecuador (artículo 13 Ley 67), Chile (artículo 2 Ley 19799) y México (artículo 89 Decreto sobre Firma Electrónica); mientras que la firma digital fue objeto de definición por parte de las disposiciones originadas en Costa Rica (artículo 8 Ley 8454) y Colombia (artículo 2 Ley 527). Solo la legislación peruana (inclusive el Reglamento a la Ley) establece ambas definiciones, es decir, las definiciones de firmas electrónicas (artículo 1 Ley 27269) y

digitales (artículo 3 Ley 27269), dejando expresamente estipulado que la segunda es un tipo de firma electrónica.

Se considera que las definiciones de firma digital colombiana, costarricense y peruana, podrían ser consideradas, como modelos de disposición legal a ser acogidos por otros países. Sin embargo, la firma digital es una tecnología específica de firma electrónica, por lo que se recomienda que se use el concepto de firma electrónica en vez de digital, para no sujetar la ley a una tecnología específica.

La definición de firma electrónica adoptada en Ecuador y en Perú, son referencias a ser tomadas en consideración al momento de redactar una norma única y uniforme que pueda regir en grupos de países.

Es importante recordar que para que haya una aplicación semejante en los países de las normas sobre comercio electrónico, los conceptos sobre los cuales se basan deben ser iguales o equivalentes y debe haber consenso en los conceptos y definiciones. Los seis países analizados pueden basarse en los mismos conceptos y definiciones de lo que se considera como firma electrónica, firma digital, certificado digital, entidad/autoridad de certificación, mensaje de datos, por mencionar algunos.

4.1.2.5 Fuerza probatoria

Acompaña la validez jurídica. Se trata de un mandato a quienes tienen la responsabilidad de evaluar una prueba. La intención es darle la misma validez como prueba a los documentos y firma electrónica como la tienen los documentos y firma tradicionales.
A continuación los artículos de las legislaciones referentes a este principio con relación a los Mensajes de datos y a la Firma electrónica o digital.

Ley Modelo CNUDMI sobre Comercio Electrónico

> "Artículo 9. — Admisibilidad y fuerza probatoria de los mensajes de datos
> 1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:

> *a)* Por la sola razón de que se trate de un mensaje de datos; o *b)* Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.
> 2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente." (CNUDMI, 1999, p.7)

> **Ley Modelo CNUDMI para Firma Electrónica:**
> **Artículo 6. Cumplimiento del requisito de firma**
> "1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.
> 2. El párrafo 1 será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.
> 3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1 si: ..." (CNUDMI, 2002, p.11).

Y se establece los requisitos que debe tener la firma.

Análisis

Todos los países tienen incorporado dentro del texto normativo el mandato de que los mensajes de datos y la firma electrónica o digital tienen valor probatorio y validez jurídica, aunque ninguno de ellos coincida en la redacción del texto.

Perú (artículo 7 y 8 Reglamento de la Ley 27269) y Chile (artículos 3 y 5 de la Ley 19799) establecen que solo los documentos firmados electrónicamente podrán ser ofrecidos como prueba. Chile además indica que deben tener firma electrónica avanzada para que sea aceptado como prueba en juicio.

Colombia (arts. 10, 11 y 28 de la Ley 527) admite su fuerza probatoria; Ecuador (artículos. 52, 54, 55 de la Ley 67) establece que los mensajes de datos tienen valor y efectos legales. Colombia y Ecuador prevén que para la valoración y efectos legales de los mensajes de datos se observará lo dispuesto en el Código de Procedimiento Civil de cada uno de estos países.

México establece en la definición de firma electrónica, que un mensaje de datos con firma electrónica es admisible como prueba (art. 89, 89 bis del Decreto sobre firma electrónica).

Colombia agrega además a su conjunto de normas sobre comercio electrónico que para la valoración de la fuerza probatoria de los mensajes de datos, se tendrán en cuenta reglas de derecho positivo, como la sana crítica para la apreciación de las pruebas.

Colombia y Ecuador están de acuerdo en que para valorar la fuerza probatoria de un mensaje de datos, deberá estimarse la fiabilidad del método por el que el mismo haya sido generado, archivado, comunicado o conservado. Este requisito ha sido igualmente consagrado en la Ley Modelo. La norma ecuatoriana incluye algunas variantes.

Costa Rica reconoce la fuerza probatoria de los documentos electrónicos en las mismas condiciones que los documentos físicos (artículo 4 Ley 8454).

Es necesario que los mensajes de datos sean reconocidos como medios legales de prueba y que a los mismos se admita valor y eficacia probatorios. También es importante que se establezca que para que un mensaje de datos pueda admitirse como prueba deberá estimarse la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente como lo establece la Ley Modelo, Colombia y Ecuador.

4.1.2.6 Equivalencia Funcional

Este es un principio fundamental de la regulación del comercio electrónico, componente importante para el cumplimiento del objetivo de dar seguridad jurídica a las transacciones electrónicas.
Este principio se refiere a darle el mismo valor jurídico a los documentos y firmas electrónicas que a los equivalentes en papel.

Ley Modelo de la CNUDMI sobre Comercio Electrónico:

"Artículo 6. — Escrito
1) Cuando la ley 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 ulterior consulta.
2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.
3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7. — Firma
1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:
a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y
b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.
2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.
3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 8. — Original
1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:
a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;
b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.
2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o
conservada en su forma original.
3) Para los fines del inciso a) del párrafo 1):
a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso
de su comunicación, archivo o presentación; y
b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.
4) Lo dispuesto en el presente artículo no será aplicable a: [...]."(CNUDMI, 1999, p. 5)

Análisis

En lo básico, la Ley Modelo (artículos 6, 7, 8 Ley Modelos sobre Comercio Electrónico) establece:

- Escrito: cuando se requiera que la información conste por escrito, el requisito

quedará cumplido con un mensaje de datos, si éste es accesible para una consulta posterior.

- Firma: cuando se exija la presencia de una firma se entenderá satisfecha si se usa un método que permita identificar al iniciador y que el contenido cuenta con su aprobación.
- Original: cuando se requiera que la información sea presentada y conservada en su forma original, el requisito quedará satisfecho con un mensaje de datos, si ha conservado la integridad de la información desde que se generó.

El texto de los artículos de Colombia (artículos 6, 7, 8 Ley 527) es idéntico al texto de la Ley Modelo con una variación mínima en su redacción, pero que se interpreta el mismo significado.

Ecuador establece los artículos equivalentes a Escrito y Original (artículos 6, 7 Ley 67), su redacción varía un poco, pero conserva el mismo significado. No se refiere a la firma.

Perú no tiene artículos específicos para establecer la equivalencia funcional explícitamente, sin embargo, todo el articulado de la Ley 27269 y su Reglamento permite establecer esta equivalencia, en especial los artículos 5 y 6 del Reglamento a la Ley 27269.

Chile establece la equivalencia funcional de una manera distinta a la propuesta por la Ley Modelo, en un solo artículo indica que los actos y contratos firmados electrónicamente tienen los mismos efectos que los realizados por escrito y en soporte de papel (artículo 3 Ley 19799).

México sigue el texto de la Ley Modelo con variaciones mínimas en su redacción (Artículo 89, 93, 93 bis, 97 del Decreto sobre firma electrónica).

Costa Rica expresamente establece la equivalencia funcional entre los documentos expresados en forma electrónica que los documentos en medios físicos, e indica que

los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita (artículo 3 y 9 de la Ley 8454). No se refiere específicamente a los términos de mensajes de datos y firma electrónica.

De igual manera, como anteriormente se mencionó, es importante una uniformidad o estandarización de la normativa para dar igualdad jurídica y de interpretación a las mismas situaciones en diferentes países, para protección de los ciudadanos en los casos de controversias.

4.1.2.7 Neutralidad tecnológica

Este principio se refiere a que las legislaciones no deben atarse a una tecnología específica.

Ley Modelo de la CNUDMI para Firma Electrónica:

> "Artículo 3. Igualdad de tratamiento de las tecnologías para la firma.
> Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1 del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable." (CNUDMI, 2002, p. 11).

Análisis

Todos los países, a excepción de Colombia, coinciden en enmarcar sus desarrollos legislativos en este principio. Sin embargo, sus textos normativos lo expresan de forma diferentes a la Ley Modelo.

Colombia del todo no tiene explícito este principio en su texto.

Chile establece, en su artículo 1 de la Ley 19799, que las actividades reguladas por esta Ley se someterán a una serie de principios entre ellos el de neutralidad tecnológica.

En el artículo 2 de la Ley 8454 de Costa Rica, establece que en la implementación, interpretación y aplicación de esta Ley se debe observar, entre otros, el principio de igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas.

Ecuador lo establece en su artículo 10 del Decreto 3496, indica que la firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y su reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y su reglamento.

Artículo 89 y 96 del Decreto sobre firma electrónica de México indican que las actividades reguladas por este Título se someterán en su interpretación y aplicación al principio de neutralidad tecnológica, entre otros. Además indica que no se deben excluir, restringir o privar de efecto jurídico cualquier método para crear una Firma Electrónica.

El artículo 9 del Reglamento de la Ley 27269 de Perú estipula que se permite las firmas electrónicas generadas de diferentes formas, utilizando diferente tecnologías e independientemente de su soporte material pero que debe ser aprobada por la autoridad competente de acuerdo con el principio de neutralidad tecnológica.

Se recomienda indicar expresamente como lo hace Perú, el concepto de neutralidad tecnológica, y analizar la conveniencia de establecer que la tecnología que se utilice para generar la firma electrónica debe ser autorizada por la autoridad competente, en el sentido de sopesar los beneficios de dar mayor seguridad a la transacción con el de no restringir el comercio.

4.1.2.8 Autonomía de la voluntad

Se refiere a la libertad de las partes de establecer algún acuerdo y de la forma que deseen.

Ley Modelo de la CNUDMI sobre Comercio Electrónico:

> "Artículo 4. — Modificación mediante acuerdo
> 1) Salvo que se disponga otra cosa, en las relaciones entre las partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del capítulo III podrán ser modificadas mediante acuerdo.
> 2) Lo dispuesto en el párrafo 1) no afectará a ningún derecho de que gocen las partes para modificar de común acuerdo alguna norma jurídica a la que se haga referencia en el capítulo II." (CNUDMI, 1999, p.5).

Ley Modelo de la CNUDMI para Firma Electrónica:

> "Artículo 5. Modificación mediante acuerdo
> Las partes podrán establecer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable." (CNUDMI, 1999, p.5).

Análisis

Todos los países reconocen el principio de libertad contractual, permitiendo a los usuarios usar las herramientas legales para establecer y señalar las condiciones de validez de sus transacciones.

Algunas normas establecen disposiciones aplicables en contratos electrónicos que no hayan sido pactadas por las partes.

La Ley Modelo reconoce este principio permitiendo que pueda darse la modificación mediante acuerdo (artículo 4 Ley Modelo sobre Comercio Electrónico, y artículo 5 de la Ley Modelo sobre Firmas Electrónicas).

Chile no tiene expresado este principio en el texto de la Ley 19799.

Colombia expresa este principio en el artículo 4 de la Ley 527, con el mismo texto que el artículo 4, inciso 1 de la Ley Modelo sobre Comercio Electrónico.

Costa Rica tiene este principio como uno de los rectores de la Ley (artículo 2 de la Ley 8454).

Ecuador lo establece en el capítulo dedicado a los derechos de los consumidores, y lo detalla desde la perspectiva de la aceptación del consumidor de recibir mensajes de datos y usar medios electrónicos. Indica que el consumidor debe ser informado sobre el uso de medios electrónicos y dar su consentimiento (artículo 48 y 49 de la Ley 67).

México expresa la autonomía de la voluntad como un principio que rige las actividades de ese Título (artículo 89 del Decreto sobre Firma Electrónica). Se interpreta que la frase, en los artículos 90 bis, 91, 91 bis y 94 del Decreto sobre Firma Electrónica, “salvo pacto en contrario”, permite la modificación de acuerdo si así lo pactan las partes.

Perú establece el principio de la autonomía de la voluntad para usar otras firmas generadas fuera de la Infraestructura Oficial de Firma Electrónica en su artículo 2 del Reglamento de la Ley 27269.

Solo Colombia utiliza el mismo texto de la Ley Modelo.

Es importante dejar claro la importancia de la autonomía de la voluntad, que permite la libertad contractual. Se recomienda una sola redacción para protección de las partes y evitar diferentes interpretaciones.

4.1.2.9 Compatibilidad Internacional

Este principio se refiere a que se debe cumplir con estándares internacionales. Es decir, que los requerimientos técnicos exigidos para los mensajes, contratos, firmas y certificaciones electrónicas cumplan con los estándares a nivel internacional; y sea posible reconocer en ambas vías estos asuntos. El reconocimiento en ambas vías se refiere a que el país reconozca certificaciones extranjeras, y viceversa, que los otros países reconozcan las certificaciones nacionales.

Ley Modelo de la CNUDMI sobre Comercio Electrónico:

> Artículo 3. — Interpretación
> 1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.
> 2) Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que ella se inspira. (CNUDMI, 1999, p.4)

Ley Modelo de la CNUDMI para firma electrónica:

> "Artículo 12. Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras
> 1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:
> *a)* el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni
> *b)* el lugar en que se encuentre el establecimiento del expedidor o del firmante.
> *2.* Todo certificado expedido fuera *[del Estado promulgante]* producirá los mismos efectos jurídicos en *[el Estado promulgante]* que todo certificado expedido en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.
> 3. Toda firma electrónica creada o utilizada fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que toda firma electrónica creada o utilizada en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.
> 4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines del párrafo 2, o del párrafo 3, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.
> 5. Cuando, sin perjuicio de lo dispuesto en los párrafos 2, 3 y 4, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable." (CNUDMI, 2002, p.15)

Análisis

En los textos normativos analizados no todos los países se refieren a la compatibilidad internacional expresamente.

Costa Rica, Perú y Ecuador no tienen expresado el término de Compatibilidad Internacional, sino que establecen en su articulado el reconocimiento de certificados expedidos en el extranjero: el artículo 13 de la ley 8454 de Costa Rica, el artículo 48 del Reglamento de la Ley 27269 de Perú y el artículo 28 de la Ley 67 de Ecuador.

El artículo 3 de la Ley 527 de Colombia tiene el mismo texto que el artículo 3 de la Ley Modelo sobre Comercio Electrónico, que se refiere a la Interpretación. Ambas indican que para la interpretación de la Ley habrán de tenerse en cuenta su origen

internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Colombia no tiene expresamente el término de Compatibilidad Internacional. Es de observar que a pesar de que Colombia sigue en gran medida la Ley Modelo de la CNUDMI sobre Comercio Electrónico en su texto normativo, no incluye los reconocimientos de certificaciones y firmas electrónicas extranjeras como sí lo tiene previsto en el artículo 12 de la Ley Modelo sobre Firmas Electrónicas.

Los artículos 1 y 15 de la Ley 19799 de Chile y los 89 y 114 del Decreto sobre Firma Electrónica de México, tienen incorporado entre sus principios el de Compatibilidad Internacional, y ambos países también incorporan en su normativa el reconocimiento de certificados extranjeros.

Solo Costa Rica establece requisitos para reconocer las certificaciones digitales emitidas en el extranjero: que el certificador extranjero esté respaldado por uno registrado en el país por existir una relación de corresponsalía o cumplan con los requisitos del artículo 19 de la ley 8454 y exista un acuerdo recíproco en ese mismo sentido entre Costa Rica y el país de origen del certificador extranjero (artículo 13 Ley 8454).

Es importante indicar expresamente el principio de compatibilidad internacional y explicar su significado además de incluir los términos en que puede darse, como Costa Rica, que establece que se reconocerá las certificaciones digitales emitidas en el extranjero, siempre y cuando estén respaldadas por un certificador registrado en el país, o cumpla con los requisitos del artículo 19 y haya un acuerdo recíproco entre Costa Rica y el país origen del certificador extranjero. En el caso de la redacción de la norma (artículo 13 ley 8454) de Costa Rica, es importante analizar si estos requisitos no restringirían el comercio, y más bien sería más conveniente adoptar la redacción de la ley Modelo.

4.1.2.10 Disposiciones relacionadas con los contratos

Las leyes sobre certificados, firmas y mensajes de datos o documentos electrónicos analizados también incorporan disposiciones relacionadas con la celebración de contratos electrónicos. A continuación sólo se identifican las normas de los países en las que se hace referencia.

- Formación y validez de los contratos:
    - Ley Modelo sobre Comercio Electrónico: art. 5, 11, 12.
    - Chile: art. 3, 5 Ley 19799.
    - Colombia: art. 14 Ley 527
    - Costa Rica: art. 4 Ley 8454.
    - Ecuador: art. 2, 45 Ley 67
    - México: art. 89 bis, 93, 93 bis Decreto sobre firma electrónica del 29 de agosto del 2003.
    - Perú: art. 7 Reglamento a la Ley 27269.

- Reconocimiento de firma electrónica:
    - Ley Modelo sobre Firmas Electrónicas: art. 6.
    - Chile: art. 3 Ley 19799.
    - Colombia: art. 28 Ley 527.
    - Costa Rica: art. 9 Ley 8454.
    - Ecuador: art. 14 Ley 67.
    - México: art. 97 Decreto sobre firma electrónica del 29 de agosto del 2003.
    - Perú: art. 5, 6 Reglamento a la Ley 27269.

- Perfeccionamiento:
    - Ley Modelo de Comercio Electrónico: art. 14 y 15.
    - Chile: No.
    - Colombia: Art.20, 21, 22, 23, 24, 25 Ley 527.
    - Costa Rica: No.
    - Ecuador: Art. 46 Ley 67,
    - México: Art.91, 91 bis, 94 Decreto sobre firma electrónica del 29 de agosto

del 2003.
    - Perú: No.
- Jurisdicción, arbitraje, controversias:
    - Chile: No.
    - Colombia: No.
    - Costa Rica: No.
    - Ecuador: art. 47 Ley 67
    - México: No.
    - Perú: No.

- Atribución, Presunción de origen:
    - Ley Modelo sobre Comercio Electrónico: art. 13, 14.
    - Chile: Art. 2 inc. 9 Ley 19799.
    - Colombia: art. 16, 17 Ley 527.
    - Costa Rica: art. 10 Ley 8454.
    - Ecuador: art. 10 Ley 67
    - México: art. 90 u 90 bis Decreto sobre firma electrónica del 29 de agosto del 2003.
    - Perú: art. 8 Reglamento a la Ley 27269.

- Concordancia del mensaje enviado con el recibido:
    - Ley Modelo sobre Comercio Electrónico: art. 14.
    - Colombia: art. 18 Ley 527.
    - Chile, Ecuador, Costa Rica, México: No.

- Mensajes de datos duplicados:
    - Ley Modelo sobre Comercio Electrónico: art. 13.
    - Colombia: art. 19 Ley 527.
    - Ecuador: art. 12 Ley 67.
    - México: art. 95 Decreto sobre firma electrónica del 29 de agosto del 2003.
    - Chile, Costa Rica, Perú: no tiene.

- Acuse de recibo, presunción de recepción:
    - Ley Modelo sobre Comercio Electrónico: art. 14.
    - Colombia: art. 20, 21 y 22 Ley 527.
    - México: art. 92 Decreto sobre firma electrónica del 29 de agosto del 2003.
    - Costa Rica: No.
    - Chile: No.
    - Perú: No.
    - Ecuador: No.

- Efectos jurídicos del acuse de recibo:
    - Ley Modelo sobre Comercio Electrónico: art. 14.
    - Colombia: art. 22 Ley 527.
    - Chile, Ecuador, Perú, Costa Rica, México: No.

- Tiempo y lugar de envío y recepción:
    - Ley Modelo sobre Comercio Electrónico: art. 15.
    - Colombia: art. 23, 24, 25 Ley 527.
    - Ecuador: art. 11 Ley 67.
    - México: art. 91, 91 bis, 94 Decreto sobre firma electrónica del 29 de agosto del 2003.
    - Perú: No.
    - Chile: No.
    - Costa Rica: No.

4.1.2.11 Otros asuntos

Las leyes analizadas también incluyen normas sobre:

1. Entidades de certificación
2. Entidad de registro o validación
3. Certificados digitales
4. Derechos de los usuarios o consumidores
5. Infracciones informáticas

6. Transporte
7. Utilización por el Estado.

Las cuales se comentarán a continuación. En el anexo 2 se encuentra un resumen de la normativa analizada.

1. Entidades de certificación

Los seis países: México, Perú, Colombia, Ecuador, Chile, Costa Rica, establecen disposiciones relacionadas con las entidades de certificación.

Cuatro de ellos coinciden en exigir que quienes presten servicios de certificación sean Personas Jurídicas. (Empresa Unipersonal o jurídica: Ecuador; Notarios y corredores públicos, personas privadas morales, instituciones públicas: México; Notarios y cónsules: Colombia; cualquier persona Nacional o extranjera Públicas o Privadas: Chile, Costa Rica; persona natural o jurídica: Perú).

Todas las normas exigen capacidad económica y financiera, así como técnica suficiente para desempeñar sus funciones, y deben ser autorizadas por un órgano de control.

2. Entidad de registro o validación

Perú es el único país que establece disposiciones sobre entidades de registro separadas a las entidades de certificación. Estas entidades deben cumplir la función de levantamiento de datos y comprobación de la información del solicitante de un certificado digital. Deberán registrarse ante la autoridad de control. Se trata de personas jurídicas que cuenten con el respaldo económico suficiente para realizar sus funciones.
Los restantes países (México, Chile, Ecuador, Costa Rica, Colombia), las funciones de registro son parte de las funciones de las entidades de certificación.

3. Certificados digitales

Todos los países coinciden en regular los certificados digitales con algunas variaciones en los respectivos reglamentos.

La revocatoria de certificados está contemplada en las normas de Colombia, Chile, México, Perú, Ecuador y Costa Rica.

El reconocimiento internacional de certificados está presente en las normas de México, Costa Rica, Perú, Ecuador y Chile.

Las normas de los seis países contemplan requisitos para los certificados digitales, también establecen un tiempo de duración del certificado.

El término de extinción del certificado sólo está presente en las leyes de Ecuador, México y Chile.

Las normas de Ecuador y Costa Rica permiten la suspensión de certificados.

Las normas de Perú y Chile hablan de cancelación de certificados.

Todas las normas, a excepción de la de Ecuador, contemplan la actividad de llevar el registro de los certificados digitales.

4. Derechos de los usuarios o consumidores

El capítulo III de la Ley 67 de Ecuador, se contemplan artículos específicos sobre los siguientes aspectos relacionados con los derechos de los consumidores: derecho a dar el consentimiento expreso, a ser informado, a acceder a la información, a elegir si recibe información por escrito o electrónica, derecho de retracto, derecho a que no se le envíe mensajes periódicos a su dirección electrónica.

El artículo 41 de la Ley 527 de Colombia establece, como una función de la Superintendencia de Industria y Comercio, la función de velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en

los mercados atendidos por las entidades de certificación. Y el artículo 46 establece la prevalencia de las leyes de protección al consumidor.

En el artículo 12, inciso j) de la ley 19799 de Chile, se establece que es obligación del prestador de servicios de certificación de firma electrónica cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada.

Las leyes de comercio electrónico analizadas de México, Perú y Costa Rica no mencionan nada con respecto a los consumidores.

5. **Infracciones informáticas/ delitos informáticos**

El Título V de la ley 67 de Ecuador se refiere a las infracciones informáticas. Incluye disposiciones que reforman su Código Penal. Se modifican algunos tipos penales y se incluyen otros: falsificación electrónica, violación de información protegida, accesos no autorizados, daños informáticos, apropiación ilícita, violación a la intimidad.

Las normas de los demás países no incluyen nada relacionado con las infracciones informáticas.

6. Transporte

Colombia es el único que siguiendo las recomendaciones de la ley Modelo de comercio electrónico de UNCITRAL, incluye un capítulo sobre transporte de mercancías y sobre la aplicación del principio de equivalente funcional y de la validez jurídica a los actos que componen el contrato de transporte de mercancías (artículos 26 y 27 de la ley 527).

7. **Utilización por el Estado**

Las normas de México, Colombia, Perú, Ecuador no establecen nada al respecto de la utilización de las firmas y documentos electrónicos por parte del Estado.

Las normas de Costa Rica (artículo 1 de la Ley 8454) y Chile (Título II de la Ley 19799) establecen en sus leyes la posibilidad de que el Estado utilice la firma y documentos electrónicos en su relación con otras instituciones públicas, así como con los particulares.

En el anexo 2 se encuentra el resumen de lo analizado en estas secciones anteriores.

4.1.3 Análisis de la Ley 8454 de Costa Rica

Se observa que la normativa costarricense, a diferencia de la mayoría de los países analizados, tiene una redacción completamente diferente a la Ley Modelo sobre comercio electrónico o a la Ley Modelo sobre firmas electrónicas de la CNUDMI.

A pesar de lo anterior, la Ley costarricense incorpora normas para garantizar todos los principios de seguridad jurídica, como puede verse en el cuadro correspondiente del Anexo 2: Reconocimiento jurídico, fuerza probatoria, equivalencia funcional, neutralidad tecnológica, autonomía de la voluntad y compatibilidad internacional.

Del análisis realizado se puede determinar algunos vacíos en la normativa costarricense en los siguientes aspectos:

- Referencia a firma digital
- Perfeccionamiento de contratos electrónicos
- Legislación y Jurisdicción aplicable
- Protección al Consumidor
- Infracciones Informáticas
- Otras debilidades

En el anexo 6 se encuentra el resumen de estos vacíos y debilidades.

4.1.3.1 Referencia a firma digital

Es claramente admisible el considerar como un vacío, que la ley costarricense haya hecho referencia a la firma digital, en lugar de la firma electrónica. Esto debido a que la firma digital hace referencia a una tecnología particular de creación de una firma electrónica.

Hubiera sido más conveniente haber incorporado en la ley el término de firma electrónica por cuanto esta es más amplia, y abarca cualquier firma electrónica y no sólo la digital.

Es probable que en los próximos años, la tecnología haya evolucionado y la firma digital se torne obsoleta y haya que recurrir a otros tipos de firma electrónica para asegurar las transacciones electrónicas y esto hará necesario la modificación de la Ley para que se permita la nueva firma, un proceso muy engorroso y difícil pues debe pasar por la Asamblea Legislativa del país.

En este sentido, el Proyecto de Ley 14276, versión del 25 de junio de 2004 (que dio origen a la actual Ley 8454), incorporaba el concepto de firma electrónica y no de firma digital, como puede verse en su artículo 13.

Se recomienda realizar la modificación respectiva para que en la Ley 8454 se haga referencia a la firma electrónica en vez de la firma digital.

4.1.3.2 Perfeccionamiento de contratos electrónicos

En la Ley 8454 no hay referencia sobre el perfeccionamiento de contratos electrónicos, o sobre el tiempo y lugar de emisión y recepción de documento electrónico.

Este vacío debe llenarse de alguna manera, ya sea adicionando los artículos necesarios para que se establezca explícitamente cuándo y dónde se entiende por perfeccionado un contrato electrónico, para protección de las partes, y principalmente del consumidor en los casos de relaciones de consumo. Como lo ha hecho Ecuador, Colombia y

México.

El Proyecto de Ley 14276 versión del 25 de junio de 2004 (que dio origen a la actual Ley 8454), establecía en sus artículos 8, 9 y 10 lo relacionado a contratos electrónicos, domicilio electrónico y lugar de emisión y recepción de los mensajes o documentos electrónicos. Estos artículos eran los equivalentes para poder establecer sobre el perfeccionamiento del contrato electrónico.

Es necesario definir en la Ley, el tiempo y lugar donde se considera que se envió y se recibió el documento electrónico, así como el acuse de recibo del documento.

De acuerdo con Moreno (2002), el acuse de recibo es una cautela que se toma para el aseguramiento por parte del autor de que el documento ha sido recibido por el destinatario. Este acredita que se recibió el mensaje y de quién se recibió.

El acuse de recibo permite establecer el tiempo y lugar donde la aceptación de una oferta se ha dado y por tanto, el tiempo y lugar de perfección del contrato, para los casos de las transacciones comerciales electrónicas.

Se recomienda que se incorpore explícitamente en la Ley 8454 lo relacionado al perfeccionamiento de contratos electrónicos, o más bien, el tiempo y lugar de emisión y recepción de documento electrónico, y no dejar simplemente a la interpretación de lo que el Código Civil y el Código de Comercio establezcan al respecto, en los casos de una transacción comercial electrónica.

Ambos Códigos no tienen incorporado el término de contrato de compra y venta electrónico, y abría que interpretar que una transacción de este tipo es análoga a una que se realiza entre partes no reunidas (artículo 1012 del Código Civil) o una que se negocia por correspondencia (artículos 443 y 444 del Código de Comercio), esto debido a que en estos casos se da un plazo para que el proveedor mantenga la oferta por un tiempo determinado hasta que reciba la aceptación del consumidor.

4.1.3.3 Legislación y jurisdicción aplicable

Muy ligado al perfeccionamiento del contrato (o tiempo, lugar y acuse de recibo de recepción del documento electrónico), y que la Ley 8454 no lo contempla, está lo relacionado a la legislación y jurisdicción aplicable. La Ley 8454 tampoco indica nada al respecto de la legislación y jurisdicción aplicable.

Al dar reconocimiento y validez jurídica a los documentos electrónicos, estos pueden contener manifestación, declaración y aceptación de voluntades. Y si alguna de las partes incumple, da derecho a que la parte lesionada plantee la denuncia o demanda. Debe mencionarse en la Ley cómo se procede en estos casos, como lo ha hecho Ecuador con su artículo 47 que reza:

> "Art. 47.- Jurisdicción.- En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario.
>
> Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta ley y demás normas legales aplicables.
>
> Cuando las partes pacten someter las controversias a un procedimiento arbitral en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje." (Ley 67 de Ecuador, 2002, p. 9).

Se observa que en este artículo se incluye la protección al Consumidor, pues solo en caso de que el afectado sea un consumidor rige la jurisdicción del domicilio del consumidor.

En materia de comercio electrónico, donde las transacciones comerciales que se realizan pueden ser fácilmente entre partes ubicados en distintos países, es necesario establecer los mecanismos de solución de controversias, jurisdicción y legislación aplicable y las posibilidades de arbitraje.

En este sentido, el anterior artículo incorpora un aspecto novedoso como es la posibilidad de un arbitraje por medios telemáticos y electrónicos.

4.1.3.4 Protección al Consumidor

La Ley 8454 no menciona nada al respecto sobre protección al consumidor, probablemente deja a la Ley 7472 de Promoción de la Competencia y Protección Efectiva del Consumidor, todo lo relacionado a este.

Sin embargo, recuérdese que la Ley 7472 es anterior a toda esta revolución del desarrollo de las tecnologías de comunicación e Información, y que por lo tanto, muchos aspectos relacionados a este nuevo desarrollo no quedaron contemplados en la Ley 7472.

Entre las cosas no contempladas en la Ley está todo lo relacionado a la evolución de los documentos de papel al documento electrónico, así entonces, los contratos de papel a contratos electrónicos y las compras y ventas por medios electrónicos, etc.

Sería conveniente incluir en la Ley 8454 al menos la mención, como lo ha hecho Colombia, en el artículo 41, dando la función a la Superintendencia de Comercio e Industria de:

> "10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación." (Ley 527 de Colombia, 1999, p. 15).

Y el artículo 46 que indica:

> "ARTICULO 46. PREVALENCIA DE LAS LEYES DE PROTECCION AL CONSUMIDOR. La presente ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor." (Ley 527 de Colombia, 1999, p.17).

Por otro lado, es importante incluir los nuevos aspectos de protección al consumidor, con relación al nuevo desarrollo tecnológico, en la Ley 7472. En un capítulo posterior se analizará el tema de Protección a Consumidor con más detalle.

4.1.3.5 Infracciones Informáticas

La Ley 67 de Ecuador incluye todo un título de reformas a su Código Penal para incluir las infracciones informáticas.

En el caso de Costa Rica, existe en el Código Penal la tipificación de tres tipos de delitos informáticos: violación de comunicaciones electrónicas (artículo 196 bis del Código Penal), fraude informático (artículo 217 bis del Código Penal) y alteración de datos y sabotaje informático (artículo 229 bis del Código Penal).

Además en las diversas leyes del país se encuentran sanciones de penas de prisión a infracciones a los sistemas de información de las instituciones del Estado. Entre ellas se encuentran: Ley 7535 de Justicia Tributaria, en la que se reforma los artículos del 90 al 98 del Código de Normas y Procedimientos Tributarios; los artículos 221 y 222 de la Ley 7557 General de Aduanas y el artículo 111 de la Ley 8131 de Administración Financiera de la República y Presupuestos Públicos.

Sin embargo, se recomienda realizar una investigación exhaustiva sobre los tipos de infracciones informáticas que pueden ocurrir por el nuevo desarrollo de las tecnologías de información y comunicación, e incluir, las no contempladas aún, en el Código Penal, o en las leyes específicas.

4.1.3.6 Otras debilidades

Además de las anteriores, se detectan otras debilidades de la Ley 8454, que a continuación se comentan.

El artículo 12, inciso e) indica que las instituciones públicas y el Estado pueden fungir como un certificador respecto de sus despachos y funcionarios. Este artículo permite interpretar que se permitirá tener más de una Autoridad Certificante Raíz, pues cada Institución Pública podrá otorgar certificados a sus funcionarios.

Habría que analizar la conveniencia y la capacidad del país para que sus Instituciones puedan ser Autoridades Certificantes, principalmente por el costo de la inversión que se requiera para implementar la Infraestructura de Clave Pública.

Por otro lado, es necesario analizar las experiencias de otros países sobre el establecimiento de más de una Autoridad Certificante Raíz. Pues puede resultar difícil hacer compatibles, por problemas de interoperabilidad, certificados extendidos por diferentes Autoridades Certificantes Raíces.

El artículo 13, indica que para reconocer un certificado digital emitido en extranjero, éste debe estar respaldado por un certificador nacional en virtud de una relación de corresponsalía, o cuando haya un acuerdo recíproco entre Costa Rica y el país del certificador extranjero y cumpla con los requisitos, trámites y funciones establecidos en el artículo 19 de la Ley. Esto implica que no se reconoce automáticamente los certificados digitales emitidos en el extranjero, lo que supone una traba al comercio electrónico.

El artículo 16 permite la revocación de los certificados extendidos por un Certificador cuando éste cese sus actividades. El cese de actividades de un Certificador no debería afectar la vigencia de los certificados que éste ya había extendido. Se requiere que se establezca explícitamente cómo se abordará estos casos sin afectar a las personas que recibieron certificados extendidos por el Certificador antes de su cese de actividades.

El artículo 18 de la Ley establece que la garantía de fidelidad puede ser por hipoteca, fianza o póliza de fidelidad de un ente asegurador, o un depósito en efectivo. Más bien, se debería establecer que la garantía de fidelidad sólo podrá ser por depósito en efectivo. Pues los otros tipos de garantías establecidos requiere de toda una gestión legal y mucho tiempo para hacerla efectiva, y obligaría a la Dirección de Certificadores de Firma Digital a realizar un proceso largo y difícil que no es conveniente.

El artículo 23 de la Ley establece la creación de la Dirección de Certificadores de Firma Digital, perteneciente al Ministerio de Ciencia y Tecnología, como el órgano administrador y supervisor del Sistema de Certificación. Se deduce de esto que la Autoridad Certificadora de rango superior o raíz es el Ministerio de Ciencia y Tecnología.

Esto se considera como debilidad debido a que la Infraestructura de Clave Pública requiere una inversión considerable, en todo sentido, para implementarla, y habría que analizar si el Ministerio de Ciencia y Tecnología (MICIT) tiene la capacidad para realizar la inversión requerida.

Para la solución de esto último, el MICIT ha firmado un convenio con el Banco Central de Costa Rica, con la intención de que el Sistema Interbancario de Negociación y Pago Electrónico (SINPE) se convierta en una entidad certificadora que cumpla con los requisitos de seguridad internacionales; para ello deberá invertir en los equipos e infraestructura necesarios, y utilizar la infraestructura de comunicación ya existente entre el SINPE y los Bancos, lo que permitirá un ahorro considerable y ofrecer a un costo muy bajo el certificado digital a todos los usuarios bancarios que utilizan Internet (Fonseca, 2007).

Además, el artículo 25 de la Ley establece que la jefatura de la Dirección de Certificadores de Firma Digital será nombrada por el ministro de Ciencia y Tecnología y será un funcionario de confianza. Hay que analizar la conveniencia de este tipo de nombramientos, pues esto hará que el puesto sea un nombramiento de tipo político al vaivén de los Gobiernos.

Por último, y con relación a las entidades de certificación es necesario explicitar jurídicamente la regulación de estas entidades, que incluya además los siguientes elementos: tipo de productos que pueden brindar, los servicios concatenados a tales productos, controles administrativos a partir de la inscripción de un registro de estas entidades, entre otros.

4.2 Seguridad tecnológica del comercio electrónico

Desde el aspecto de seguridad tecnológica, se han desarrollado tecnologías para garantizar la seguridad de las operaciones electrónicas, estas tecnologías constituyen lo que se conoce como Criptografía y la Firma Digital. En el capítulo 2, sección 2.5 se ha

desarrollado ampliamente lo referente a esta tecnología. Por lo tanto, esta sección solo repasará algunos aspectos de importancia con relación a la seguridad tecnológica.

4.2.1 Los principios de seguridad en una comunicación electrónica

Como se ha indicado en el marco teórico, se requiere asegurar las transacciones electrónicas con relación a cuatro aspectos básicamente:

- Autenticidad: que las partes son quienes dicen ser.
- Confidencialidad: Solo el autorizado puede conocer la información.
- Integridad: que la información no ha sido modificada.
- No repudio: no se pueda negar que se ha participado en la comunicación.

Se ha explicado anteriormente con detalle que el uso de la criptografía asimétrica, el cual utiliza dos claves (una privada y otra pública) y firmas digitales, permiten asegurar los cuatro aspectos mencionados.

La criptografía asimétrica permite asegurar la confidencialidad de la información que se transmite; y el uso de la firma digital permite asegurar la autenticidad, integridad y no repudio de la información que se envía.

El sistema de la criptografía asimétrica utiliza dos claves, una privada y otra pública, que están matemáticamente relacionadas de tal forma que un mensaje cifrado con una clave sólo lo puede descifrar con la otra clave. Y es prácticamente imposible llegar a conocer la clave privada conociendo la clave pública. La clave pública es conocida por todos o susceptible de ser conocida; mientras que la clave privada por su parte es conocida sólo por el titular.

La importancia de la clave pública radica en que por la misma se verifica la firma digital y, por tanto, es prueba de la autoría e integridad del documento electrónico. La importancia de la clave privada por su parte viene avalada por ser generadora de la firma digital; es decir, el autor ha de firmar digitalmente el documento mediante su clave privada, la cual lleva asociada una clave pública (Moreno, 2002, p.155).

Dado que la firma digital se genera a partir de la clave privada del autor, se produce una asociación entre la clave privada y firma digital que trae como consecuencia que el autor no pueda negar su firma (no repudio), pues sólo él conoce la clave privada.

Para este sistema se requiere la presencia de una tercera parte confiable, llamadas Autoridades Certificantes que son las autorizadas a entregar las claves privada y pública a las personas que lo soliciten, y dan fe de la identificación de ellas. Además de entregar estas claves, también entrega el certificado digital que contiene la clave pública. Las personas solo deben dar a conocer su clave pública. La clave privada debe resguardarla.

Un mensaje enviado junto con la firma digital, requiere de la clave pública del remitente para poder verificar que el contenido del mensaje no fue alterado, que el remitente está plenamente identificado y que no puede repudiar el mensaje (la clave pública del remitente se encuentra en el certificado digital, que es enviado junto con el mensaje y la firma digital al receptor). Y si además, estos (el mensaje, la firma digital y certificado digital) se cifra con la clave pública del receptor, sólo éste puede descifrar el mensaje.

Indica Pérez (2003) que la identificación de los contratos electrónicos y la coincidencia entre el mensaje emitido y el mensaje recibido en la contratación serán garantizadas por los certificados digitales emitidos por una entidad de certificación. Por lo tanto, la firma digital y entidades de certificación son componentes fundamentales de la seguridad, lo que permitirá la confianza de quienes contratan.

Como puede observar, desde el punto de vista tecnológico, el sistema ofrece gran seguridad a la transacción electrónica. Sin embargo, desde el punto de vista humano la seguridad puede perderse, pues la seguridad de este sistema depende de que el usuario mantenga la clave privada bien resguardada.

Por otro lado, se resalta el hecho de que una vez que el mensaje haya sido descifrado por el receptor, la seguridad del mensaje ya no dependerá del sistema tecnológico utilizado en el envío del mensaje, sino más bien de los elementos de seguridad que se

tenga para resguardar, almacenar, y procesar la información en su destino. Estos elementos de seguridad incluyen entre otros: uso de clave por la persona autorizada a manipular la información (para evitar accesos no autorizados), protocolos, controles y auditorías para asegurar la debida utilización de la información (usos conforme al fin), y planes de contingencia para casos de siniestros (incendio, humedad, robo).

Complemento a la seguridad de la información que viaja a través de la red, están las tecnologías para dar seguridad a los servidores y para realizar pagos electrónicos seguros, que fueron ampliamente explicados en la sección 2.5 del Marco Teórico.

En resumen, el aspecto técnico para dar seguridad al pago electrónico (tarjeta de crédito, transferencias de fondos, dinero electrónico, etc.) se ha realizado por mecanismos de pago seguros mediante los protocolos SSL y SET. Desde el punto de vista jurídico, se hace necesaria una regulación específica sobre el uso de tarjetas como medio de pago electrónico, sobre todo la determinación de la responsabilidad de los prestadores de servicios de la sociedad de la información en los mecanismos de pago electrónico. Es decir, la responsabilidad de la entidad emisora de la tarjeta por el uso fraudulento que pueda realizarse por un usuario distinto del titular de la misma (Moreno, 2002).

4.2.2 La prueba documental electrónica

La prueba documental electrónica, se refiere a la posibilidad de acceder o tener el documento electrónico u otros elementos que permitan demostrar la existencia de una relación contractual contraída por medios electrónicos. Se refiere a los asuntos como: dónde están los documentos electrónicos?, tiene el usuario disponibilidad efectiva de los mismos?, cómo se acredita el autor?, existe prueba del pago?, etc., todo esto es importante para respaldar cualquier reclamo de incumplimiento de contrato.

Por lo anterior esta sección analizará el lugar donde se almacena el documento electrónico, desde el punto de vista tecnológico de la transacción electrónica.

Al analizar el proceso técnico de creación y transmisión de un documento electrónico, se observa que puede intervenir una tercero (prestador de servicios técnico), ajeno a la relación jurídica que se establezca, pero con vinculación con las partes, al registrar, conservar y custodiar los documentos electrónicos, es decir, la prueba. Se establece entonces una relación técnica con efectos jurídicos como a continuación se explica.

El emisor y el receptor se conectan a través de una Red de comunicación o plataforma (Internet en este caso), ambos establecen una relación de servicios con una prestador de servicios (en este caso de Internet, de hospedaje, o servicios de la sociedad de la información en términos de la Unión Europea; el sujeto, emisor y receptor, es el "cliente" y el prestador de servicios es el "servidor").

Cuando el emisor envía un mensaje de datos al destinatario, este documento electrónico puede crearse en la propia terminal del cliente o sistema cliente o conectado a la Red de comunicación en el servidor; de igual forma el destinatario, cliente, lo recibe en su propia terminal mediante el sistema cliente o en el servidor que está permanentemente conectado a la Red, aunque se visualice en el terminal.

En este esquema básico se plantea la interrogante de dónde se encuentra el documento electrónico? La respuesta es cualquiera de las siguientes según Moreno (2002):

Si el emisor tiene sistema cliente, en la propia terminal, además de en el servidor del emisor y del destinatario.
Si el emisor no tiene sistema cliente, en el servidor del emisor y del destinatario.
Si el receptor tiene sistema cliente, en la propia terminal, además de en el servidor del emisor y del destinatario.
Si el receptor no tiene sistema cliente, en el servidor del emisor y del destinatario.

En resumen, como puede observarse, los documentos son siempre almacenados en los servidores tanto del emisor-cliente como del destinatario-cliente.

En el caso del comercio electrónico, para operar y realizar transacciones electrónicas, desde el punto de vista técnico, la empresa necesita un sistema, plataforma o aplicación Web de comercio electrónico, para ello la empresa necesita un servidor, que puede ser propio, o contratar los servicios de hospedaje de un prestador de servicios. En este caso, dónde se encuentra el documento electrónico.

Para explicar esto, Moreno (2002) establece una plataforma de tres capas que se simplifica en el siguiente esquema:

- Capa de presentación o de cliente
- Capa de negocio o intermedia
- Capa de datos o de origen de datos

Desde el punto de vista de la prueba documental electrónica, interesa la capa de presentación y la de datos, ya que la capa de negocio estaría dentro del campo denominado "e-business".

La capa de presentación o de cliente es la parte programada para presentar la empresa, los productos, servicios, etc., e interactuar con el cliente en este caso el consumidor. Es lo que ve el consumidor, y éste puede introducir datos desde su terminal mediante un navegador. Esta capa es donde se inserta la publicidad, por lo que la prueba:

- de la consideración de la publicidad como parte de la oferta vinculante,
- de la licitud e ilicitud de la misma mediante la calificación o no, en su caso, de engañosa, desleal, subliminal, o prohibidas,
- de las condiciones generales de contratación,

debe ser acreditada mediante los documentos electrónicos que componen la capa de presentación, junto con otros elementos.

En este caso, si la empresa utiliza el servicio de hospedaje, la prueba de la declaración contractual está donde radica la plataforma o aplicación Web de comercio electrónico.

En este caso, el consumidor debería guardar la página Web y el código fuente por el procedimiento de “guardar como” en su computador e incluso imprimirla (Moreno, 2002).

La capa de datos no es visible para el usuario, en esta se almacenan los datos que el usuario o empresa introduce, orden de pedidos, acuses de recibo y el documento electrónico; todo en formato de datos ordenados, ya que en dicha capa se gestionan las bases de datos: de entrada y salida de productos, de compras, de proveedores, de clientes, de datos personales, etc.

Desde el punto de vista jurídico, es muy importante este elemento de la aplicación de comercio electrónico para la prueba de las transacciones, tanto para el destinatario, consumidor o empresa, como para el prestador de servicios técnico o comercial, pues en este nivel es donde se almacena o registra toda la información.

Indica Pérez (2003) que la prueba de las obligaciones que nacen de los contratos celebrados por medios electrónicos, se regirá por las reglas generales de la contratación y de las normas procesales del país, lo que la ley requiera a efectos de prueba. Cuando el contrato conste por escrito, siempre que no exista otra formalidad y la ley no disponga lo contrario, el requisito se entenderá satisfecho en el ámbito de la contratación por medios electrónicos, si los mensajes electrónicos que han dado lugar a la celebración del contrato son archivados y se mantienen accesibles para su posterior consulta.

En resumen, la tecnología permite dar respaldo de la existencia de los documentos electrónicos. Solo se hace la observación de que, en el caso de la capa de datos, esta prueba depende de que no se borre, ya sea accidental o de manera fraudulenta, los datos de donde se encuentran almacenados.

4.3 Conclusiones y recomendaciones

El elemento de seguridad en el tema de comercio electrónico requiere soluciones a nivel jurídico y técnico. Los aspectos estrictamente técnicos requieren de un marco normativo que permita dar seguridad jurídica a la transacción comercial electrónica. La seguridad de una transacción electrónica está basada en los principios de: autenticación o identidad del remitente, integridad del mensaje, no repudio del mensaje y confidencialidad, y se logra con la tecnología de criptografía asimétrica, firma electrónica y autoridades o entidades de certificación.

La validez de estas soluciones tecnológicas requiere de normas jurídicas que le de reconocimiento y fuerza probatoria a la firma electrónica y mensajes de datos o documentos electrónicos y regule lo relacionado a las entidades de certificación.

Se considera que la tecnología que respalda la utilización de la firma digital y certificados digitales, para asegurar los principios de seguridad jurídicos mencionados, ofrece un nivel alto de seguridad a la transacción electrónica. Sin embargo, aún este sistema de seguridad puede ser vulnerada en el caso de pérdida de la clave privada por parte del titular. Esto último es una vulnerabilidad que no puede ser achacable a la tecnología pues su origen es humano.

En relación con las entidades de certificación, éstas tienen el rol principal de asociar de un modo inequívoco la identidad de una persona concreta, a una clave determinada. Esto es necesario, porque el juego de claves utilizado para crear una firma digital no tiene una asociación intrínseca con nadie en especial, y entonces la solución de que aparezca un tercero confiable que certifique a la persona realmente asociada con ese par de claves, es lo que completa el margen de seguridad a todo este sistema de la firma digital basada en la criptografía asimétrica de clave pública.

La regulación de los sujetos prestadores de este servicio público requiere de normas jurídicas. Posiblemente en este punto se observa mayor ausencia de normas, porque todavía se tiene muy poco con respecto a los prestadores de servicios de certificación.

En el caso de Costa Rica, se tiene solo lo establecido en la Ley 8454 y su Reglamento, y que se refiere a: atribuciones y responsabilidades. Es necesario poner en evidencia entre otros elementos: tipo de productos que pueden brindar, los servicios paralelos a tales productos, controles administrativos a partir de la inscripción de un registro de estas entidades. Es decir, todo lo relacionado con la Infraestructura de Claves Públicas.

En Costa Rica, por el principio de la autonomía de la voluntad, es posible que los prestadores actúen de manera privada sin autorización de la Autoridad Certificadora. Pero solo los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital tendrán pleno efecto legal frente a terceros, así como respecto del Estado y sus instituciones (artículo 10 del Reglamento de la Ley 8454, Decreto Ejecutivo No. 33018).

En general, se observa en la legislación comparada sobre el marco jurídico de las firmas electrónicas y mensajes de datos, que rigen los principios de libertad de prestación de servicios, libre competencia, autonomía de la voluntad, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel.

Esta nueva normativa no afecta sustancialmente las normas relativas a la celebración, solemnidad, formalización, validez y eficacia de los contratos y actos jurídicos. Esto último es una demostración del principio de equivalencia funcional de la firma electrónica, de la firma digital, incluso del documento electrónico, a los actos correspondientes en el mundo tradicional o en el mundo no virtual.

Las leyes y normativas internacionales también ofrecen algunas definiciones técnicas que se requieren en una infraestructura de clave pública. Hay todo un componente técnico en esta normativa que se va alimentando de los estándares tecnológicos vigentes, por la necesidad de establecer la seguridad jurídica mínima sin que se limite la evolución de la técnica. Así, un marco jurídico debe ser tan amplio para que pueda prever y abarcar nuevos desarrollos de la tecnología, y específico que permita regular lo

necesario.

Acerca de los prestadores de servicios de certificación, la Directiva 1999/93/CE de la Unión Europea, enuncia que los países pueden crear sistemas de acreditación, tanto de los prestadores como de los productos de la firma electrónica que estos prestadores brindan. Pero son sistemas voluntarios, de libre competencia, destinados a mejorar los niveles de calidad de estos servicios de certificación.

Se observa que estos prestadores de servicios de certificación pueden actuar en un ámbito de libre competencia, sin necesidad de autorización previa. Pero al mismo tiempo, se crean unos sistemas de acreditaciones para mejorar de alguna manera el nivel de calidad de estas entidades que están o estarán operando en el mercado.

Esta Directiva consagra el principio de no autorización (para establecer servicios de certificación), sin detrimento de la posibilidad de establecer sistemas de acreditación voluntaria (art. 3 Directiva 1999/93/CE). Lo primero constituye la aplicación de una regla mayor como es la libertad de comercio, sobre cuyo tema existe consenso de mantener y no limitar en ninguna de estas nuevas modalidades emergentes vinculadas con las redes telemáticas. Lo segundo lleva como propósito la mejora de los niveles de calidad de estos servicios, a través de un reconocimiento particularizado, de tipo exclusivamente técnico, que permita la competencia en la materia.

Esta estrategia normativa también permite, en los casos de prestadores reconocidos o inscritos como tales, una serie de controles administrativos.

Las funciones que cumplen estos prestadores son fundamentalmente las de emitir certificados electrónicos con la tecnología necesaria para ello, y también revocarlos bajo determinadas causales. Con este último propósito, se publican listas de las suspensiones o revocaciones.

En el caso de Estados Unidos, el texto normativo federal “Electronic Signatures in Global and National Commerce Act” del 30 de junio de 2000, consagra la validez para

las formas electrónicas de documentación, incluyendo la firma electrónica, por la vía de establecer que ninguna ley, estatuto, regulación o cualquier otra regla de derecho (incluyendo los contratos) pueden denegar efecto legal, validez y fuerza probatoria a dicha documentación por el solo hecho de tener forma electrónica.

Esta norma federal protege al consumidor en las transacciones electrónicas. Para ello exige que el consumidor debe consentir el uso del medio electrónico y no haya revocado dicho consentimiento, y que se le haya informado a través de un estatuto detallado en cuanto a derechos, opciones, etc.

En los casos de los países latinoamericanos analizados, todos tienen sus leyes particulares en la materia, y todos siguen, en mayor o menor medida, la Ley Modelo de la CNUDMI, a excepción de Perú y Costa Rica (en la sección correspondiente se hizo un análisis de legislación comparada, y hay una sección específica que analiza la Ley 8454 de Costa Rica).

En términos generales, en los textos normativos analizados se impone la tesis de que todas las firmas electrónicas, en principio, son admisibles. Se considera que el elemento más importante que consagra estas leyes sobre comercio electrónico y firmas electrónicas analizadas consiste en que por medio de la normativa, se puede otorgar plena validez legal a la firma digital o electrónica en los distintos países, igualándola en su fuerza legal a la firma tradicional.

Estas leyes reconocen que la mayor parte del desarrollo de todo tipo de comercio se basa hoy día en acuerdos de voluntad entre particulares, en actos o contratos que en su gran mayoría son consensuales, y que sólo requieren el consentimiento de ambas partes para perfeccionarse. Las leyes asimilan los actos y contratos que se realicen de forma digital o electrónica a los contratos consensuales, con lo que les otorga el mismo valor legal y por lo tanto los asimila a una categoría legal de contratación ya existente, evitando así tener que entrar a modificar una serie de normas.

Es decir, las normas expresan la idea de que las firmas electrónicas y los documentos

electrónicos no pueden ser rechazadas a priori por un juez, cualquiera que sea su especialidad, aunque podrán ser valoradas de acuerdo con su diferente nivel de seguridad. En la Ley Modelo de la CNUDMI se expresa que no se puede dar menos valor a la firma electrónica que a la firma tradicional, y por supuesto que la firma digital es el estándar actual, sin perjuicio de que pueda haber otras tecnologías tanto o más seguras que ella.

Otro asunto importante en esta materia es lo relacionado a la jurisdicción y ley aplicables, y como puede verse del análisis realizado, sólo Ecuador establece un artículo en este sentido (artículo 47 Ley 67).

De acuerdo con Vásquez (2002), en una contratación electrónica si no hay una previa aceptación de foro, resulta prácticamente imposible establecer una relación con algún tipo de norma que permita asumir una jurisdicción adecuada.

Por la autonomía de la voluntad, las partes pueden escoger libremente la ley aplicable a un contrato transnacional, los más frecuentes en el comercio electrónico a través de Internet. Las normas de conflicto reenviarían al país que tiene más puntos de contacto con el contrato que se trata.

En los casos que involucran consumidores, y este no haya indicado el foro al que se somete, es necesario establecer que las normas de protección al consumidor tienen prevalencia, y por tanto, la legislación y jurisdicción aplicable será las que mejor convenga a los intereses del consumidor.

En general, los elementos relacionados con la seguridad jurídica y tecnológica, deben desarrollarse e implementarse de tal forma que permita la confianza para que las personas puedan realizar comercio electrónico de manera similar como el comercio tradicional, y este debe promoverse de tal forma que permita el acceso a toda la población consumidora, es decir, sin distinción de su condición socioeconómica y educativa, pues toda persona tiene derecho a que se le ofrezca las condiciones para participar de las ventajas de una sociedad que se informatiza y en este caso, de las

ventajas del comercio electrónico.

Como puede derivarse del análisis anterior, los organismos internacionales y los diferentes países han realizado esfuerzos para dar seguridad jurídica y tecnológica a las transacciones electrónicas. Las soluciones propuestas están relacionadas con la firma electrónica o digital, entidades certificadoras, y el establecimiento de las normas necesarias para asegurar la validez y reconocimiento jurídico de los mensajes de datos o documentos electrónicos, y hacerlos equivalentes a los documentos de papel.

En este sentido se reconoce el esfuerzo de la CNUDMI de trabajar en una Ley Modelo que ha permitido que los países la utilicen para proponer sus propias leyes internas.

Se hace la observación que, en esta materia de comercio electrónico, es necesario que los países establezcan acuerdos o convenios, con normas superiores que dé uniformidad de tratamiento e interpretación y que permita proteger de manera similar a todos los consumidores del comercio electrónico, sin importar el país de donde pertenece.

Las soluciones a los asuntos relacionados con el comercio electrónico deben ser resueltas en instancias a nivel superior al propio país, esto debido a que el comercio electrónico da oportunidad de establecer relaciones a nivel internacional muy fácilmente, y por lo tanto se debe proteger las partes de manera satisfactoria y sin vulnerar los derechos de los involucrados.

De acuerdo con Iriarte (2005), la firma digital en esencia es la misma, tecnológicamente hablando; sin embargo, la diversidad de definiciones genera divergencias semánticas y doctrinales que a su vez generan diversas consecuencias jurídicas. Por lo que resulta importante una armonización en este sentido.

También afirma Irabien (2003), que si se lograra una adecuación jurídica global, la desconfianza que actualmente impera en relación a la firma digital desaparecería, o por lo menos habría menos temor a caer en controversias jurídicas por celebrar actos

jurídicos por medios telemáticos nacionales o internacionales.

Por lo tanto, es necesario armonizar lo relacionado a la normativa sobre firmas y certificados digitales y documentos electrónicos, y establecer una normativa común que de confianza a las partes de utilizar el medio electrónico para realizar transacciones comerciales, como lo ha hecho por ejemplo, la Unión Europea. Se debe analizar la posibilidad de armonizar: ámbito de aplicación, definiciones, alcances y principios, además de las prohibiciones, sanciones, procedimientos, jurisdicción aplicable, instancias de apelación, etc., para evitar interpretaciones diferentes que puedan vulnerar los derechos de las partes involucradas, y sobre todo cuando las partes pertenecen a diferentes países e involucren a consumidores.

Indica Iriarte (2005), que se requiere de una normativa subregional y regional que facilite el uso transfronterizo de las firmas digitales y certificados digitales emitidas en la región; sin embargo, por la misma característica del comercio electrónico que permite posibilidades de establecer negocios más allá de una subregión o región, sino más bien que tiene alcance mundial, la normativa debería ser mundial.

Es importante aprovechar el momento histórico en que se encuentra el desarrollo de la normativa jurídica del comercio electrónico, para establecer las relaciones necesarias entre grupos de países y tratar de establecer un marco jurídico adecuado y lo más uniforme posible.

La diversidad de definiciones y principios puede afectar la interpretación de las normas y provocar la vulneración de derechos de las partes involucradas. Es necesario un trabajo conjunto para llegar a obtener un marco jurídico adecuado para todos.

Costa Rica ha realizado un enorme esfuerzo para promulgar la Ley 8454 y su reglamento. Esta Ley, aunque difiere en la redacción de Ley Modelo, contiene todos los elementos mínimos necesarios para proveer seguridad jurídica a las transacciones electrónicas, sin embargo se detectaron algunos elementos que son necesarios que se incorporen. Se recomienda estudiar la posibilidad de plantear las modificaciones a la ley

o a su reglamento para que incorpore los vacíos encontrados y corrija las debilidades detectadas: referencia a la firma digital y no a la electrónica, no explicita sobre el perfeccionamiento de contratos ni legislación y jurisdicción aplicable, no hay referencia de la prevalencia de las leyes de protección del consumidor, y otras debilidades mencionadas en la sección correspondiente. Entre estas últimas se destaca la limitación de la Ley 8454 para el reconocimiento de certificados emitidos en el extranjero, contraria a lo que sugiere el artículo 12 de la Ley Modelo sobre Firmas Electrónicas.

En cuanto a la seguridad tecnológica provista por esta ley, se considera que el sistema de firma digital y certificados digitales provee un mecanismo bastante robusto para asegurar la autenticidad, la confidencialidad, la integridad y el no repudio en las transacciones electrónicas. Sin embargo, se hace de nuevo la observación, de que esta seguridad, provista por este sistema, puede ser vulnerada a raíz de un error humano, como puede ser la pérdida por parte del titular de su clave privada.

Paralelo con la seguridad de la propia transacción electrónica de contratación, se encuentra las que tienen relación con el pago, para las cuales se han desarrollado diversos mecanismos de pago seguro: dinero electrónico, tarjeta de crédito con protocolo SET, cheques y órdenes de pago electrónicas.

Con relación a la prueba documental electrónica, se considera que los sistemas tecnológicos permiten dar respaldo de la existencia de los documentos electrónicos, siempre y cuando estos no sean borrados de manera accidental o fraudulenta.

En este sentido, el concepto de seguridad va más allá de la seguridad de la transacción electrónica, debe considerarse la seguridad de la información en los destinos y lugares de procesamiento y almacenamiento, para evitar accesos y usos no autorizados, así como pérdida de información por accidentes o desastres.

Capítulo 5. Privacidad y protección de los datos

La protección de datos se refiere el amparo de los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, y las facultades de control que un ciudadano debe tener sobre el flujo de informaciones que circulan sobre él.

El nuevo escenario del desarrollo de las tecnologías de información y comunicación, que incluye el desarrollo de Internet y del comercio electrónico, ha generado una amenaza, como nunca antes lo había sido, para la privacidad y protección de los datos personales de los usuarios, que ha obligado a los Estados a repensar los medios utilizados hasta ahora para proteger la intimidad de los ciudadanos.

De acuerdo con Chirino y Carvajal (2003), las sociedades modernas se encuentran ante el dilema de proteger la intimidad, pero al mismo tiempo deben crear las condiciones para mejorar la comunicación de los ciudadanos, así como su autodeterminación. Tienen que velar por un mayor intercambio de informaciones y hacer transparentes muchos usos de la información, y al mismo tiempo garantizar realmente la privacidad de los ciudadanos afectados por dichas políticas.

De acuerdo con Chirino y Carvajal (2003), el derecho a la intimidad debe ser considerada en una nueva dimensión, el de la tutela de las posibilidades de participación reales del ciudadano en una sociedad que se informatiza. Esta nueva dimensión de la intimidad debe considerar la autodeterminación y las facultades de control que un ciudadano debe tener sobre el flujo de informaciones que circulan sobre sí mismo. Se trata de brindar nuevas condiciones de participación social a los individuos, pero, al mismo tiempo, asegurarles el resguardo de su autodeterminación.

Estos autores indican que la apertura de la circulación de las informaciones enfrenta al individuo a numerosos riesgos de perder su intimidad y privacidad, informaciones que se utilizarán para los más diversos fines, lícitos en algunos casos e ilícitos en otros.

Por otro lado, la importancia de la información sumada al fácil y expedito tratamiento (recolección, almacenamiento, circulación, publicación y transferencia) de la misma gracias a la tecnología, han convertido los datos personales en un bien valioso cuyo uso o comercialización constituye el principal negocio de muchas empresas. Además, los datos personales de los ciudadanos son cedidos o vendidos a empresas nacionales e internacionales para diversas finalidades no conocidas por los titulares de los datos (Remolina, 2003).

Se trata por tanto de garantizar al titular de los datos que los terceros, ya sea del sector público o del sector privado, utilizarán sus datos personales con el respeto debido, de forma que el titular de los datos pueda tener un control sobre ellos, y saber, en todo momento, qué se va a hacer con sus datos, para qué los recoge, cómo los trata y para qué los utiliza o a quién se los cede o comunica.

La intimidad es un derecho fundamental que debe ser respetado por todos, comenzando por la concientización y formación adecuada sobre los derechos del propio sujeto titular de los datos.

5.1 Principios y garantías de protección de los datos y el comercio electrónico

En el tema de la protección de la información personal se reconoce la existencia de una serie de principios generales, garantías y excepciones. Los principios generales son esenciales para garantizar, en forma directa, la adecuada protección de la información personal (y, en algunos casos, los intereses legítimos de personas jurídicas), e indirectamente, para salvaguardar los derechos a la privacidad, al honor, a la reputación, a la libertad de expresión (incluyendo la libertad de prensa), entre otros; mediante la generación de un adecuado marco jurídico en donde puedan hacerse efectivos todos y cada uno de estos derechos y garantías fundamentales del hombre.

De acuerdo con Sarra (2001), los principios generales responden a los siguientes fundamentos:

a) Legitimidad y buena fe: se refiere a que la información personal debe ser procesada en forma legítima y no pueda ser utilizada con fines contrarios a la buena fe.
b) Especificación de la finalidad, racionalidad y duración: se refiere a que el tratamiento de la información debe realizarse con fines determinados, que deben ser explícitos y legítimos; y para su divulgación debe mediar consentimiento del titular. La racionalidad de su utilización implica que los datos deben ser utilizados para los fines para los que fueron recolectados. Además la información solo deberá ser conservada por un período de tiempo razonable para la consecución de los fines para los cuales fue recolectada.
c) Pertinencia y exactitud: La información sometida a procesamiento debe ser adecuada, pertinente y no excesiva con relación al ámbito y los fines.
d) No discriminación: Se debe evitar el tratamiento de los datos de las personas que pueda converger en actos ilegítimos o discriminatorios. Para esto se ha establecido la prohibición de compilar datos sensibles que incluyan información sobre el origen racial o étnico, vida sexual, opiniones políticas, religiosas, filosóficas o cualquier otra creencia y la pertenencia a asociaciones, sindicatos, etc. Es decir, cualquier tipo de información que pudiera derivar en actos de discriminación sobre las personas.
e) Confidencialidad y seguridad de la información: Se debe garantizar que la información personal sólo será tratada por personas autorizadas, y que ésta información estará protegida contra destrucción, pérdida, alteración o difusión, accesos no autorizados, utilización fraudulenta, contaminación por virus de computadoras, etc. Para esto se deberán adoptar las medidas técnicas de seguridad y de organización necesarias para garantizar un adecuado resguardo de los datos.

Para que estos principios puedan ponerse en operación, se deben ofrecer las siguientes garantías, de acuerdo con Sarra (2000), Téllez (2004) y LOPD (1999). Se comenta además su importancia en el ambiente de comercio electrónico.

a) Derecho de conocimiento: los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
    1) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información;

2) de las consecuencias de la obtención de los datos o de la negativa de suministrarlos;
3) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas;
4) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición;
5) de la identidad y dirección del responsable del tratamiento o de su representantes.

Este derecho de conocimiento es aplicable al comercio electrónico, y aun cuando el consumidor no compre ni contrate nada y sólo haya navegado en la Red, acción que por sí sola se considera un acto de comercio o de consumo, tal como lo sería en el comercio tradicional, el que un consumidor visitara diferentes establecimientos comerciales requiriendo información sobre determinados productos con el fin de adoptar una decisión de consumo. Generalmente para acceder a la información de una página Web ya sea para comprar o no, se solicita que el usuario dé cierta información personal, pero no se explica para qué lo requiere o si estos datos serán objeto de algún tratamiento, cedidos o vendidos a terceros.

El desarrollo de Internet y del comercio electrónico ha generado una amenaza para la privacidad de los consumidores. Internet permite a los proveedores recolectar, analizar y usar la información con gran facilidad y eficiencia. Y en muchos casos sin que el propio consumidor se de cuenta de ello.

Una transacción por Internet generalmente requiere que el consumidor provea de una cantidad de información que normalmente en el comercio tradicional no se solicita. Además, en Internet es usual el ofrecimiento de servicios gratuitos a cambio de información de los usuarios. Toda esta información es recopilada sin informar al consumidor la utilización que se le va a dar, las medidas de protección que tendrán, ni los derechos que tiene sobre ella (acceso, rectificación, oposición).

También cuando el consumidor navega por Internet, él desconoce que su navegación puede ser grabada por mecanismos de seguimiento. Las compañías de comercio electrónico utilizan numerosos métodos para identificar y efectuar seguimientos de los consumidores en la red. Uno de los métodos más conocidos actualmente consiste en la utilización de las denominadas “cookies”. Estas consisten en que los sitios donde se visita deja una pista en el disco duro (cookie) del usuario. Esta pista permite al sitio conocer las veces que el consumidor visita al sitio y hacer un seguimiento de la actividad del consumidor, pudiéndose crear así un perfil de gustos de éste. El titular del sitio puede negociar con determinadas empresas la transmisión de los datos que luego será utilizado en campañas publicitarias dirigidas a seguros potenciales consumidores.

Solo el hecho de grabar pistas en el disco duro del consumidor ya es una flagrante violación a la privacidad. Aunque el consumidor puede fijar el nivel de seguridad de los cookies, lo cierto es que la mayoría de los consumidores no tienen conocimiento sobre ellos, por lo tanto, aceptan niveles bajos de protección de cookies sin conocer lo que son ni sus implicaciones.

Por otro lado, muchos sitios Web requieren para que puedan acceder a ellos, el permiso para grabar cookies, de lo contrario no permiten que los consumidores accedan a sus páginas. Al menos en estos casos, se le está haciendo saber al consumidor la posible grabación de cookies, y es decisión de él si acepta o no. Pero como se dijo antes, la mayoría de los consumidores desconocen qué son, para qué sirven y sus consecuencias.

La ilicitud de esta práctica reside en la invasión de la esfera personal y por consiguiente en la vulneración del derecho a la intimidad de una persona. Además, una vez obtenidos esos datos de forma ilícita, el consumidor no podrá nunca controlar el fin para el que podrían ser utilizados, que incluso podrían trascender el simple ámbito publicitario.

La posibilidad de que, una vez conocidas sus preferencias, el sujeto pueda ser objeto de comunicaciones comerciales no solicitadas ni deseadas agrava dichas conductas.

Esto último lleva a la problemática del “spam” o correo electrónico comercial no solicitado.

La información de las direcciones de correo electrónico puede ser obtenida de muchas formas y permiten al proveedor enviar publicidad y así reclutar nuevos consumidores. La información de las direcciones fue entregada a terceros sin que el consumidor supiera de ello.

b) Derecho a que los datos sean de calidad: los datos que se recolecten deben ser exactos, pertinentes, adecuados y no excesivos, y recolectados para los fines determinados.

En el comercio electrónico, muchas veces el objetivo consiste en obtener la mayor cantidad posible de información sobre el consumidor, para poder determinar sus intereses y hábitos de consumo, creando verdaderos perfiles humanos, y así poder dirigir una publicidad que difícilmente el consumidor podrá rechazar. Además, esa publicidad es enviada al consumidor sin su consentimiento e irrumpe la privacidad de éste cuando se encuentra navegando por Internet.

Los datos que se recolecten debe ser solo para la identificación del usuario o consumidor, y no debe solicitarse datos que no sean relevantes para la transacción que se está realizando. Además los datos que se recolecten deben ser exactos, es decir, no contener errores que luego pueda perjudicar al propio consumidor. Dentro de esta exactitud, se considera también que los datos deben ser actuales, pues los datos muy antiguos pueden no reflejar adecuadamente la situación del titular y por tal motivo deben ser corregidos o eliminados.

La pertinencia de los datos depende del tipo de transacción, en el caso de una compra y venta electrónica, los datos serán los necesarios para realizar la contratación electrónica. No se deben pedir más datos de los necesarios, ni otros que no interesen para dicha transacción. Y solo serán usados para llevar a cabo la compra y venta, y almacenados el tiempo necesario para respaldar la transacción y cualquier reclamo de garantía u otra disconformidad.

c) Derecho de acceso: las personas tendrán derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

Este derecho es importante en el comercio electrónico, ya que es tanta la información que se intercambia, que puede que las propias personas no recuerden o sepan la información que han autorizado a recabar y las condiciones en que lo han hecho, por lo que este derecho les permitirá conocer el flujo de datos que sobre ellas se tiene, y lograr ejercer los derechos de cancelación y oposición, si lo desean. Estos derechos junto al de conocimiento, componen el denominado *habeas data o habeas scriptum* de acuerdo con Del Peso (2000).

El problema del comercio electrónico, es que el mismo usuario no tiene control de todos los sitios Web que ha visitado y menos aquellos en donde ha entregado información personal, por lo tanto, es difícil que pueda ejercer un derecho de acceso a sus datos, cuando no se acuerda de los sitios visitados. Los programas navegadores guardan un registro de los sitios visitados, esto podría facilitarle al usuario la memorización de los lugares donde entregó información personal, pero esto solo es posible si el equipo desde donde accedió a Internet sea de uso personal o restringido.

d) Derecho de rectificación y cancelación: permite que el interesado solicite una modificación en los términos de alteración o ampliación, o una supresión o cancelación de aquellos datos que, referidos a su persona, considere como inexactos o irrelevantes o que requieran actualizarse.

Lograr la rectificación o cancelación de los datos almacenados en un archivo sobre una persona cuando no sean correctos permite evitar una toma de decisión que puede afectarle.

Para ejercer este derecho, el titular de los datos debe conocer el contenido de los datos almacenados sobre él, para poder saber si son correctos o actuales, y en caso contrario solicitar la rectificación o supresión.

Muchas veces ocurre que los datos son almacenados por un período largo de tiempo en bases de datos de los sistemas de información, y no son actualizados. Es deber del titular conocer en dónde ha entregado datos, y solicitar la rectificación cuando no sean correctos. Pero también es deber del propietario de la base de datos, eliminar los datos después de un tiempo prudencial, este tiempo debe ser solo lo suficiente para respaldar la transacción comercial de eventuales reclamos.

En el ambiente de comercio electrónico, el deber del titular de conocer dónde ha entregado datos es a veces imposible de cumplir, como se vio anteriormente, o una carga de trabajo que desalentaría el uso de la Red. Por otro lado, el deber del propietario queda a la confianza y buena fe de que lo hará, sin ninguna garantía de su cumplimiento.

e) Derecho de oposición: permite a los interesados a oponerse, al tratamiento de los datos que le conciernen. En este caso sus datos deben ser dados de baja en el tratamiento, cancelándose las informaciones a su simple solicitud.

Esto es cuando el titular de los datos no esté de acuerdo con su procesamiento, o no desee que sus datos sean considerados en el procesamiento, puede presentar su oposición y sus datos deberán ser cancelados.

Para que la oposición se pueda dar, el titular de los datos debe conocer la utilización que se les está dando a ellos, y esto, en el ambiente electrónico, puede ser difícil, puesto que el titular entrega los datos para la transacción que realiza, pero desconoce la utilización que le puedan dar después. El problema viene por la falta de control que tiene el titular sobre los datos personales que entrega.

En principio, una persona puede oponerse al tratamiento de datos falsos, discriminatorios y sensibles, siempre y cuando conozca del tratamiento.

f) Derecho al consentimiento: En todo procesamiento de datos se requiere que el interesado preste su consentimiento, salvo cuando exista una disposición en contrario.

Otro problema se encuentra en la posibilidad de venta o cesión de la información personal de los consumidores sin el consentimiento de los titulares de la misma.

El problema aquí es que no hay control por el titular de sus propios datos. Una vez que los datos han sido entregados, no es posible para el titular saber para qué serán utilizados, solo media la confianza de que el proveedor los utilizará para los fines de la transacción electrónica, pero no hay certeza de que así lo sea. No hay control por el propietario de que sus datos personales serán utilizados correctamente para el fin determinado y que le solicitarán su consentimiento para utilizarlos para otros fines.

Una norma en este sentido al menos establecería la obligación de que los datos personales solo pueden ser procesados o cedidos a terceros si el titular ha consentido su procesamiento y lo haya autorizado, y da la posibilidad de reclamar cuando este derecho se haya violado.

g) Derecho a fijar el nivel de protección: Mediante el derecho de autodeterminación se otorga a la persona la posibilidad de determinar el nivel de protección que desea que se otorgue a los datos que le conciernen. Por otro lado, el responsable del tratamiento de los datos deberá adoptar medidas técnicas y de organización apropiadas para asegurar la protección de los datos contra daños, pérdidas o accesos no autorizados.

Esto permite que la persona decida el nivel de seguridad que desea para sus datos personales. Sin embargo, esta decisión conlleva el establecimiento de ciertos parámetros de tipo técnico que generalmente no lo realiza el propio usuario sino que es una decisión que lo hace un técnico informático o personal afín. Lo que significa que el nivel de seguridad, al fin y al cabo, no lo define el usuario y debe confiar en la definición

del nivel de seguridad que lo realiza una tercera persona (administrador de la Red, proveedor de servicios, etc.).

Por otro lado, en el comercio electrónico, los propios proveedores deberían ofrecer el máximo nivel de seguridad a la información personal que solicitan, para proteger los datos de usos fraudulentos, accesos no autorizados, pérdida, alteración o difusión. Generalmente, en el comercio electrónico, las medidas de seguridad para almacenar los datos personales no son suficientes, y esto hace más vulnerable la intromisión a las bases de datos y la sustracción de datos sensibles.

Una de las razones de esta insuficiencia del nivel de seguridad en la protección de datos se debe a la ignorancia del proveedor así como del consumidor, los cuales desconocen las grandes posibilidades que existen a nivel tecnológico de que terceros accedan a la información que viaja en la red o que está almacenada en un sitio, y la alteren o utilicen para fines no autorizados, sin que el titular o el proveedor se de cuenta de ello.

h) Derecho de uso conforme al fin consiste en que el interesado pueda exigir que su información personal sea destinada para los objetivos específicos por los cuales se proveyó.

Se debe garantizar que la información no será utilizada para otros fines. En el comercio electrónico ocurre que los datos que recopilan del consumidor luego se utilizará para enviarle publicidad no solicitada, o también puede pasar que su información sea vendida o cedida a otras empresas para fines mercadotécnicos.

¿Cuáles son los mecanismos que tiene el consumidor para saber y controlar los datos que entrega en una transacción de comercio electrónico? Y ¿cuáles procedimientos existen para poder reclamar cuando se da cuenta que sus datos están siendo usados para otros fines? Estos problemas requieren soluciones a nivel normativo, que permita exigir el uso de los datos conforme al fin.

Por lo tanto, se debe garantizar al consumidor que sus datos sólo serán utilizados para los efectos de concretar la transacción comercial electrónica. Y se debe consultar al consumidor su conformidad para darle cualquier otro uso a sus datos.

i) Derecho para la prohibición de interconexión de archivos: este derecho se refiere a que las distintas bases de datos que contienen información personal no puedan consultarse y/o vincularse indistintamente.

Este derecho en el ambiente de comercio electrónico es muy importante, porque puede evitar la interconexión de archivos para la creación de perfiles del usuario, o para conocer con detalle todas las transacciones que realiza o llevar un seguimiento de donde se encuentre ubicado.

La interconexión de bases de datos permite la recopilación masiva, instantánea e indiscriminada de datos sobre una persona desde cualquier parte del mundo. Es fácil incorporar información personal en bases de datos y transferirla a terceros u otras bases de datos ubicadas en cualquier parte del mundo, además puede ser unida y compilada en segundos para hacer referencia a cualquier aspecto de la persona: datos biográficos, datos de domicilio, datos familiares, datos laborales, información financiera, información médica, información ideológica, información académica, información policíaca, pasatiempos, hábitos, información sobre viajes y comunicaciones, información patrimonial, entre otros.

Es muy fácil que un tercero obtenga excesiva información sobre una persona alrededor del mundo sin que la misma lo haya autorizado o no se entere de qué está pasando con su información, quién la tiene o para qué la está utilizando.

j) Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente: este derecho pretende asegurar al interesado que no será sometido a una decisión que pudiera tener efectos jurídicos significativos sobre él, cuando ésta hubiere sido adoptada sobre la única base de un tratamiento automatizado de datos y fuera destinada a evaluar determinados aspectos de su

personalidad, conducta, fiabilidad, rendimiento laboral, etc. Con este objetivo, se otorga al interesado la posibilidad de impugnar los actos administrativos o cualquier decisión privada que implique una valoración de su comportamiento en las circunstancias aludidas.

En la actualidad, prácticamente todos los procesos de selección y otorgamiento de beneficios, becas, incentivos, bonos, créditos u cualquier otro tipo de beneficio, se realizan a través de sistemas de información automatizados. Estos sistemas se alimentan con datos de los solicitantes y mediante una fórmula diseñada automáticamente con parámetros establecidos en la programación (que estandarizan una situación) realizan la valoración de cada una de las solicitudes y da un resultado que permite a la administración u otra tomar las decisiones de otorgamiento de los beneficios. Generalmente esta fórmula se diseña para capturar los valores de los datos con los cuales realiza el cálculo o evaluación correspondiente.

Se debe permitir al consumidor aportar otros elementos que pueden ser considerados para tomar una nueva decisión sin intervención del sistema. Pues no es posible estandarizar todos los casos, siempre existirán excepciones que se deben considerar de forma separada.

Este derecho permite que el individuo impugne valoraciones realizadas sobre la base de un tratamiento automatizado, permitiendo que la persona pueda presentar nuevos datos para su consideración y realizar una nueva valoración.

k) Derecho de indemnización: Este derecho se refiere a la facultad que poseen los afectados por infracciones a la normativa de protección de datos, de ser indemnizados.

Esto es importante, porque en el comercio electrónico donde interviene un consumidor, éste es la parte más vulnerable que debe ser protegida por el Estado. Cualquier daño que sufra el consumidor debido a la transacción comercial electrónica, debe ser indemnizado por el proveedor.

En el comercio electrónico, esto se complica en las transacciones que traspasan fronteras. Se deben establecer mecanismos que permitan la indemnización de forma ágil y eficaz para los consumidores.

l) Derecho de tutela: este derecho otorga a las personas la facultad de reclamar ante la autoridad competente, frente a las actuaciones contrarias o que violen sus derechos sobre la protección de sus datos personales.

El Estado debe establecer el organismo competente o los procedimientos adecuados que asegurarán la protección de las personas frente al tratamiento indebido de sus datos personales, o cuando se le deniegue el ejercicio de cualquiera de sus derechos. Se debe establecer mecanismos ágiles y eficientes para los casos en que la violación de los derechos ocurre por un proveedor o empresa no ubicada en el país.

La garantía de ciertos derechos debe proveerla el Estado (tutela, indemnización) para que el consumidor pueda tener acceso al reclamo cuando considere que sus derechos han sido lesionados.

m) Derecho a la no discriminación: se refiere a que se prohibirá la recolección de datos sensibles que puedan resultar en la discriminación de las personas por su condición, ya sea: social, étnico, sexual, salud, político, religioso, filosófico, gremial, etc.

En el comercio electrónico se debe evitar la recolección de datos sensibles, solo se debe recolectar los datos necesarios para concretar una contratación de compra y venta electrónica.

Es necesario educar al consumidor sobre sus derechos y responsabilidades, para que pueda realizar compras seguras y satisfactorias en Internet, que permita un adecuado equilibrio entre el desarrollo de la economía y su protección como ciudadano.

Haciendo un recuento de las actividades que realiza un consumidor para llevar a cabo una transacción de compra y venta electrónica, y considerando el análisis anterior se puede identificar que en una compra y venta por Internet, debe cumplirse lo siguiente, para proteger la privacidad del consumidor:

1- Informar al consumidor si el sitio que accede está grabando cookies en su computador, y las consecuencias de ello. Es decir, informar desde este momento sobre los cookies y para qué sirven, y obtener el consentimiento del consumidor.
2- El consumidor debe ser responsable de informarse para fijar el nivel de seguridad adecuado a sus intereses.
3- Informar al consumidor si el sitio está grabando su información personal electrónica y no electrónica y el uso que se dará a esa información y consultar si está de acuerdo.
4- Informar sobre el nivel de protección que tendrá sus datos, y que estos no serán cedidos, vendidos o transferidos a terceros sin su consentimiento. El nivel de seguridad debe proteger los datos de usos fraudulentos, accesos no autorizados, pérdida, alteración o difusión.
5- En caso de que la transacción comercial sea con una empresa ubicada en el extranjero, informar al consumidor si sus datos serán transferidos a un país con poca protección de datos personales, para obtener su consentimiento para la recolección de datos.
6- Consultar al consumidor si desea que se le envíe publicidad a su dirección electrónica o cuando se encuentra navegando por Internet.
7- Informar los derechos que tiene el consumidor sobre sus datos, si puede consultarlos, rectificarlos, oponerse a su procesamiento, o acceder a ellos en cualquier momento.
8- Los datos que se recolecten debe ser exactos, pertinentes, adecuados, no excesivos, y utilizados conforme al fin establecido (para la transacción de compra y venta electrónica), y se mantendrá por un período finito de tiempo (lo necesario para respaldar la realización de la compra y venta electrónica y los casos de cumplimiento de garantías).

9- Prohibir que se interconecten archivos para procesar datos de un consumidor para obtener perfiles de sus actividades, sin su consentimiento expreso.
10- Prohibir la recolección de datos sensibles que puedan después utilizarse para negar una venta o un servicio al consumidor, o tratarlo de manera diferente.
11- Permitir que el consumidor impugne una valoración que se ha tomado con base solo a los datos procesados automáticamente. Y valorar su condición tomando en consideración otros datos aportados por él que pueden cambiar su valoración inicial.
12- El Estado debe garantizar la tutela de las personas a la protección de sus datos personales, y en consecuencia también los derechos del consumidor a la protección de sus datos personales. Y la indemnización de las personas cuando sus derechos han sido lesionados.
13- El Estado debe informar y educar a las personas para que puedan establecer relaciones de consumo responsable (tome sus propias medidas de seguridad, conozca lo que ocurre en la red, sea cauto al realizar una transacción comercial electrónica, se cerciore para qué le piden datos personales y los derechos que tiene sobre ellos, y sobre todo que conozca los procedimientos para reclamar cuando sus derechos le sean violados).

5.2 Disposiciones de organismos internacionales

En cuanto a la vida privada y en especial los datos personales, existe a nivel mundial, una preocupación para su protección.

A raíz de los desarrollos tecnológicos, a comienzos de la década del 70 los países europeos comenzaron a sancionar leyes de protección de datos. Esta corriente continuó en la década de los 80 con la aprobación de acuerdos internacionales, en especial las directrices de la OCDE y el Convenio del Consejo de Europa para la Protección de las Personas con relación al Tratamiento Automatizado de los Datos de Carácter Personal, abierto a la firma en Estrasburgo el 28 de enero de 1981 (Palazzi, 2002).

Y luego veinte años después, la Unión Europea decidió armonizar estas legislaciones a través de una Directiva sobre la materia.

Un resumen de los principios rectores establecidos por estos organismos puede verse en el anexo 11.

5.2.1 OCDE

La OCDE adoptó el 23 de setiembre de 1980 sus líneas directivas relativas a la protección de la vida privada y los flujos transfronterizos de informaciones. Esta Recomendación constituye el primer documento de ámbito supranacional que analiza en profundidad el derecho a la protección de datos de carácter personal y establece los principios fundamentales de este derecho.

Su adopción se funda en la constatación por parte del Consejo de la OCDE de la inexistencia de una uniformidad en la regulación de esta materia en los distintos Estados miembros que dificultaba el flujo de datos personales entre los mismos. Por esta razón, la Recomendación tiene la finalidad de establecer unas reglas básicas reguladoras del derecho que garanticen la inexistencia de obstáculos a la libre transferencia internacional de datos entre los Estados miembros.

Estas líneas directivas establecen los siguientes principios fundamentales que han de regir el tratamiento de datos de carácter personal y que han de guiar la regulación nacional que pudiera ser adoptada en esta materia. Estos principios son los siguientes (OCDE, 2002):

- principio de limitación en materia de recopilación de datos: se debe establecer límites para la recogida de datos, la obtención debe ser por medios lícitos con el consentimiento del sujeto.
- principio de la calidad de los datos: datos deben ser relevantes para el propósito de su uso y en la medida de lo necesario, deben ser exactos, completos y actuales.

- principio de la especificación de la finalidad de la recopilación: se debe especificar en qué se usarán los datos.
- principio de limitación de uso: los datos no deben ser usados para otros propósitos, excepto cuando se tenga el consentimiento del titular o por imposición legal o de las autoridades.
- principio de salvaguardia de la seguridad: se debe dar protección razonable de seguridad a los datos contra pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación.
- principio de transparencia: se debe tener una política general de transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales, contar con medios ágiles para determinar la existencia y naturaleza de datos personales, el propósito de su uso e identificar y ubicar al controlador de los datos.
- principio de la participación individual: se refiere al derecho de acceso y de rectificación.
- principio de responsabilidad: el controlador de los datos es responsable del cumplimiento de las medidas que hagan efectivos los principios anteriores.

Estos principios han sido una guía para que los países desarrollen su normativa sobre la protección de los datos personales.

Se resalta el hecho de que la Recomendación no hace referencia a la creación de autoridades nacionales de protección de datos personales, sino que únicamente impulsa la adopción de medidas nacionales de desarrollo de las directrices.

Estas directrices se complementan con la adopción, el 26 de noviembre de 1992 de la Recomendación OCDE relativa a la seguridad de los sistemas de información (Puente, 2005).

5.2.2 Naciones Unidas

El 14 de enero de 1990 se aprueba la Resolución 45/95 de la Asamblea General de las Naciones Unidas, relativa a los principios rectores para la reglamentación de los ficheros computarizados de datos personales (conocida como “Directrices de Protección de Datos de las Naciones Unidas”). Esta Resolución establece una lista mínima de principios de protección de datos que deberían ser adoptados por las legislaciones internas de todos sus Estados miembros. De acuerdo con Puente (2005), es el primer documento de ámbito mundial en esta materia.

Los principios básicos reconocidos por la Recomendación 45/95 se resumen en los siguientes (Naciones Unidas, 1990):

- Principio de legalidad y lealtad: la información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni utilizados para otros fines.
- Principio exactitud: obligación de los responsables de comprobar periódicamente la exactitud y pertinencia de los datos y garantizar su completitud. Además de actualizar los datos sometidos a tratamiento.
- Principio de especificación de la finalidad: especificar para qué se utilizarán los datos, informar a la persona interesada y mantener los datos por un período especificado de acuerdo con el fin.
- Principio de acceso de la persona interesada: derecho a conocer, sin demoras ni gastos excesivos, los datos tratados y sus potenciales destinatarios y a que se proceda a la rectificación supresión de los datos cuyo tratamiento sea ilícito, injustificado o inexacto.
- Principio de no discriminación: por el que se establece una regla general de prohibición del tratamiento de datos referidos al origen racial, la vida sexual, las opiniones religiosas o políticas o la participación en asociaciones o sindicatos.
- Facultad para hacer excepciones: Limitación de las excepciones a los principios, por razón de la protección de la seguridad nacional, el orden público, la salud o la moral pública y los derechos y libertades de terceros.

- Principio de seguridad: con la finalidad de proteger los tratamientos contra riesgos naturales o su pérdida accidental, como humanos, como accesos no autorizados, el uso fraudulento de los datos o contaminación de virus informáticos.
- Supervisión e imposición de sanciones: cada parte debería designar una autoridad imparcial e independiente de supervisión del cumplimiento de los principios y la posibilidad de imposición de sanciones penales o de otra índole por la contravención de los mismos.
- Transferencias internacionales: debería existir un flujo libre de datos de carácter personal entre Estados que establezcan garantías comparables de protección de la vida privada.

5.2.3 Consejo de Europa

El Consejo de Europa adopta en Estraburgo, el día 28 de enero de 1981, el Convenio 108 del Consejo de Europa. Este Convenio, de acuerdo con Puentes (2005), es el primer instrumento internacional de carácter vinculante adoptado en esta materia, especificando de forma clara los principios y las obligaciones de los responsables de los tratamientos y de los propios Estados signatarios, en la protección de la intimidad y la privacidad de las personas en relación con el tratamiento de sus datos de carácter personal. Las Directrices de la OCDE así como de las Naciones Unidas constituyen simplemente documentos orientadores de la actividad de los Estados miembros de ambas organizaciones, sin perjuicio de la recomendación que los mismos contienen de cumplir los principios establecidos en esos textos.

Los principios básicos de protección establecidos en este Convenio son los siguientes (Convenio 108, 1981):

- Compromiso de las Partes: Cada Parte tomará las medidas necesarias para hacer efectivos los principios básicos para la protección de datos enunciados en el presente Convenio. Las medidas debe adoptarse en el momento de la entrada en vigor del Convenio con respecto a dicha Parte.

- Calidad de los datos: los datos de carácter personal obtenidos para un tratamiento automatizado debe ser obtenidos de forma leal y legítima, para los fines determinados, adecuados, pertinentes y no excesivos, exactos y actuales, mantenidos por el tiempo necesario para el cumplimiento de los fines. Y deben identificar a la persona a quien conciernen los datos.
- Categorías particulares de datos: No pueden tratarse los datos que revelen origen racial, opiniones políticas, convicciones religiosas u otras, datos relativos a la salud, vida sexual, condenas penales.
- Seguridad de los datos: Se deben tomar medidas apropiadas de seguridad para proteger los datos contra destrucción accidental o no autorizada, pérdida accidental, así como contra el acceso, modificación y difusión no autorizada.
- Garantías complementarias para las personas concernidas:
    - Conocer de la existencia de un fichero automatizado de datos de carácter personal, su finalidad, identidad y residencia de la autoridad controladora del fichero.
    - Obtener sin demora ni gastos excesivos la confirmación de la existencia de un fichero con sus datos personales, así como la comunicación de dichos datos en forma inteligible.
    - Obtener la rectificación o supresión de los datos erróneos, inexactos o sensibles.
    - Disponer de un recurso si su petición no se atiende.
- Se admiten excepciones que deben ser prevista por la ley de la Parte y que sea para proteger la seguridad del Estado, la seguridad pública, para los intereses monetarios del Estado, o para represión de infracciones penales; para la protección de la persona y de los derechos y libertades de otras personas; para fines estadísticos y de investigación científica, siempre que no atente contra la vida privada de las personas.
- Sanciones y recursos: Cada Parte se compromete a establecer sanciones y recursos contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos enunciados.
- Protección amplia: No se debe limitar la facultad de cada Parte de conceder una protección más amplia que la prevista en este Convenio.

El Convenio crea una estructura institucional permanente e impone a los Estados miembros la obligación de designar una autoridad que habrá de tener competencias para garantizar la aplicación de los principios del Convenio en el Derecho interno, cooperar con las restantes autoridades designadas e intercambiar información.

El 8 de noviembre de 2001 se emitió un Protocolo adicional del Convenio 108, que completa las previsiones del Convenio en determinadas materias, tales como los movimientos internacionales de datos y la exigibilidad de la existencia en los Estados signatarios de una autoridad independiente cuya función sea velar por el cumplimiento de las disposiciones nacionales adoptadas en materia de protección de datos de carácter personal (Puente, 2005).

5.2.4 Unión Europea

En el caso de la Unión Europea existe una protección bien establecida.

Diversas Directivas, como es el caso de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, tienen el objetivo de armonizar las legislaciones que protegen los datos personales y ofrecer un nivel máximo de garantía a los ciudadanos de la Unión Europea.

Estas Directivas imponen obligaciones sobre quienes adquieren, almacenan, usan, difunden y en general procesan datos personales y al mismo tiempo otorga a los ciudadanos el derecho a consentir ese tratamiento de datos personales y el derecho a acceder a la información almacenada y corregir errores o inexactitudes.

5.2.4.1 Directiva 95/46/CE

La Directiva 95/46/CE, es el texto de mayor relevancia en el marco de la protección de datos en el ámbito Europeo, de acuerdo con Puente (2005), al regular la materia en toda su extensión e implicar su adopción la homogenización de las normas de protección de datos de todos los Estados miembros.

Esta Directiva ha tenido incidencia en la normativa de protección de datos más allá de la propia Unión Europea, dado que las normas de la misma en materia de transferencias internacionales de datos vienen a imponer un régimen básico al que deberán resultar adecuados los terceros Estados no miembros de la Unión, para que los datos puedan ser transmitidos libremente a esos Estados.

La Directiva 95/46/CE establece los siguientes principios para determinar la licitud del tratamiento de datos:

La calidad de los datos: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.

La legitimación del tratamiento: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento.

Se prohíbe el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

La información a los afectados por dicho tratamiento: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernen.

El derecho de acceso del interesado a los datos: para ejercer la rectificación, supresión o bloqueo de los datos cuando no correspondan.

Las excepciones y limitaciones de los derechos anteriores solo en caso de salvaguarda de la seguridad y defensa del Estado o la protección del interesado.

El derecho del interesado a oponerse al tratamiento: el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento.

La confidencialidad y la seguridad del tratamiento: el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizado.

La notificación del tratamiento a la autoridad de control: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

Esta Directiva establece que sus disposiciones “se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero” (Directiva 95/46/CE, 1995, p. 11). De acuerdo con Palazzi (2005), esta Directiva amplía el marco de garantías del derecho a la protección de datos respecto de las directrices de la OCDE y de las Naciones Unidas, así como respecto del Convenio 108, dado que sus aplicaciones serán también aplicables a los tratamientos no automatizados de datos incorporados a ficheros.

Las disposiciones no se aplican al tratamiento de datos personales efectuadas por una persona física en el ejercicio de las actividades exclusivamente personales o domésticas, ni cuando tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal (artículo 3 y 13 de la directiva 95/46/CE).

La Directiva diferencia las figuras del responsable y el encargado del tratamiento, estableciendo en su artículo 17 que es obligación del responsable del tratamiento aplicar las medidas de seguridad para la protección de los datos así como elegir al encargado que reúna las garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas. Además indica que la relación entre el responsable y el encargado debe estar formalizada en un contrato vinculante, que deberá constar por escrito o en otra forma equivalente, imponiendo al encargado la obligación de implantar las medidas adecuadas de seguridad.

En cuanto a la calidad de los datos, hace referencia a los principios de tratamiento leal y lícito, finalidad y prohibición del uso incompatible, proporcionalidad, exactitud y actualización y conservación de los datos exclusivamente durante el tiempo en que sean necesarios para el cumplimiento del fin.

La Directiva delimita claramente los supuestos en que podrá procederse al tratamiento de datos de carácter personal. El artículo 7 indica que se permite el tratamiento en los siguientes casos:

- el interesado ha dado su consentimiento de forma inequívoca, o
- es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
- es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

- es necesario para proteger el interés vital del interesado, o
- es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
- es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

Estos supuestos se ven reducidos en caso de tratamiento de datos sensibles (artículo 8 de la Directiva).

El artículo 15 de la Directiva reconoce el derecho de las personas "a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc." (Art. 15 Directiva 95/46/CE, 1995, p.17).

El Capítulo IV de esta Directiva se refiere al régimen sistemático de las transferencias internacionales de datos a terceros países.

En esta materia, el artículo 25 de la Directiva 95/46/CE establece que se permite la transferencia de datos personales a terceros países solo si dichos países garantizan un nivel adecuado de protección. Su artículo 26 establece excepciones en los casos siguientes: el interesado haya dado su consentimiento, ejecución de un contrato a petición del interesado, necesaria para la salvaguardia de un interés público o vital para el interesado, por disposiciones legales o reglamentarias.

Para el cumplimiento del apartado 2, del artículo 26 de la Directiva 95/46/CE, en la que se establece que los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de

protección adecuado, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas, se emite la Decisión 2001/497/CE del 15 de junio de 2001 y la Decisión 2002/16/CE del 27 de diciembre de 2001.

Estas Decisiones establecen las cláusulas contractuales tipo que ofrecen las garantías adecuadas con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los correspondientes derechos. Esta decisión establece las obligaciones del exportador e importador de datos, la responsabilidad por los daños que se sufran, cooperación con las autoridades de control, legislación aplicable, entre otros elementos. Una sección posterior retoma el análisis de la transferencia internacional de datos.

El artículo 27 de la Directiva 95/46/CE promueve la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales y comunitarios adoptadas por los Estados miembros. Este artículo introduce un régimen relacionado con el fomento de la autorregulación.

Los artículos 28 y 29 de esta Directiva establece que cada Estado miembro designará una o varias autoridades públicas independientes encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la directiva. También crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión.

5.2.4.2 Otras Directivas relacionadas

También se encuentra una serie de directivas relacionadas con la materia de protección de datos que a continuación se mencionan.

El artículo 8 de la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo que establece el marco común de firma electrónica, indica que los Estados deben cumplir con la Directiva 95/46/CE relativa a la protección de la persona física en lo que respecta al tratamiento de datos personales y libre circulación de estos datos. Y la Directiva 97/66/CE relativa al tratamiento de datos personales y a la protección a la intimidad en el sector de telecomunicaciones, también indica que los proveedores de servicios de certificación solo pueden recabar datos personales directamente del titular o con su consentimiento y sólo en la medida necesaria para expedir y mantener el certificado y para ningún otro fin.

La Directiva 97/66/CE establece que los proveedores de servicios de telecomunicación deben adoptar la medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios. Si existe riesgo de violación a la seguridad de la red así deben informarlo a sus abonados.

Establece que los Estados miembros deben garantizar por medio de normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación. Se prohíbe la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas, deroga la Directiva 97/66/CE adicionando otros temas. Establece que las nuevas tecnologías, en particular Internet y el correo electrónico, han de cumplir determinados requisitos para asegurar el derecho a la intimidad. Esta Directiva 2002/58/CE es la norma específica sobre protección de datos en el sector de

las comunicaciones electrónicas, que complementa a la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

La Directiva 2002/58/CE tiene por objeto establecer y garantizar un alto nivel de protección de los datos personales de los abonados y usuarios de los servicios de comunicaciones electrónicas, al tiempo que se respeta el principio de "neutralidad tecnológica". El ámbito de protección conferido por esta Directiva, al igual que ya ocurría con la Directiva 97/66/CE, es el del tratamiento de los datos personales en redes públicas de comunicaciones electrónicas. El artículo 13 de la Directiva 2002/58/CE solo permite la comunicación con fines de venta si el usuario ha dado su consentimiento previamente, no obstante, cuando la dirección de correo electrónico fue obtenida en el contexto de una venta de producto o servicio, se podrá enviar mensajes publicitarios siempre que se permita la oposición posterior del usuario.

Esta Directiva contiene normas esenciales destinadas a garantizar la confianza de los usuarios en los servicios y tecnologías de las comunicaciones electrónicas. Tales normas se centran en la prohibición de los mensajes electrónicos no solicitados (spam), el régimen de acuerdo previo del usuario y la instalación de cookies. También incluye normas sobre la conservación de los datos sobre las conexiones por parte de los Estados miembros con fines de vigilancia policial.

Se encuentra también la Carta de los Derechos Fundamentales de la Unión Europea, que en su artículo 8 establece el derecho a la protección de los datos personales. Indica que los datos se tratarán de modo leal, para los fines establecidos y con el consentimiento del titular, además toda persona tiene derecho a acceder a sus datos y a su rectificación.

La Unión Europea ha promulgado también el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos de la Comunidad y sobre la libre circulación de estos

datos. El Reglamento está destinado a garantizar la protección de los datos personales en el marco de las instituciones y organismos de la Unión Europea.

El texto prevé disposiciones por las que se garantiza un elevado nivel de protección de los datos personales tratados por las instituciones y los organismos comunitarios; y el establecimiento de un organismo supervisor independiente encargado de controlar la aplicación de estas disposiciones denominado Supervisor Europeo de Protección de Datos. Esta instancia será comparable a las autoridades del mismo tipo establecidas por los Estados miembros de acuerdo con la directiva sobre protección de datos. Los ciudadanos podrán así presentar una denuncia directamente ante dicha autoridad si consideran que no se respetan los derechos protegidos por el Reglamento.

El Reglamento permite a los ciudadanos gozar de derechos exigibles legalmente, como los de consulta, rectificación, bloqueo y supresión de los datos personales que consten en los archivos de cualquier institución u organismo de la Comunidad.

En resumen, todas las directivas de la Unión Europea permiten proteger a las personas frente al tratamiento no autorizado de sus datos personales, estableciendo los siguientes derechos: acceso, rectificación, oposición, consentimiento, fijar el nivel de protección, uso conforme al fin; prohíbe el tratamiento de datos personales que revelen datos sensibles; protege la transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado; el uso indebido por parte de las instituciones y organismos del Estado creando un organismo encargado de controlar la aplicación de estas disposiciones denominado Supervisor Europeo de Protección de Datos a nivel de la Unión Europea y no de un país específico.

El enfoque europeo busca otorgar un mayor nivel de protección a los ciudadanos, en vez de otorgar preeminencia a los intereses económicos. Este enfoque también tiene problemas: no fomenta los emprendimientos de comercio electrónico, pues hace que el proceso sea más difícil y complicado; por otro lado, la implementación de las normas no es un proceso fácil ni ágil, pues tardan muchos años para que lleguen a estar en funcionamiento.

Por otro lado, también la Unión Europea ha promovido la autorregulación y la adopción de códigos de conducta como puede verse en las siguientes decisiones.

Mediante la decisión 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999, se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Las líneas de acción de este plan incluyen:

> **"-crear un entorno más seguro** por medio de una red europea de líneas directas (*hot lines*) y el fomento de la autorregulación y la adopción de códigos de conducta;
> **-desarrollar sistemas de filtrado y clasificación**, en particular demostrando las ventajas de estos procedimientos y facilitando un acuerdo internacional sobre el diseño de un sistema de clasificación;
> **-fomentar acciones de sensibilización** a todos los niveles para informar mejor a los padres y a todos los que se ocupan de los menores (profesores, trabajadores sociales, etc.) sobre la mejor manera de protegerlos contra la exposición a contenidos que podrían ser nocivos para su desarrollo;
> **-acciones de apoyo** que evalúen las implicaciones jurídicas, coordinándolas con iniciativas internacionales similares y evaluando el impacto de las medidas comunitarias." (Resumen Decisión 276/1999/CE, 1999, p.2)

Obsérvese que en este Plan se incluye dentro de sus líneas de acción el fomento de la autorregulación y la adopción de códigos de conducta. Además la Directiva 2000/31/CE del 8 de junio de 2000, en su artículo 16 estableció que los Estados miembros promoverán la elaboración de códigos de conducta.

El 11 de mayo de 2005 el Consejo adoptó la Decisión No.854/2005/CE por la que se crea el programa "Safer Internet Plus", con el objetivo de favorecer una utilización más segura de Internet y las nuevas tecnologías en línea. El programa abarcará el período 2005-2008, en sustitución del plan "Safer Internet" (1999-2004). Este Plan igualmente contempla el fomento de la autorregulación y la adopción de códigos de conducta.

Se concluye que la Unión Europea no sólo ha impulsado la creación de una normativa para dar seguridad y protección a la privacidad a los ciudadanos, sino que también ha promovido el fomento de la autorregulación y la adopción de códigos de conducta en la industria.

5.2.5 Estados Unidos

Paralelo al origen de la protección de datos en Europa, el mismo problema comenzó a ser objeto de debate en los Estados Unidos a comienzos de los años 70. En 1973 el Gobierno norteamericano elaboró un estudio recomendando la aprobación de ciertos principios para el tratamiento de datos personales. Estos principios nunca fueron aprobados en una legislación por el Congreso, pero Estados Unidos contó desde un comienzo con dos leyes: la Privacy Act y la Fair Credit Reporting Act, relacionadas con los datos almacenados por el Gobierno y los registros de informes crediticios (Palazzi, 2002).

Después de este comienzo, Estados Unidos se limitó a aprobar leyes de protección de datos personales legislando sólo ciertos sectores y promoviendo la autorregulación como una alternativa eficiente a la regulación estatal.

Para la industria y el comercio, el tratamiento adecuado de la información personal y la confianza de los ciudadanos en dichos tratamientos, son condiciones necesarias para el desarrollo del comercio electrónico.

El tema de la autorregulación surge como una alternativa de la industria y el comercio de llevar a cabo acciones que permita asegurar la protección de la privacidad de las personas sin la necesidad de la intervención del Estado. Esto debido a que mayores regulaciones por parte del Estado pueden obstaculizar el desarrollo del comercio electrónico.

Es por esta razón que Estados Unidos cuenta con un marco jurídico bastante amplio en materia de privacidad, con normas sectoriales sin conexión entre ellas. Indica Velasco (2003), que la política de regulación de los Estados Unidos ha evolucionado de tal forma que hoy en día se ha ocupado más de legislar aquellos sectores que se consideran más sensibles y vulnerables para la sociedad, como son el sector salud y la protección y confidencialidad de la información que proporcionen niños menores de edad a sitios en Internet.

La autorregulación de los Estados Unidos ha estado a cargo en gran medida del sector privado, que ha respondido satisfactoriamente a las necesidades de sus grandes corporaciones y protegiendo en la medida de lo posible los derechos básicos de los consumidores y de los ciudadanos.

En este sentido, Estados Unidos tiene una política mucho más flexible sobre privacidad y protección de datos que la Unión Europea, cuyo objetivo es proteger y tutelar los derechos de consumidores y la población vulnerable y permite un esquema más liberal para el sector empresarial.

Según Velasco (2003), estos mecanismos de autorregulación de las empresas fomentan y reactivan el comercio electrónico, promueven las inversiones del sector de tecnologías de información y permiten que las pequeñas y medianas empresas puedan realizar comercio electrónico en todos los niveles.

De acuerdo con Reidenberg (1999), la autorregulación de los Estados Unidos no ha dado el resultado esperado, es sólo una hipótesis para las empresas americanas, pues la Industria no ha asumido su responsabilidad de la autorregulación. Después de dos décadas, las Industrias no habían implementado políticas efectivas de privacidad.

> 'Por más de veinte años los grupos de trabajo e investigación formados en el gobierno regularmente llamaron la atención sobre la falta de estándares para el tratamiento de datos personales en la sociedad americana, pero en sus conclusiones siempre sostuvieron que "la industria requería mas tiempo para autorregularse"'.(Reidenberg, 1999, p.3).

Sin embargo, en los últimos años, la industria ha mejorado sus iniciativas para la protección de la privacidad. La falta de una alternativa legal y la presión del Gobierno han promovido el surgimiento, de iniciativas privadas, de diversos tipos de servicios encargados de promover la confianza entre consumidor y vendedor y de certificar la credibilidad de una página Web.

En Ferreira (2003) se mencionan las siguientes instituciones encargadas de este tipo de servicios: TRUSTe, BBBOnLine, Entrust Technologies, CPA Web Trust, Open Ratings,

GeoTrust, Webtrust, Betterweb y Verisign. Estas instituciones son una nueva categoría de intermediarios en la red.

TRUSTe: certifica la seguridad de las transacciones y acredita la voluntad de la empresa de proteger la información personal de sus clientes. Es un programa a través del cual las páginas de Internet acuerdan revelar sus políticas de privacidad y son licenciados para usar un logo que indica que ese sitio protege la privacidad.

BBBOnline: es una organización sin ánimo de lucro financiada por sus miembros, proporciona a los consumidores informes de empresas para ayudarles en sus decisiones de compra.

El CPA Web Trust: tiene el doble objetivo de incrementar la confianza del consumidor en la seguridad y la confidencialidad y de dar a conocer el comercio electrónico.

Verisign: se ha convertido en el líder mundial de servicios de confianza para Internet y ofrece autentificación, validación y pago a nivel internacional. Para transacciones elevadas existe la posibilidad de utilizar los servicios de una entidad que garantiza el pago hasta que el comprador recibe y acepta el producto adquirido.

De acuerdo con Ferreira (2003):

> "Se trata de unos mecanismos de autorregulación que se basan en una estructura de autoridades certificadoras, que autentifican la identidad de los participantes. Su modelo de negocio consiste en aconsejar a compradores y vendedores acerca del nivel de calidad, confianza y competencia de una empresa." (Ferreira, 2003, p.1).

Menciona Ferreira (2003) que en España existen también algunas entidades que proveen este tipo de servicios, como la Fábrica Nacional de la Moneda y Timbre (FNMT), la Asociación Española de Comercio Electrónico (AECE), la Agencia de Certificación Española (ACE) y la Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE). La FNMT, que emite diversos tipos de certificados, ha puesto en marcha un proyecto denominado CERES (Certificación Española), que establece una autoridad pública de certificación española que autentifique y garantice la

confidencialidad de las comunicaciones online entre ciudadanos, empresas u otras instituciones y administraciones públicas.

A pesar de estos esfuerzos de autorregulación, estos mecanismos todavía tienen mucho camino que recorrer. Los esfuerzos mencionados tienen muchas debilidades y dificultades que no permiten garantizar al 100% la seguridad requerida.

En Reidenberg (1999) se puede encontrar algunas de las debilidades detectadas de estos mecanismos autorregulatorios, como los que a continuación se mencionan.

TRUSTe puede auditar a los licenciados para verificar el cumplimiento de la política de privacidad. Sin embargo el programa ha tenido varios problemas. Cerca de 450 empresas están licenciadas para usar el logo, pero este es un número trivial comparado con el número de sitios de Internet en Estados Unidos. De hecho, una de las empresas amparadas por este logo, Geocities tiene la distinción de haber sido la primera compañía sometida a un sumario de la Comisión Federal de Comercio por haber traficado información personal, y cerca de un cincuenta por ciento de los promotores de TRUSTe no se han molestado en suscribirse al programa y licenciar el uso del logo.

TRUSTe incluso tiene en su Web un hipervínculo a un servicio de búsqueda de información en Internet que no revela ninguna política de privacidad y pertenece a una compañía que ni siquiera está listada como licenciante de TRUSTe.

En el caso de BBBOnLine la idea es proveer un mecanismo de decisión para disputas sobre privacidad online. El programa comenzó oficialmente el 17 de marzo de 1999. Pero ignora la cuestión de que el consentimiento no puede ser la base adecuada para el procesamiento de cierta información personal, tal como datos sobre salud y sólo requiere a las páginas web revelar ciertas prácticas, carece de remedios legales para las víctimas de violación a la privacidad y no tiene el requisito de proveer acceso completo a los datos personales. Asimismo, BBBOnLine usa una definición muy vaga de “información personal de individuos” sin circunscribir el ámbito de las obligaciones de sus participantes.

Otra iniciativa importante de privacidad surge en mayo de 1998 (Villate, 1998), cuando el World Wide Web Consortium (W3C) aprobó un protocolo de privacidad conocido como Proyecto Plataforma para Preferencias de Privacidad (P3P). Este protocolo es una especificación para que los sitios web expresen sus prácticas de privacidad y los usuarios establezcan sus preferencias sobre dichas prácticas.

Menciona Villate (1998) que Birchman, de la Facultad de Derecho de la Universidad de Miami, considera que "debido a su naturaleza extremadamente técnica, los usuarios de P3P pueden tener que depender crecientemente de terceras partes para establecer la configuración de sus preferencias individuales". Y esto plantea serios interrogantes sobre la existencia de un verdadero control del usuario sobre su esfera privada.

Según Reidenberg (1999), el mecanismo de autorregulación se basa principalmente en la creencia de que la notificación y el consentimiento van a resolver el asunto de la privacidad. E indica que fundarse solo en los principios de “notificación” y “consentimiento” ignora los otros principios básicos de tratamiento de datos personales y demuestra cómo la autorregulación no ha funcionado.

Reidenberg (1999) menciona el ejemplo de la función "*smart browsing*” de los programas navegadores como Netscape Communicator e Internet Explorer, que envían al fabricante un archivo oculto de las direcciones de Internet visitadas por el usuario. Indica que esto es una clara violación a la privacidad, viola los principios de limitación de la finalidad y limitación del almacenamiento temporal pues las direcciones de Internet visitadas son almacenadas más allá de la comunicación con un sitio remoto para procesar perfiles personales.

5.3 Transferencia Internacional de Datos

Dentro del tema de protección de datos se incluye un tema importante que requiere de un análisis aparte para profundizar sobre la problemática y los aspectos de regulación requeridos para evitar abusos y vulneración a la intimidad.

Esta sección hará énfasis al tema de la transferencia internacional de datos. Este tema tiene una relación directa con el comercio electrónico, puesto que el comercio electrónico permite establecer relaciones comerciales en las que necesariamente involucra la transferencia de datos personales desde el consumidor al vendedor, y es probable que esta transferencia de datos traspase fronteras nacionales.

5.3.1 OCDE, Convenio 108 del Consejo de Europa, Directivas de la Unión Europea

Con relación a este tema, la OCDE publicó en sus Directrices sobre protección de la privacidad y flujo transfronterizos de datos personales de 1980, un capítulo sobre Principios básicos de aplicación internacional: restricciones en el flujo y la legitimidad.

Este capítulo establece que no se debe restringir el intercambio de datos personales con otros países miembros, excepto cuando el país receptor todavía no observe de forma sustancial las directrices sobre privacidad.

También se permite que un país miembro restrinja el intercambio de datos a ciertas categorías de datos personales sobre las que rijan normativas específicas, contenidas en su legislación nacional sobre privacidad, que por su naturaleza no tiene una protección equiparable en el país receptor.

Los países miembros deberán seguir todos los pasos razonables y apropiados para asegurar que el flujo transfronterizo de datos personales, incluido el tránsito a través de un país miembro, se realice de forma ininterrumpida y segura.

Indica que los países miembros deberán evitar la elaboración de leyes, políticas y prácticas destinadas a proteger la privacidad y las libertades individuales que pudieran crear obstáculos al flujo transfronterizo de datos personales excediendo los requisitos para tal protección.

El Convenio 108 del Consejo de Europa establece en su artículo 12 sobre el flujo transfronterizo de datos de carácter personal. El artículo establece la regla general de

que una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte. No obstante, esta regla podrá verse exceptuada en dos supuestos: cuando exista un incumplimiento de las obligaciones previstas en el Convenio, exigidas por su artículo 4 o cuando el Estado de destino sea un mero paso intermedio para la transmisión de los datos desde un Estado signatario a otro no signatario.

El 8 de noviembre de 2001 se emitió un Protocolo adicional del Convenio 108 que tiene como objeto subsanar las lagunas del Convenio 108 y garantizar su aplicación por los Estados Parte, perfeccionando asimismo el régimen de las transferencias internacionales de datos.

El artículo segundo del Protocolo dispone que cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección. Dicha regla sólo se verá exceptuada si el derecho interno así lo establece a causa de intereses concretos del afectado, o intereses legítimos, especialmente los de carácter público, o si se prevén las suficientes garantías, que pueden resultar, en particular, de cláusulas contractuales, por parte del responsable del tratamiento y dichas garantías se estiman adecuadas por las autoridades competentes de conformidad con el derecho interno (Puente, 2005).

En el caso de la Unión Europea, el Capítulo IV de la Directiva 95/46/CE regula la transferencia de datos personales a terceros países. La Directiva prohíbe la transferencia de datos personales a países que no tengan leyes adecuadas de protección de datos.

En el artículo 25 de su directiva 95/46/CE establece que la transferencia de datos personales a un tercer país solo es posible si ese país garantiza un nivel adecuado de protección. Y en su artículo 26 establece excepciones, es decir, establece las situaciones en que los Estados miembros podrán efectuar una transferencia de datos

personales a un país tercero que no garantice un nivel de protección adecuado, con arreglo al apartado 2 del artículo 25 que indica:

> "2.El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países." (Directiva 95/46/CE, 1995, p.21)

La normativa comunitaria evidencia la preocupación europea por evitar un tratamiento inadecuado de los datos personales y la necesidad de establecer un control que marque unos límites de garantía y seguridad en la transferencia de los datos personales que cruzan fronteras.

Por otro lado, el intercambio de datos entre distintos países, es necesaria para la evolución y el ejercicio de actividades económicas, así como garantía y respeto a la libre circulación de personas y cosas, dentro de los límites y acatamientos, en beneficio de las relaciones sociales, culturales y económicas entre los pueblos.

Este control está establecido en el artículo 25, inciso 3, que indica que los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado. Si la Comisión comprueba que un tercer país no garantiza un nivel de protección adecuado de privacidad, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate (artículo 25 inciso 4). A su vez la Comisión debe iniciar en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4 (artículo 25 inciso 5).

Las excepciones, indicadas en el artículo 26 de esta misma directiva, son las siguientes:

> "1.No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:
>
> 1. el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

> 2. la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
> 3. la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
> 4. La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
> 5. la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
> 6. la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta." (Directiva 95/46/CE, 1995, p.22).

Además indica que:

> "2.Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas. (Directiva 95/46/CE, 1995, p.22).

Esto último abre la posibilidad de las transferencias a terceros países que no garanticen un nivel adecuado de protección de los datos, siempre que el responsable o encargado del tratamiento sí lo garantice a través de cláusulas contractuales y otros instrumentos. En razón de esto, se desarrollaron diversos mecanismos para permitir estas transferencias, que se describirán a continuación.

5.3.2 Cláusulas contractuales tipo

Para el cumplimiento del apartado 2, del artículo 26 de la Directiva 95/46/CE, se emiten la Decisión 2001/497/CE del 15 de junio de 2001 y la Decisión 2002/16/CE del 27 de diciembre de 2001.

La Decisión 2001/497/CE establece la posibilidad de utilizar cláusulas contractuales tipo para ofrecer garantías adecuadas con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los correspondientes derechos, en los casos en que se realicen transferencias a terceros países sin niveles adecuados de protección de datos personales.

Esta decisión permite el uso de cláusulas contractuales tipo que pueden ser utilizadas por un responsable del tratamiento de los datos establecido en la Comunidad Europea para ofrecer garantías suficientes para la transferencia de datos a un responsable del tratamiento establecido en un tercer país.

Las cláusulas contractuales tipo estipulan las medidas de seguridad técnica y organizativas necesarias que deben aplicar los responsables del tratamiento de los datos con el fin de garantizar el nivel de seguridad apropiado. La seguridad debe garantizar la protección de los datos contra: destrucción accidental o ilícita o su pérdida accidental, alteración, divulgación o acceso no autorizado o cualquier otra forma ilícita de tratamiento.

La Decisión establece en un anexo las “Cláusulas Contractuales Tipo” en que se indica los detalles mínimos que se deben especificar en el Contrato sobre la transferencia. El contrato establece entre otras: las obligaciones del exportador e importador de datos, la responsabilidad por los daños que se sufran, cooperación con las autoridades de control y legislación aplicable.

De manera similar la Decisión 2002/16/CE pretende regular la transferencia de datos personales entre un responsable de tratamiento ubicado en Europa y un encargado de tratamiento ubicado en un tercer país fuera de la Unión Europea.

La diferencia entre la Decisión 2002/16/CE y la 2001/497/CE es que la primera regula una relación de subordinación entre importador de datos, que es un simple ejecutor de las instrucciones del exportador, y el responsable (o exportador) del tratamiento que es quien encarga un trabajo concreto al importador. Por este motivo en esta Decisión el énfasis de las responsabilidades es sobre el exportador. En la primera el importador realizará el tratamiento por cuenta del exportador de datos y de conformidad con sus instrucciones. En la segunda, tanto el exportador e importador de los datos son capaces de determinar los fines y medios del tratamiento.

5.3.3 Normas Corporativas Vinculantes

Por otro lado, el Grupo de Trabajo del artículo 29 (en adelante GT29) creado por la Directiva de la Unión Europea 95/46/CE, se organiza en subgrupos para analizar diversos aspectos de la protección de datos. En el año 2005, uno de los subgrupos trabajó el tema de las Normas Corporativas Vinculantes (NCV) o "Building Corporate Rules" (BCR).

Las NCV son instrumentos permitido por la Unión Europea, que flexibiliza los movimientos internacionales de datos personales entre un grupo de empresas multinacionales con filiales establecidas incluso fuera del espacio económico Europeo. Es un nuevo mecanismo válido para legitimar las transferencias de datos personales entre empresas de un mismo grupo.

Estas normas tienen su origen en la aprobación del documento de trabajo WP74, de 3 de junio de 2003, por el grupo de trabajo del artículo 29 (GT29), establecido en virtud del citado artículo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Este proyecto se inició por iniciativa de varias multinacionales, cuando comenzaron a plantearse la posibilidad de facilitar garantías adecuadas en el sentido del Artículo 26 de la Directiva de Protección de Datos, pero no utilizando las herramientas tradicionales como los contratos, sino planteando un conjunto de normas vinculante para las filiales ubicadas fuera de la comunidad europea del grupo empresarial en relación a los datos personales transferidos.

El artículo 26 párrafo 2 de la Directiva 95/46/CE prevé que un Estado miembro podrá autorizar una transferencia de datos con destino a un tercer país que no tenga un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes. De esta forma, las normas corporativas vinculantes son un instrumento que permitiría a las empresas ofrecer garantías para poder llevar a cabo transferencias de datos hacia terceros países.

Uno de los subgrupos del GT29 trabajó, durante el año 2005, en las Normas Corporativas Vinculantes para la transferencia internacional de datos. Con el fin de estudiar este procedimiento de autorizaciones, basado en la autorregulación y la cooperación entre autoridades, el subgrupo adoptó dos documentos:

-WP107: en el que se establece un procedimiento de cooperación para la emisión de posiciones comunes sobre las garantías proporcionadas por las reglas corporativas vinculantes que permitan a las empresas transferir datos.

-WP108: que establece un modelo de "checklist" para la aprobación de las normas corporativas vinculantes.

Las NCV describen con suficiente detalle el flujo de datos, propósitos del procesamiento, personal encargado, actividad económica perseguida, etc., que permitan asegurar que el tratamiento de los datos es adecuado.

Las actualizaciones de los datos pueden ser posibles en las siguientes condiciones: no se hacen transferencias de datos hasta que el exportador esté seguro de que el miembro cumple con las normas; una persona o departamento identificado del grupo corporativo debe tener una lista completa y actualizada de los miembros, guardar registro de cualquier actualización a las normas y proveer información a las autoridades de protección de datos cuando lo requieran; actualizaciones a las normas y cambios en la lista de miembros deben ser reportados a las Autoridades de Protección de Datos, justificando brevemente las razones de la actualización.

Las NCV para la transferencia internacional de datos deben contener:

-Previsiones que garanticen el cumplimiento. El grupo corporativo debe asegurar el cumplimiento de las normas.

-Auditoría: Las normas deben someterse a procesos de auditoría y notificar las actualizaciones a las Autoridades de Protección de Datos.

-Manejo de denuncias o quejas: Debe establecerse un sistema que permita manejar las denuncias. El uso de mecanismos de resolución alternativa de conflictos debe promoverse y de acuerdo con la legislación aplicable.

-Deber de cooperación con las Autoridades de Protección de Datos: Debe estar claro el deber de cooperar con las Autoridades de Protección de Datos, esto garantiza una protección adecuada que permite a un individuo plantear la denuncia cuando sea lesionado y canalizarla adecuadamente.
-Responsabilidad: Las normas deben contener la previsión de la responsabilidad en caso de lesiones.
-Jurisdicción: Se aplican las que se indiquen en la Directiva de Protección de Datos y en las leyes nacionales.
-Transparencia: Es el deber de informar al titular sobre el tratamiento que se le hará a sus datos, que serán transferidos a otros miembros del grupo corporativo fuera de la Comunidad Europea y que el grupo corporativo garantizará su protección.

Las NCV complementan las cláusulas contractuales o los contratos-tipo aprobados por la Comisión Europea. Las NCV son una alternativa a las cláusulas contractuales tipo que pueden suscribirse entre exportador e importador para la regulación de una transferencia internacional que suponga una cesión de datos, cuando el destinatario de los datos está ubicado en un país fuera de la Unión Europea y que no goza de un nivel de protección adecuado.

5.3.4 Acuerdo de Puerto Seguro

En Estados Unidos la protección de datos está regulada parcialmente en una multitud de normas específicas y sectoriales sin conexión entre ellas, poniéndose casi todo el énfasis en la autorregulación y sin que exista una autoridad o autoridades de control encargadas de garantizar eficazmente el cumplimiento de las reglas y la aplicación de unos estándares universalmente aceptados. Por ello, esta situación hacía inviable la posibilidad de una declaración de adecuación de los Estados Unidos por parte de la Comisión Europea (Aced, 2005).

Esta situación de los Estados Unidos daba problemas para el establecimiento de negociaciones comerciales con Europa, pues las exigencias de las Directivas de la Unión Europea sobre protección de datos hacían difícil esta relación. Sobre todo la

directiva relacionada con las transferencias de datos personales a terceros países que garanticen, al titular de los datos, una protección mínima y necesaria conforme a lo dispuesto en la normativa comunitaria.

Las compañías multinacionales estadounidenses que operan en Europa presionaron para que el Departamento de Comercio de los Estados Unidos y la Comisión Europea buscaran un acuerdo que resolviera estas dificultades.

Después de un arduo trabajo el Grupo de Trabajo, establecido por las autoridades Europeas, llegaron a definir los Principios de Puerto Seguro, que ofrecían un nivel de protección adecuado para la transferencia de datos personales desde Europa a Estados Unidos, y se tomó la Decisión 2000/520/CE el 26 de julio de 2000.

Puerto Seguro es una Decisión de adecuación de carácter sectorial a la que pueden acogerse, exclusivamente, compañías establecidas en los Estados Unidos.

Para que una empresa estadounidense pueda disfrutar de los beneficios de Puerto Seguro debe satisfacer un conjunto de condiciones mínimas. Debe ser una compañía establecida en Estados Unidos., sujeta a la jurisdicción de la Comisión Federal de Comercio (FTC) o al Departamento de Transportes de los Estados Unidos (únicas entidades reconocidas hasta el momento por la Comisión Europea) y haber manifestado de forma inequívoca y pública su compromiso de cumplir las condiciones establecidas en Puerto Seguro.

Los principios contenidos en la Decisión sobre Puerto Seguro son los siguientes:

- Notificación: informar al titular el propósito de la recolección de datos.
- Opción: el titular puede decidir si permite que su información se divulgue a un tercero o utilizado para otro fin.
- Transferencia ulterior: establece que las entidades deben aplicar los principios de notificación y opción antes de revelar información a terceros.

- Seguridad: Las entidades que tratan información personal deben tomar precauciones para evitar su pérdida, mal uso, consulta no autorizada, divulgación, modificación o destrucción.
- Integridad de los datos: Adoptar medidas para que los datos sean exactos, completos, actuales y pertinentes a los fines de la recolección.
- Acceso: el titular puede acceder a sus datos para modificarlos o suprimirlos cuando no sean exactos.
- Aplicación: Se refiere a que se deben tener mecanismos que permitan garantizar el cumplimiento de los principios para que las personas afectadas puedan reclamar incumplimientos y sancionar a la entidad.

Estos principios hacen referencia al derecho de información, consentimiento, comunicación a terceros, seguridad, calidad de datos, derecho de acceso y recursos, responsabilidad y sanciones, aunque con un contenido bastante más limitado. Estos principios genéricos se completan con un conjunto de Preguntas más Frecuentes (FAQs) que intentan aclarar y precisar el alcance de los mismos y dar una solución a algunas dudas interpretativas que pudieran surgir en su aplicación (Aced, 2005).

Las FAQs son quince y hacen referencia a datos especialmente protegidos, excepciones relativas al ejercicio del periodismo, responsabilidad subsidiaria de los proveedores de servicios de Internet o telecomunicaciones, excepciones a los principios de notificación, opción y acceso para los bancos de inversiones y sociedades de auditorías, la función de las autoridades de protección de datos europeas, condiciones y compromisos adquiridos a través de la auto certificación, verificación del cumplimiento de Puerto Seguro, alcance del derecho de acceso, condiciones especiales referentes a los datos de Recursos Humanos transferidos desde la UE, regulación contractual de los tratamientos por cuenta de terceros, resolución de litigios y ejecución, precisiones sobre el derecho de opción, transferencia de información sobre viajes, transferencia de datos relativos a productos médicos y farmacéuticos y, finalmente, sobre la información extraída de registros públicos e información de dominio público (Decisión 2000/520/CE de Unión Europea).

5.4 Análisis de legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México, Perú.

Los países latinoamericanos han establecido la protección a la vida privada como un derecho de rango constitucional a partir del cual se han iniciado la redacción de los proyectos de leyes específicas que regulan dicha materia.

5.4.1 Normas Constitucionales

En la Constitución Política de Chile no existe una norma expresa, pero la construcción jurídica de la protección de datos personales se basa en el artículo 19 n° 4, inciso primero, de la Constitución Política de la República, que reza:

> "CAPITULO III. De los Derechos y Deberes Constitucionales
> Artículo 19.- La Constitución asegura a todas las personas: (…)
> 4º.- El respeto y protección a la vida privada y a la honra de la persona y de su familia."
> (Constitución Política de Chile con reformas al 2005, 1980, p.12)

En la Constitución Política de Colombia se encuentra el artículo 15 que establece el derecho de las personas a la intimidad personal y familiar y al buen nombre, e indica que el Estado debe respetarlos y hacerlos respetar. También establece el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

El artículo dispone que, en la recolección, tratamiento y circulación de datos, se respete la libertad y demás garantías consagradas en la Constitución.

También establece que las formas de comunicación privada son inviolables, excepto por orden judicial para los casos que la ley establezca.

La Carta Constitucional costarricense no contempla, específicamente el derecho a a la protección de datos de carácter personal, como un derecho específico a ser tutelado. Pero su artículo 24 establece la protección en el ámbito de intimidad del hogar, de las comunicaciones y de los documentos privados, dejando a la ley la regulación de las interceptaciones telefónicas y el secuestro de documentos. Indica que los documentos

privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República son inviolables.

Se encuentran en la Constitución Política de Ecuador los siguientes derechos tutelados: El inciso 8 del artículo 23 de la Constitución garantiza la intimidad personal y familiar; inciso 13 la inviolabilidad y el secreto de la correspondencia; inciso 21 del mismo artículo prohíbe la utilización de la información personal de terceros referentes a sus creencias religiosas, filiación política, datos sobre salud y vida sexual.

El artículo 94 de la Constitución de 1998 de Ecuador establece la tutela por medio del hábeas data:

> "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.
> Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.
> Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización.
> La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional" (Constitución Política de Ecuador, 1998, p. 17).

En México, El artículo 16 de la Constitución de los Estados Unidos Mexicanos señala que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones. Del mismo modo regula casos relativos a la práctica de cateos, visitas domiciliarias, la exhibición de documentos y papeles personales, así como la violación de correspondencia. Las disposiciones señaladas no se refieren específicamente a la regulación de los datos personales propiamente, sino al derecho a la privacidad.

La Constitución Política de Perú de 1993, en el artículo 2°, inciso 6) establece el derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. A su vez el artículo 200º inciso 3) de la Constitución Política de 1993, establece la Garantía Constitucional del Hábeas Data (Ley Nº 26301 modificada por la Ley Nº 26545, y la Ley Nº 23506), que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5, 6 y 7 de la Constitución.

El artículo 2° inciso 5 que norma por primera vez el derecho a solicitar de cualquier entidad pública, sin expresar la causa, la información que requiera y a recibirla, salvo que esa información afecte la intimidad personal, o aquellas que expresamente se excluyan por ley o por razones de seguridad nacional.

Es así que el derecho a la información ante una entidad pública encuentra como uno de sus límites a la intimidad personal. A su vez la misma norma constitucional protege el secreto bancario y la reserva tributaria, los cuales sólo pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del congreso con arreglo a ley y siempre que se refieran al caso investigado.

El inciso 7) del mismo artículo, reconoce los derechos a la intimidad, al honor y a la propia imagen; y por último el inciso 10) del referido artículo 2°, consagra también la reserva e inviolabilidad de las comunicaciones y documentos privados, los cuales no pueden ser abiertos, interceptados, intervenidos ni incautados sino por mandato motivado del Juez, con las garantías previstas en la Ley.

5.4.2 Leyes generales o en proyecto

Chile fue el primer país de Iberoamérica que aprobó la ley de protección a la privacidad, que contiene varios principios fundamentales sobre protección de datos personales.

La ley chilena 19628 sobre la protección de la vida privada, indica en su artículo 4 que el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. Y que el titular de los datos debe ser debidamente informado respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

También este artículo 4 legaliza el spam o correo comercial no solicitado al indicar que:

> "No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su

> profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios." (art.4 Ley 19628, 1999, p.4).

Su artículo 6 indica que:

> "los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos." (art. 6 Ley 19628, 1999, p.5).

El artículo 16 de esta ley establece el recurso del hábeas data, aunque no se refiere a este término explícitamente.

Colombia no tiene una norma general de Protección a la Vida Privada.

Ecuador no tiene una norma general de Protección a la Vida Privada, sin embargo, en la Ley 67 de Comercio electrónico, firmas y mensajes de datos establece en su artículo 9:

> "Art. .9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.
>
> La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.
>
> No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.
>
> El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo." (Ley 67 de Ecuador, 2002, p.2).

Igualmente México no tiene una norma general de protección a la vida privada. Sino que mediante el artículo 76 bis de la Ley Federal de Protección al Consumidor amplía el alcance de la Ley en transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.

Esta Ley mexicana es la primera en Latinoamérica en referirse a la protección de datos personales en sistemas y servicios en línea, pero legisla sólo en este tipo de transacciones. Además adopta un enfoque basado en la protección al consumidor, cuando pueden existir situaciones donde la recopilación y tratamiento de información no provenga de una relación con el consumidor, por lo que hay un vacío jurídico que persiste (Palazzi, 2002).

Perú no tiene una norma general de protección a la vida privada, pero se encuentra en el Código Civil lo siguiente:

> "Artículo 16.- Confidencialidad de la correspondencia y demás comunicaciones.
> La correspondencia epistolar, las comunicaciones de cualquier género o las grabaciones de la voz, cuando tengan carácter confidencial o se refieran a la intimidad de la vida personal y familiar, no pueden ser interceptadas o divulgadas sin el asentimiento del autor y, en su caso, del destinatario. La publicación de las memorias personales o familiares, en iguales circunstancias, requiere la autorización del autor." (Decreto legislativo 295 Código Civil, 1984)

Podría considerarse aquí, que los datos recopilados en las contrataciones por medios electrónicos, son parte de una comunicación y por lo tanto amparado por el Código Civil.

Ecuador, Perú, Colombia, México y Costa Rica no tienen ninguna ley general de protección de datos personales. Sin embargo, Perú, Colombia, México y Costa Rica han presentado proyectos a discusión:

Colombia tiene en estudio el proyecto de ley estatutaria N° 143 de 2003, por la cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, tratamiento y circulación de los mismos. Y tiene otro Proyecto de Ley Estatutaria 071-2005, del 10 de agosto de 2005, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones.

Costa Rica tiene el Proyecto de Ley No.15.178 Protección de la persona frente al tratamiento de sus datos personales. El texto pasó a Comisión Permanente de Asuntos Jurídicos de la Asamblea Legislativa el 27 de marzo de 2003.

También tiene otro proyecto de Ley No.14785 que adiciona un nuevo capítulo denominado Del Recurso de Habeas Data al Título III de la Ley 7135 de Jurisdicción Constitucional, este proyecto pasó a estudio de la Comisión Permanente de Asuntos Jurídicos el 18 de junio de 2002.

Por otro lado, está el Proyecto de Ley No.14029 de Acceso a Internet, con dictamen afirmativo de mayoría de la Comisión Permanente de Asuntos Económicos del 15 de mayo de 2001, establece en su artículo 6, inciso g) que los proveedores de servicios de Internet no pueden ceder los datos personales a terceros sin autorización del titular; y su inciso b) establece la inviolabilidad de las comunicaciones y documentos privados por Internet.

Aunque Costa Rica no tenga una Ley propiamente relacionada con la Protección de Datos, el acceso no autorizado a datos personales o privados contenidos en medios electrónicos, informáticos, magnéticos y telemáticos tiene protección en el Código Penal costarricense, y en otras normas específicas como la Ley General de Aduanas, la Ley de Administración Financiera de la República y Presupuestos Públicos, el Código de Normas y Procedimientos Tributario, entre otras.

Se encuentra en el Código Penal costarricense el artículo 196 bis que establece la violación de comunicaciones electrónica como un delito. Este artículo establece penas de seis meses a dos años al que vulnere la intimidad de otro. Es decir que sin su consentimiento se apodere, accede, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino mensajes, datos e imágenes contenidas en medios electrónicos, informáticos, magnéticos y telemáticos. Y las penas serán de uno a tres años, si estas acciones son realizadas por los propios encargados de los soportes electrónicos, informáticos, magnéticos y telemáticos en donde se encuentra almacenado los datos.

Los artículos 217 bis y 229 bis del Código Penal se refieren al fraude informático y al sabotaje informático respectivamente, los cuales consisten en acceso, modificación o daño a los datos contenidos en los sistemas informáticos. Estos artículos establecen penas de uno a diez años de prisión.

México tiene presentado el Proyecto de decreto de Ley Federal de Protección de Datos personales desde el 2001, y en su capítulo VI establece lo relacionado al Hábeas Data.

Perú tiene un anteproyecto de ley de Protección de Datos Personales elaborado por la comisión especial constituida por el Poder Ejecutivo mediante la Resolución Ministerial N° 094-2002-JUS, está todavía en trámite.

El anexo 3 se muestra si las legislaciones de los países analizados tienen garantizado el respeto a la privacidad de acuerdo con los derechos y garantías mencionados, además se presenta dos cuadros comparativos donde se resume toda la normativa relacionada analizada.

5.5 La Sala Constitucional costarricense y la protección de datos

Como se puede observar del análisis de las secciones anteriores, Costa Rica no cuenta ni con una ley de protección de datos personales ni con el recurso de Hábeas Data expresamente en su normativa.

Sin embargo, el hábeas data se ha convertido en un instrumento de tutela reactivo que ha sido ampliamente aplicado por Sala Constitucional costarricense, tomando como base la misma Ley de la Jurisdicción Constitucional, así como la interpretación amplia que la propia Sala ha hecho del artículo 24 de la Constitución Política.

La jurisprudencia de la Sala Constitucional ha evolucionado notablemente, los primeros fallos se establecen en contra de los archivos criminales administrados por el Organismo de Investigación Judicial (voto 2609-91, 2680-94 mencionado en Chirino y Carvajal (2003)). En una de las primeras sentencias se considera el suministro de

informaciones conservados en esos archivos a terceras personas (desviación del fin original del tratamiento de datos) como lesivo al principio de legalidad y a la dignidad de la persona.

La sentencia 1261-90 reconoce el derecho a la intimidad y el derecho a acceder al amparo para protegerlo. En esta sentencia, la Sala anuló por inconstitucional la posibilidad de intervenir, inclusive con fines de investigación policial, las líneas telefónicas (Barth, 2005).

También en la sentencia 9080-94, Barth (2005) indica que la Sala Constitucional avaló la negativa de la institución aseguradora de vehículos de mostrar los datos declarados por quien sufrió una colisión, inclusive a la parte contraria en el mismo accidente automovilístico. La sentencia declaró el carácter confidencial de esos datos resguardados por el asegurador.

La sentencia 4147-97 (reiterada en la sentencia 4154-97), la Sala acogió el recurso de amparo planteado por quien exigió del patrono que le mostrara el expediente personal abierto durante el proceso de reclutamiento de personal. En esta sentencia el tribunal afirma un principio esencial en el derecho de la autodeterminación informativa: el derecho al acceso a los datos personales acopiados en una investigación.

Posteriormente, y ya en el orden de fallos más reciente, el Voto 4154-97, habla expresamente del hábeas data y su regulación, planteando que el objeto de este recurso es la protección de la persona para conocer o rectificar la información pública o privada que exista sobre ella. En este sentido se encuentra en Chirino y Carvajal (2003) lo siguiente:

> "La Sala Constitucional ha reconocido la existencia de un amparo especial, denominado "hábeas data" cuyo objetivo esencial consiste en el ejercicio de una facultad de corrección de los datos que se hallan en bancos de datos públicos y privados.
> La primera sentencia que alusión (sic) a este tema es la número 4154-97. Califica al hábeas data, correctamente, como una institución de carácter procesal, cuya tutela se extiende a bienes jurídicos tales como el honor, la intimidad y la dignidad de la persona." (Chirino y Carvajal, 2003, p. 244).

La Sala Constitucional reconoce los peligros de la sociedad informatizada con el fallo 1345-98, de acuerdo con Chirino y Carvajal (2003):

> 'Fue el primer fallo donde se establece una relación inequívoca entre los peligros de la "sociedad informatizada" y el derecho a la intimidad.
> Hace un reconocimiento de los riesgos que las tecnologías de la comunicación y la información podrían traer para la sociedad y el ciudadano, sobre todo en lo referido al acceso a los datos personales' (Chirino y Carvajal, 2003, p.240).

> 'Los magistrados constitucionales hacen evidente que "…esfera privada ya no se puede reducir al domicilio o a las comunicaciones sino que es factible preguntarse si debe incluir "la protección de la información" para reconocerle al ciudadano una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar.' (Chirino y Carvajal, 2003, p.241).

Esta sentencia, indica Barth (2005), marca un hito en materia del derecho a la autodeterminación informativa. El problema sometido al conocimiento del Tribunal se desencadenó porque una empresa suministró a un banco información sobre una persona, contra la cual existía, según la empresa, una deuda incobrable. En realidad, la deuda estaba prescrita y el recurrente así exigía que se aclarara en la base de datos. En igual sentido se dirige la sentencia 8996-2002.

En el expediente 15178 del proyecto de ley de Protección de la persona frente al tratamiento de datos personales, menciona que el Voto 1345-99, abre la posibilidad de una tutela de acceso, con base en el derecho a la autodeterminación informativa, para que la gente pueda conocer las informaciones que sobre ellas se encuentren registradas, e incluye una descripción de los derechos que lo asisten.

En un fallo más sistematizado, el 5802-99, la Sala Constitucional entra a analizar el registro y los bancos de datos y los objetivos del hábeas data, así como los principios que rigen el ejercicio de estos derechos. En esta sentencia, la Sala se pronuncia en cuanto al deber de excluir del archivo policial las reseñas de personas absueltas o sobreseídas definitivamente en un proceso penal. Indica la Sala que "Mantener su ficha en el archivo no solo roza con el derecho a la autodeterminación informativa, sino también con el principio de inocencia" (Barth, 2005, p.265).

Indica Chirino y Carvajal (2003) que este fue el primer fallo donde la Sala abordó los principios que regulan el tratamiento de datos personales, y dio cabida a que el ciudadano pueda controlar la forma en que se realiza el tratamiento de datos personales, dentro de la tutela procesal del hábeas data.

Las siguientes sentencias de la Sala son mencionadas en Barth (2005). La sentencia 6481-99, la Sala considera también confidenciales los datos presentados por un tercero en la oferta dentro de una licitación pública, y rechaza la petición de tener acceso a ellos.

La sentencia 2885-2002 obligó a la empresa excluir de sus archivos datos sobre los parientes de quien solicita el crédito, pues esto se desvía de la finalidad del archivo.

En la sentencia 2002-6783 la Sala obligó a una empresa que aclarara la identidad de una persona cuyos datos constaban en el archivo. El problema surgió porque la empresa de datos suministra a un banco el historial crediticio de una persona, pero al no constar ningún número de identificación, y por existir la posibilidad de personas con igual nombre, no es posible determinar exactamente si se trata de quien gestiona el crédito. Igual sentido se pronunció la Sala en sentencia 2002-10438.

La sentencia 2000-3820, declaró con lugar un recurso de amparo a favor de un periodista que reclamaba tener acceso a los pasaportes diplomáticos de varios funcionarios del servicio exterior. El acceso debe darse no solo a los periodistas, sino a toda persona que lo solicitara. En este mismo sentido se pronuncia la Sala en la sentencia 2002-4802 en relación con la lista de personas autorizadas por el Ministerio de Obras Públicas y Transportes para brindar el servicio de transporte público; y la sentencia 2003-3489 que obliga a un banco estatal, en aras de la transparencia, a revelar la información de las cuentas corrientes que tienen a su nombre los distintos partidos políticos y las sociedades anónimas que utilizaron para canalizar los fondos de la campaña electoral.

Se observa que la Sala ha desarrollado varios principios esenciales en torno al derecho a la protección de datos personales: el derecho a la intimidad y a la protección de datos personales, a la tutela de ese derecho por la vía del recurso de amparo, derecho a exigir la exclusión del registro de información contenidos en archivos, derecho a la confidencialidad, derecho al acceso a sus datos personales, el derecho a la actualización de los datos, derecho a la exclusión de información sensible y el derecho a una adecuada identificación de la persona cuyos datos se almacenan. También la Sala ha establecido excepciones de dar información personal a terceras personas.

Este recuento de la jurisprudencia de la Sala Constitucional en materia de protección de datos permite observar el avance que ha tenido la jurisprudencia nacional en materia de hábeas data, como un estándar de tutela reactivo de indudable importancia. No obstante, al igual que en otros países, aún es necesario acordar tutelas preventivas, que reaccionen antes de que se ocasionen riesgos de incalculables proporciones para una gran cantidad de ciudadanos, sobre todo en la nueva era de la sociedad de la información y del conocimiento.

Hoy resulta indispensable ofrecer al país una regulación integral que ofrezca mecanismos preventivos que considere el desarrollo tecnológico, para completar la tutela reactiva que ya ofrece el máximo tribunal constitucional.

Un resumen de todos estos votos se encuentra en el anexo 12.

5.6 Análisis del Proyecto de Ley 15178 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales de Costa Rica

El actual proyecto parte de la premisa de que la vía del hábeas data ya ha sido adecuadamente aplicada por la Sala Constitucional, y ya ha ido ampliándose su uso, incluso, para establecer ciertos elementos de calidad en el tratamiento de datos. Resulta evidente, entonces, que debe incluirse en una legislación una consideración amplia de las etapas del tratamiento de la información que forman parte normal de todos los procesos informativos en el ámbito público y privado, incluyendo, el flujo transfronterizos de datos.

El cuadro comparativo de la normativa de Protección de la Privacidad o Datos Personales del Anexo 3 se indica claramente los derechos incluidos en el Proyecto de Ley 15178 de Protección de la Persona frente al tratamiento de sus datos personales de Costa Rica.

Puede observarse del cuadro, que el Proyecto de ley de Costa Rica no incluye dos derechos: Derecho para la prohibición de interconexión de archivos y el Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente.

Sería conveniente adicionar ambos derechos, pues el primero se refiere a que no se permite interconectar diferentes archivos para procesar datos personales con el fin de crear perfiles de gustos, preferencias o de simple consumo, de la persona. Recuérdese que con la tecnología actual, es muy fácil y veloz conocer todo acerca de una persona con solo procesar los datos que de ella se encuentran en distintas bases de datos. Se debe prohibir, a los responsables de los datos, la transmisión o cesión de datos personales a terceros, que podrían utilizarlos con fines no autorizados; además, no debe permitirse que se interconecten archivos para cruzar información de las personas.

También es necesario incluir el derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente, porque el procesamiento automático de datos personales no garantiza que se consideren todos los elementos importantes de una persona para valorar o tomar una decisión sobre ella. Recuérdese que el procesamiento automático tiene parámetros definidos para evaluar alguna situación de la persona, pero no todas las situaciones de la personas son iguales, y más de alguna requiere de tratamiento aparte por sus condiciones personales.

El primer capítulo se refiere al objeto y fin del proyecto de Ley, así como una lista de definiciones de algunos de los conceptos contenidos en su articulado.

Establece que el objetivo de la ley es garantizar a cualquier persona física o jurídica, sean cuales fueren su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en

relación con su vida privada y demás derechos de la personalidad; asimismo, la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

No establece el ámbito de aplicación como un artículo aparte. Sería conveniente incluirlo para especificarlo. Se recomienda seguir la Directiva 95/46/CE que establece que las disposiciones de la Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

El capítulo II del Proyecto de Ley establece los principios básicos para la protección de datos, regulando los aspectos relacionados con el derecho de las personas respecto del manejo de sus datos, reconociendo los deberes de obtención del consentimiento del afectado, calidad, seguridad y cesión de los datos, categorías de datos que requieren de una protección mayor a la regla general (datos sensibles), garantías efectivas de acceso a la información personal, corrección, supresión y actualización de la misma. También prevé la posibilidad de las entidades de emitir protocolos de actuación.

Con respecto a la seguridad, el artículo 7 establece en su inciso 2 que el responsable del fichero deberá adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

El inciso 3 indica que no se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que garanticen plenamente su seguridad e integridad y los de los centros de tratamientos, equipos, sistemas y programas.

El inciso 4 establece que por vía de reglamento, se establecerán los requisitos y las condiciones que deban reunir los ficheros automatizados y los manuales y las personas que intervengan en el acopio, almacenamiento y uso de los datos.

Por último el inciso 5, obliga al secreto profesional al personal que intervenga en cualquier fase del proceso de recolección y tratamiento de los datos de carácter personal.

El artículo solo se refiere a la seguridad de los datos almacenados en los ficheros automatizados y manuales, debe indicarse también la seguridad de los datos en tránsito a través de los medios electrónicos de comunicación.

Con respecto a la seguridad de los datos personales que se transmiten a través de la red, esta se logra por medio del sistema de Criptografía asimétrica, con autoridades certificantes y firmas digitales. Pero la seguridad en los lugares de recepción, procesamiento y almacenamiento de la información debe incluir entre otros: políticas empresariales o institucionales sobre medidas de seguridad, protocolos de seguridad, auditorías, controles, mecanismos tecnológicos para su resguardo (claves para los responsables), así como medidas de protección contra daños fortuitos (incendio, humedad, etc.).

Es importante que se establezca explícitamente la obligación de que las empresas, que manejan datos de las personas, tengan todas las medidas adicionales de seguridad necesarias para la protección adecuada de los datos de las personas.

Con relación a la cesión de datos, indica el artículo 6 que los datos de carácter personal conservados en archivos o bases de datos públicos o privados, sólo podrán ser cedidos a terceros para fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del afectado, y que el consentimiento no será exigido cuando así lo disponga una ley o se trate de la cesión de datos personales al Estado o una institución pública de salud o de investigación científica en el área de la salud, relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.

Se resalta la importancia de la disociación, pues inclusive en el caso de que sea el Estado el que requiera los datos personales para cumplir con sus fines, es necesario que los datos no puedan asociarse a persona determinada.

Sobre los protocolos de actuación, se resalta el hecho de que el artículo 13 establece la posibilidad de que las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, almacenamiento y uso de datos personales, de emitir un protocolo de actuación, en el cual establecerán los pasos que deberán seguir, en la recolección, almacenamiento y manejo de los datos personales, de conformidad con las reglas previstas en la Ley.

Estos protocolos deben ser inscritos ante el Registro de archivos y bases de datos y aprobados por la Agencia de Protección de Datos Personales, la cual podrá verificar que el titular del archivo esté cumpliendo con los términos de su código de conducta. Estos protocolos permitirán que las entidades actúen de manera ágil y sencilla, en tanto se sometan a los términos de sus propios protocolos.

Estos protocolos de actuación o código de conducta son mecanismos de autorregulación. Sin embargo, este artículo sólo establece la posibilidad de emitir el protocolo de actuación. Sería importante incluir a nivel de ley, que el Estado incentivará la adopción de mecanismos de autorregulación, para promover que las empresas implementen estos mecanismos para la protección de la privacidad y del tratamiento de datos personales.

El capítulo III del Proyecto establece como regla general, la prohibición de la transferencia internacional de datos. Su único artículo 14 establece que las personas públicas y privadas encargadas del manejo de bases de datos y los archivos físicos, estarán imposibilitadas para transferir datos que hayan recibido directamente de los titulares de la información o de terceros, pero se exceptúan de esta prohibición las transferencias que cumplan las siguientes reglas:

> **"a)** Que la Agencia para la Protección de Datos Personales autorice la transferencia a la persona o institución receptora, pública o privada, por corroborar que con dicho traslado no están siendo vulnerados los principios rectores del manejo de datos personales, descritos en esta Ley.
> **b)** Que el titular de la información haya autorizado expresa y válidamente tal transferencia.
> **c)** Si se trata de una persona o institución pública o privada domiciliada en el extranjero, dicha transferencia solo podrá ser llevada a cabo si, además de las condiciones antes mencionadas, dicho receptor está domiciliado o tiene como base un país que ofrezca un nivel de protección de los datos personales, igual o superior al establecido en Costa Rica." (art.14, Proy de Ley No.15178, p.19)

Este artículo es importante para los casos de transacciones comerciales electrónicas que traspasan fronteras. Por lo tanto no se podrá transmitir datos a países que tengan un nivel inferior de protección de datos que al establecido en Costa Rica. Con esta norma se pretende prevenir la violación a las reglas sobre manejo de datos personales producida por su indebida cesión a personas domiciliadas en países que cuentan con una pobre protección de datos personales. Con esta norma, Costa Rica estaría regulando la materia en forma similar a la prevista en la normativa producida por la Unión Europea (Directiva 95/46/CE).

Pero a diferencia de la Directiva Europea, el Proyecto no incluye, las mismas excepciones, por las cuales se ha permitido las transferencias de datos personales a países que no ofrecen protección adecuada. Excepción que ha permitido a las compañías acogerse a cláusulas contractuales tipo o crear sus normas corporativas vinculantes y que son aceptadas por la Unión Europea como instrumento para garantizar la protección de datos cuando el país no las ofrece.

Sería conveniente, incorporar la posibilidad de que en casos de que el país, a donde se transferirá los datos personales, no ofrezca protección adecuada, se permita la transferencia utilizando instrumentos como las normas corporativas vinculantes, los contratos con cláusulas tipo (utilizadas en la Unión Europea), u otros acuerdos similares al de Puerto Seguro, que garanticen dicha protección. Esto con el fin de no limitar las relaciones comerciales siempre que se realicen con una protección adecuada de los datos personales que se transfieren.

Otro aspecto importante del Proyecto de Ley es que crea y define en su capítulo IV la Agencia para la Protección de Datos Personales (PRODAT), dándole a ésta la autoridad para velar por el cumplimiento de la Ley y sancionar a los que la incumplan, además es la encargada de llevar el control de todos los archivos, registros o bases de datos, públicos y privados, existentes sobre datos personales. Con este órgano dotado de independencia funcional, administrativa y de criterio se intenta dar una efectiva garantía de los derechos derivados del manejo de datos personales, pues exime a los órganos jurisdiccionales, del conocimiento de los procesos de hábeas data tradicional. Sus funciones propuestas son tanto preventivas (inscripción y autorización de las bases de datos y protocolos de actuación, inspecciones oficiosas, etc.) como reactiva (atención de denuncias, imposición de órdenes y sanciones administrativas, etc.).

El capítulo V regula los procedimientos de intervención en archivos y bases de datos, el régimen disciplinario aplicable a los administradores de ficheros y los procedimientos internos para ejercer la competencia disciplinaria contra los funcionarios de la Agencia.

El Proyecto de Ley no incluye explícitamente el procedimiento a seguir en caso de violación a un derecho cometido por algún ente, público o privado, ubicado en el extranjero. El proyecto solo establece normas para aplicarse a nivel nacional y solo el artículo 14 se refiere a la prohibición de la transferencia de datos a otros países con niveles inferiores de protección. Pero, por ejemplo, cuando un proveedor vende a través de Internet y recolecta información de un consumidor nacional, no hay mecanismos para realizar un reclamo ágil y efectivo si el proveedor viola algún derecho del consumidor en relación a sus datos personales. Por lo tanto, debe agregarse en el Capítulo de Procedimientos del Proyecto de Ley, el detalle de cómo se abordaría en caso de que el denunciado sea alguien ubicado en el extranjero. Es importante indicar que en casos de que estas violaciones se den en las relaciones de consumo, la jurisdicción aplicable sea la del domicilio del consumidor.

La aprobación del Proyecto de Ley 15178 sería un avance importante que permitiría proteger los datos personales de todos los ciudadanos, y en especial al consumidor cuando éste los entrega al proveedor en sus relaciones de consumo electrónico.

En un sentido más amplio, es necesario establecer la normativa de privacidad y protección de datos personales, de lo contrario, Costa Rica podría verse como un paraíso del tráfico de datos personales y podría verse afectada en sus pretensiones de mercado global en los actuales momentos en que el país está negociando diferentes tratados de libre comercio con Estados Unidos, la Unión Europea y países asiáticos.

A la par de este proyecto debe también aprobarse el proyecto de adicionar el recurso de hábeas data expresamente a la Ley de Jurisdicción Constitucional costarricense, para garantizar el ejercicio del derecho de la persona a acceder a las informaciones personales que se encuentren disponibles en registros magnéticos y manuales con el fin de ser revisados, y si representan para la persona un perjuicio, también el de ser corregidos o eliminados. Aunque, la Sala Constitucional ya reconozca el hábeas data, como se analizó en la sección correspondiente.

Como lo indica Chirino y Carvajal (2003):

> "La compleja sociedad de la información exige que el Estado regule en forma exhaustiva y preventiva todos aquellos aspectos concernientes al acopio, almacenamiento y uso de datos personales, entrando a participar activamente en dicho proceso, mediante un control estricto que impida reducir a simple mercancía la individualidad de las personas." (Chirino y Carvajal, 2003, p.283)

> "Alcanzar altos estándares en esta materia significa además, una ineludible condición para participar en las negociaciones comerciales con mercados altamente sensibles a nuestros productos, como son los de la Unión Europea, cuyas directivas y normativas exigen que los países con los cuales se tengan relaciones de este tipo demuestren que tienen estándares similares de protección a los ofrecidos en los países miembros." (Chirino y Carvajal, 2003, p. 284)

5.7 Conclusiones y recomendaciones

Del análisis de los casos de Estados Unidos y de la Unión Europea se puede concluir lo siguiente. Para que haya un desarrollo más rápido del comercio electrónico, se requiere la confianza del consumidor. Para esto, las empresas de bienes y servicios deben labrarse una reputación que respalde y dé seguridad a todas sus transacciones electrónicas, principalmente las que realicen a través de Internet, que permita una

mayor confianza de la población consumidora para hacer compras por medio de sus páginas Web. Además, es necesaria una base legal que proteja adecuadamente la información personal y vida privada de los ciudadanos.

Es necesaria una combinación de ambos mecanismos, autorregulación y base legal, que permita una adecuada protección a la vida privada y al tratamiento de la información personal. Los ciudadanos que deseen participar en el mundo digital necesitan la seguridad de que su información personal será tratada adecuadamente. Y las empresas que realizan comercio electrónico no pueden fallar en el uso adecuado de los datos personales.

La protección de la privacidad y el tratamiento de la información personal no pueden dejarse a la libre, esperando y confiando que las empresas se autorregulen, o dejarse completamente al Estado para que emita la normativa necesaria. El desarrollo vertiginoso de la tecnología requiere una mezcla complementaria de ambas partes, Estado y empresas e industrias privadas, que permitan ofrecer al consumidor una adecuada protección de su intimidad y a la vez promuevan el desarrollo del comercio electrónico.

Por otro lado, como lo expresa Arias (2002), el país no puede pasar ningún proyecto de ley relacionado con elementos que giren alrededor de las tecnologías digitales si antes no se dicta y aprueba una ley que proteja a cada uno de los nacionales de los excesos en el tráfico y manejo de sus datos.

Los países europeos iniciaron el camino de la regulación con legislaciones de protección de datos, después vino la legislación en comercio electrónico, firmas digitales, etc. En Costa Rica está ocurriendo lo contrario, ya ha promulgado una ley sobre firmas y certificados digitales y documentos electrónicos pero todavía no tiene una para la protección de datos personales. Habría que ver lo que ocurrirá en los próximos años en materia de protección de datos personales, a raíz del vertiginoso desarrollo del comercio electrónico.

Retomando la situación de los países latinoamericanos analizados, se encuentra que Chile tiene una Ley vigente de Protección a la Vida Privada en la cual se incluye el recurso del hábeas data, un avance importante en la normativa chilena. Sin embargo no establece un órgano fiscalizador independiente que se encargue de velar por el cumplimiento de las disposiciones de esta Ley, por lo que adolecerá de una efectiva ejecución. Esta Ley chilena tampoco establece nada al respecto de la transferencia internacional de datos, lo que se concluye que se encuentra permitida, siempre y cuando se cumplan las disposiciones generales establecidas en la Ley.

De acuerdo con Palazzi (2002), la ley chilena cumple parcialmente los recaudos exigidos por Europa para considerar adecuada una legislación o un sistema de privacidad. Esto debido a que varios principios de protección requeridos por la Unión Europea no están presentes en la ley chilena, falta normas que prohíban las transferencias a terceros países y la carencia de una autoridad de aplicación que vigile el efectivo cumplimiento de las normas.

En materia de comunicaciones comerciales y marketing directo, Chile legalizó el envío de correos electrónicos no solicitados o spam, pero permite los titulares de datos personales ejercer el derecho de bloqueo y eliminación de los datos personales almacenados en una base de datos, de manera que el responsable del banco de datos no pueda continuar enviando comunicaciones comerciales y correos electrónicos no solicitados a quien ha ejercido este derecho.

En otras legislaciones, como la Ley 34/2002 sobre telecomunicaciones y servicios de la sociedad de la información y del comercio electrónico de España, en materia de comunicaciones comerciales y correos electrónicos no deseados se ha optado por la prohibición de enviar comunicaciones comerciales y correos electrónicos no deseados a las personas (artículo 21), salvo que las mismas hayan autorizado con anterioridad el envío de dichas comunicaciones y correos (artículo 22).

El problema del spam hace que muchos consumidores se vean forzados a cambiar de correo electrónico, además el spam tiene un costo en dinero para los proveedores de

servicio de Internet, y para el consumidor que paga por tiempo real de uso de su conexión a Internet.

Chile, Perú y México incluye en sus leyes de protección al consumidor, artículos relacionados a la publicidad enviada por correo electrónico, permitiendo al consumidor solicitar suspender estos envíos.

Ecuador no tiene una ley propiamente de protección a los datos personales, pero incluyó en la Ley 67 de Comercio electrónico, firmas y mensajes de datos un artículo de Protección de Datos.

México tampoco tiene una ley de protección a la privacidad, pero en su Ley Federal de Protección al Consumidor se refiere a la protección de datos en transacciones en líneas para relaciones establecidas con consumidores.

Colombia, Ecuador y Perú incluyen dentro de su norma Constitucional el recurso de Hábeas Data. En el caso de Chile, el hábeas data se encuentra en el artículo 16 de la ley chilena 19628 sobre la protección de la vida privada.

En el caso de Costa Rica, aunque expresamente no se tiene el recurso de hábeas data, la Sala Constitucional lo ha reconocido y lo ha aplicado en diversas sentencias que ha dictado, como se analizó en la sección correspondiente.

Sin embargo, el hábeas data, ya sea como acción constitucional o reglamentada a través de una ley, no alcanza a cubrir todos los problemas de la protección de datos y tiene sólo la posibilidad de solucionar algunos de los problemas ocasionados por las nuevas tecnologías de la información.

Como indica Argüello (2005), el hábeas data incluye solo los derechos de acceso y rectificación, y de acuerdo con Chirino y Carvajal (2003) es un tipo de tutela reactiva, porque el ciudadano puede accederla cuando el daño ya ha ocurrido.

Lo que indica que es necesaria la promulgación de leyes de protección de datos personales si se quiere proteger efectivamente los derechos de las personas a su intimidad, en esta nueva era de las tecnologías de información y comunicación.

Mientras no se aprueben en esos países leyes de protección de datos siguiendo los estándares europeos, no existirá una autoridad de control encargada de velar por un correcto y adecuado tratamiento de datos personales junto con un código que condense estos principios.

Aunque Perú, Costa Rica, México y Colombia no tienen todavía una ley de Protección de datos personales, o en general a la Protección de la Vida Privada, es un acierto que ya hayan presentado proyectos en este sentido para su discusión.

En el caso de Costa Rica, la norma constitucional (art. 24) garantiza la privacidad y el derecho a la intimidad, que debe ser respetada a nivel de las relaciones comerciales. Además, Costa Rica firmó la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica) el 22 de noviembre de 1969, cuyo artículo 11, inciso 2 establece: “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.”

Como se dijo, Costa Rica no tiene todavía una ley de Protección de la Vida Privada, sin embargo, el hecho de que en la Constitución lo establezca como un derecho fundamental, hace obligatorio su cumplimiento.

Se considera un avance el hecho de que ya haya un proyecto en este sentido presentado a la Asamblea Legislativa. Este proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales es muy completo en términos de aplicación de los principios de tutela y de la creación de una organización técnica específica dirigida a ser un modelo institucional de tutela.

Considerando las garantías revisadas, el proyecto de ley costarricense no establece nada sobre las siguientes garantías (ver anexo 3 el cuadro sobre Derechos a la protección de datos):
Derecho para la prohibición de interconexión de archivos,
Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente.
Por lo que se recomienda incorporar en el proyecto estas garantías.

Tampoco establece nada respecto a las cookies y a la distribución de direcciones electrónicas a terceros para asuntos mercadotécnicos, sin el consentimiento del titular de la dirección, aunque esto último puede decirse que el Reglamento autónomo de servicio para la regulación del correo electrónico masivo no deseado de RACSA viene a solventar esta situación, una medida interesante de analizar, puesto que RACSA es el proveedor del servicio de Internet, no así el responsable directo de la publicidad enviada. Esto funciona en Costa Rica, pues solo son dos proveedores de servicios de Internet y ambos son del Estado.

También es importante incorporar expresamente en la normativa sobre protección al consumidor o en la Ley de Protección de la Persona Frente al tratamiento de sus Datos Personales, lo relativo a las cookies, la distribución no autorizada de direcciones electrónicas a terceros sin el consentimiento del titular y la prohibición del spam excepto cuando el consumidor lo autorice.

Es importante incluir en la normativa relacionada con la protección al consumidor lo relacionado a la protección de datos personales, de manera semejante como lo ha hecho Ecuador incluyendo un artículo de Protección de Datos en la Ley 67 de Comercio electrónico, firmas y mensajes de datos. Esto debido a que en una relación de compra venta siempre el consumidor debe proporcionar datos personales cuyo tratamiento debe quedar debidamente normado. Esta protección debe incluir la garantía del proveedor de respetar el derecho a la privacidad y a la protección de los datos del consumidor en el ámbito informático, que incluya los siguientes derechos: conocimiento, calidad, acceso, rectificación, oposición, consentimiento, fijar el nivel de protección, uso

conforme al fin, tutela, indemnización, no discriminación, prohibición de interconexión de archivos, e impugnación de valoraciones basadas sólo en datos procesados automáticamente.

Y además, dar trámite más expedito al proyecto de Ley No.15.178 Protección de la persona frente al tratamiento de sus datos personales, el 27 de marzo de 2003 pasó a estudio de la Comisión Permanente de Asuntos Jurídicos y al proyecto 14785 para adicionar el recurso de Hábeas Data a la Ley de Jurisdicción Constitucional, que pasó a estudio de la Comisión Permanente de Asuntos Jurídicos el 18 de junio del 2002, este último para explicitar el recurso en la leyde Jurisdicción Constitucional.

Se detecta el vacío de que el proyecto de ley Protección de la persona frente al tratamiento de datos personales se refiere a la protección del ciudadano en territorio nacional y frente a empresas establecidas en territorio nacional. Si la violación de las garantías establecidas en la Ley es por parte de una empresa o persona en el extranjero, el proyecto de Ley no establece los procedimientos para que el consumidor o ciudadano pueda plantear el reclamo, y que éste sea resuelto de forma ágil y eficaz.

Un mayor detalle de los vacíos propiamente del Proyecto de Ley Protección de la persona frente al tratamiento de datos personales puede encontrarse en la sección del Análisis del Proyecto.

Ciertamente es difícil exigir a las empresas que venden a través de Internet, el respeto a las leyes costarricenses. Sin embargo, la tutela del consumidor es a través de su propio actuar, un consumidor bien informado puede denunciar las violaciones a sus derechos e iniciar los procesos para demandar su indemnización. Se recomienda que el Estado informe y eduque a los consumidores en materia derechos y deberes en el ámbito del comercio y principalmente en materia de comercio electrónico.

Por otro lado, se puede afirmar que la mayoría de los sitios que recolectan información personal de los consumidores no tienen una política de privacidad o ésta es insuficiente. Es decir, no se indica a los usuarios las medidas utilizadas para proteger la información

almacenada, cómo y a quienes se comunicarán sus datos y cómo puede el consumidor acceder a ellos.

Se recomienda incluir en la normativa de Protección al Consumidor la obligación a los proveedores, que recolecten información de los consumidores, tener políticas de privacidad. Que estas políticas se exhiba en forma clara y destacada en la página principal del sitio y en cada parte del mismo en que se recolecte información personal, y además debe ser clara, precisa y entendible.

Se propone que la política de privacidad incluya lo siguiente:

- la identificación de la empresa dueña y administradora del sitio
- la naturaleza de la información recolectada
- la justificación del almacenamiento de la información
- el uso que se le va a dar
- quiénes comparten la información recolectada
- los derechos de oposición que tiene el usuario
- el tiempo que la información es almacenada
- los mecanismos de seguridad para evitar intromisiones en el almacenamiento de la información personal, y durante la transmisión por las redes de comunicación
- cómo puede cambiar en el futuro la política de privacidad del sitio
- la identificación de la persona responsable de la privacidad de la información
- la identificación del organismo encargado de vigilar y fiscalizar en materia de tratamiento de datos personales.

Por otro lado, la seguridad en los datos personales que se transmiten a través de la red se logra por medio del sistema de Criptografía asimétrica, con autoridades certificantes y firmas digitales. Pero la seguridad en los lugares de recepción y almacenamiento de la información debe incluir entre otros: políticas empresariales o institucionales sobre medidas de seguridad, protocolos de seguridad, auditorías, controles, mecanismos tecnológicos para su resguardo (claves para los responsables), así como medidas de protección contra daños fortuitos (incendio, humedad, etc.). Debe quedar establecida en la Ley de Protección de la persona frente al tratamiento de sus datos personales la

obligación de que las empresas, que manejan datos de las personas, tengan todas estas medidas adicionales de seguridad.

Otra recomendación es el establecer explícitamente el procedimiento que debe realizar el consumidor para reclamar cuando una garantía tutelada por la ley de protección de datos sea violada, para los casos de que el infractor se encuentre en el extranjero. Esto es importante, porque en las transacciones comerciales electrónicas, los proveedores pueden ser empresas ubicadas en el extranjero, los cuales piden datos personales a los consumidores. El proyecto de ley no establece cómo se reclama en estos casos.

Con relación a la transferencia internacional de datos, la aplicación estricta de la Directiva Europea puede interrumpir y perjudicar cualquier tipo de transacción comercial que incluya el uso y transferencia internacional de datos personales, el cual se ve potenciado por el desarrollo del comercio electrónico. Cualquier comerciante en línea que está haciendo negocios en Europa, estará sujeto a las normas de protección de datos que ésta establece, lo que lo obliga a tomar las medidas necesarias para proteger la privacidad de los individuos en relación al procesamiento y difusión de datos personales y la confidencialidad de esos datos.

Los países que tienen una actividad comercial mayor con Europa tendrán inevitablemente mayor flujo internacional de datos y mayor será la posibilidad de que encuentren problemas con estos flujos de datos que pueden comprometer los datos personales de los ciudadanos europeos. Esto incluye transmisiones relativas a archivos de recursos humanos, datos personales relativos a viajes, los sistemas de reservas en el transporte aéreo, evaluaciones, información empresarial identificando sujetos tales como listados de clientes, y toda otra situación donde existe transferencia de datos personales al exterior (Palazzi, 2002).

La Unión Europea sólo requiere que los países tengan legislación “adecuada”, no que adopten esencialmente la misma legislación. La Unión Europea creó un Grupo de Trabajo para examinar las condiciones en los terceros países donde eventualmente podrían realizarse transferencias. Además la Unión Europea se encuentra en

constantes negociaciones para llegar a un acuerdo y para el caso de empresas individuales, existen vías alternativas en la Directiva para permitir las transferencias a pesar de la existencia de una prohibición general, tal es el caso de contratos o las excepciones.

En Europa no se escatiman esfuerzos dirigidos a conjugar la protección de los datos personales de los individuos de los Estados miembros con los intereses económicos que se derivan de la libre contratación internacional.

De la experiencia europea, se recomienda incorporar en el proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales la posibilidad de transferir datos a terceros países que no ofrecen nivel adecuado de protección siempre que los responsables del tratamiento cumplan con ciertas condiciones que pueden establecerse en instrumentos similares al acuerdo de Puerto Seguro, las Cláusulas Contractuales Tipo o a las Normas Corporativas Vinculantes de la Unión Europea.

Como se vio, la protección de los datos personales es una materia en el que deben participar el Estado con sus normas y las empresas con formas de autorregulación. Por esta razón, se considera importante no solo posibilitar los mecanismos de autorregulación, sino que se incentive su utilización, y así dejarlo establecido en el Proyecto de Ley costarricense.

Como Costa Rica no tiene aún la Ley, se recomienda realizar las modificaciones para incorporar las observaciones planteadas al proyecto de ley de Protección de la persona frente al tratamiento de sus datos personales y dar trámite más expedito para su aprobación, incluido el proyecto de incorporar el hábeas data a la Ley de Jurisdicción Constitucional. Y de acuerdo con Chirino y Carvajal (2003):

> "No puede el país continuar careciendo de una adecuada y detallada regulación referente al manejo de los datos de las personas. No puede seguir dependiendo casi exclusivamente de la jurisprudencia constitucional y de algunas escasas conminaciones penales como únicos mecanismos de tutela de la intimidad. No puede conformarse con algunos mecanismos de tutela reactiva ante las violaciones a la autodeterminación informativa, ni puede seguir teniendo como único órgano protector una instancia jurisdiccional genérica, saturada, y poco

> dotada de los recursos y conocimientos técnicos necesarios para garantizar una efectiva protección." (Chirino y Carvajal, 2003, p. 283).

Por otro lado, el problema de la tutela de la intimidad, en un ambiente de comercio electrónico, va más allá de la protección a nivel nacional, debido a la necesidad, facilidad y velocidad de las comunicaciones internacionales para establecer las relaciones comerciales u otras relaciones. Por tal motivo, los mecanismos de protección, leyes y otros, deben considerar esta característica de internacionalidad, y por lo tanto, las soluciones no pueden venir a nivel de un país, sino que debe pensarse en grupos de países con los que se permita establecer las relaciones. Si estas relaciones pueden establecerse con cualquier país del mundo, la solución debe ser a nivel de todo el mundo, en este caso, puede ser por medio de los Organismos Internacionales existentes, como la ONU, la OMC, la OCDE u otros.

Por lo anterior, se recomienda estudiar los mecanismos que ha utilizado la Unión Europea para que el grupo de países que lo conforman respeten y hagan cumplir las directivas sobre protección de datos personales o de la vida privada establecidas a nivel comunitario.

En los casos de archivos en manos privadas, debe encontrarse mecanismos de protección de las personas por el uso de sus datos privados semejante al establecido por la Unión Europea para la protección de los datos personales que consten en los archivos de cualquier institución u organismo de la Comunidad, creando el Supervisor Europeo de Protección de Datos.

Esto último es una propuesta que ya otros autores lo han mencionado, como Palazzi (2002) que manifiesta:

> "Tal vez la única solución posible en materia de protección de datos personales sea alcanzar un acuerdo mundial, ya sea a través de normas similares, leyes tipo, convenios internacionales, o –como está ocurriendo a la fecha-, con la diseminación del modelo europeo en América Latina, Europa del Este y algunos países de Asia.
>
> La privacidad constituye un valor importante para el desarrollo de una sociedad más democrática, fundada en el respeto de los derechos del hombre. La protección de datos personales es la herramienta destinada a hacerla efectiva en este tema tan sensible de la sociedad de la información." (Palazzi, 2002, p. 204).

También Argüello (2005) que indica que los problemas globales requieren soluciones globales y propone una Red de Protección de Datos Personales a nivel Iberoamericano, propuesta que también la hace Iriarte (2005). Y Aced (2005) visiona que lo mejor en un futuro sería llegar a la aprobación de un instrumento internacional vinculante en materia de protección de datos, con vocación universal, que permita el establecimiento de un marco jurídico seguro y estable que sin duda redundará en un incremento de la confianza de los ciudadanos y en un desarrollo más armónico de la Sociedad de la Información.

Se recomienda la promulgación de la normativa de protección de datos personales para los países que todavía no la tienen, en la que se incluya la creación de Agencias de Protección de Datos. Estas Agencias de Protección de Datos deben ser implementadas a nivel gubernamental de más alto nivel de acuerdo con Iriarte (2005), que velen por la adecuada protección de los datos personales, y crear una red regional, mejor aún una red global, que coordine los esfuerzos de estas agencias nacionales con capacidad para perseguir a los infractores de esta ley, de forma ágil, en cualquier parte de la región o del mundo en donde se encuentre.

Capítulo 6. Protección al consumidor

Para efectos del análisis, se definen los siguientes conceptos:

Página Web:

> "Las páginas *web* son las unidades básicas de despliegue de la información en la red. Cada página está esencialmente construida a partir de datos (texto y otras clases de información), cuya organización y formato se expresa mediante el lenguaje HTML [2,3]. El acto de navegar la *web* se reduce a la utilización de un programa visualizador [4], que provee la interfaz por medio de la cual una computadora -el "cliente"- solicita a otra -el "servidor"- que le envíe un archivo HTML y sus archivos asociados (imágenes, sonido, etc.). Transferidos estos datos, el programa visualizador los desplegará apropiadamente." (Hess, 2000, p.2)

Consumidor:

La definición de consumidor está presente en las seis leyes de los países analizados, aunque con diferencias en el ámbito de aplicación de sus normas.

Así, en la ley colombiana se especifica que es quien "contrate la adquisición" de un bien o servicio para satisfacer una o más necesidades (art. 1 Decreto 3466 de Colombia); esto limita el ejercicio del derecho a bs directos adquirentes, excluyendo a quien ha recibido el bien por donación o de otra forma que no sea la compra del mismo. En las demás leyes no se hace referencia a tal restricción, por lo que se entiende que cualquier consumidor tendrá derecho a reclamar.

Chile, Ecuador y Perú determinan que solamente es consumidor el "destinatario final" de los bienes y servicios, aunque no es claro quién es "destinatario final"; parte de la doctrina, como en el caso peruano, ha sostenido que solamente es destinatario final, y por ende objeto del derecho de consumo, quien adquiere un bien para fines estrictamente personales, familiares o de su entorno social inmediato, y no para ser de alguna forma incorporado en un proceso de producción.

En el caso colombiano, se ha entendido que es destinatario final el empresario que adquiere ciertos bienes que no entran directamente en el proceso de producción como insumo o materia prima, sino que son parte accesoria de la labor de empresario, y el

bien se agota en el uso que le da ésta, como por ejemplo la adquisición de uniformes para sus trabajadores.

Costa Rica y México incluye expresamente en su definición de consumidor a aquellos que adquieren productos para integrarlos a procesos de producción, transformación o comercialización o prestar servicios a terceros. Además, en estos casos, la ley mexicana indica que sólo si están acreditadas como Microempresas o Microindustrias pueden ser consumidores.

Para efectos de este estudio se entenderá que el consumidor es toda persona que compra bienes o servicios para su consumo final. Y se define al consumidor en Internet como "aquel sujeto destinatario final de bienes y servicios, que adquiera o utilice los mismos por medio de cualquier forma de contratación o intercambio de información basado en medios electrónicos sobre Internet. Se considera relación de consumo aquella, en la que en uno de los extremos de la relación existe un contratante que puede ser calificado como consumidor" (Rivero, 1997, p.51).

Además, se entenderá por "proveedor en Internet, todo aquel que mediante el uso de la plataforma tecnológica ofrecida por Internet, desarrolle actividades de producción, fabricación, importación, comercialización de bienes y prestación de servicios a consumidores, por las que cobre un precio" (Burgos, 2003, p. 267).

En este capítulo se hará un análisis integral de la normativa sobre el comercio electrónico desde la perspectiva de la protección del consumidor en los ámbitos de: la privacidad, la contratación electrónica y la seguridad.

Se analizará la situación de la normativa del comercio electrónico y la protección del consumidor en relación a tres momentos existentes en una compra vía Internet:

- Antes de la realización de una compra
- En el momento mismo de la compra
- Después de haber realizado la compra

En cada uno de estos momentos, se analizará los aspectos de la privacidad, la contratación y la seguridad que pueden afectar los derechos del consumidor. Para organizar el análisis, se presenta primero las disposiciones encontradas a nivel de organismos internacionales y de los países latinoamericanos en estudios: Chile, Colombia, Costa Rica, Ecuador, México y Perú; luego se identifican los aciertos, los vacíos y por último se presentan las recomendaciones.

En los anexos 1 y 2 puede encontrarse un resumen de la normativa relacionada.

6. 1. Protección del consumidor antes de realizar la compra

En una compra realizada a través de Internet, la protección antes de realizar la compra se refiere a la información y a la publicidad que el consumidor recibe y al respeto de su privacidad.

6. 1.1 Información y Publicidad

El derecho a la información es un derecho del consumidor y un deber para los comerciantes; esto por cuanto los conocimientos técnicos del primero son nulos o escasos frente a los del proveedor. Este derecho es el principal que debe ejercer el consumidor, y debe asistirlo durante toda las fases del negocio y la contratación; incide tanto en los aspectos previos como durante el negocio mismo y después de finalizado éste (Bruce, 2002).

Para la divulgación de la información de los bienes y servicios que ofrecen, las empresas lo llevan a cabo por medio de sus páginas Web, entre otros medios de comunicación. En esta página Web despliega la publicidad de lo que ofrecen. La publicidad es toda información susceptible de inducir a una persona a hacer una elección sobre un producto o servicio determinado.

El consumidor utiliza Internet para buscar contenidos de información que le interese, al mismo tiempo puede encontrar o le puede aparecer publicidad no deseada, contenidos ofensivos o ilegales. Esto hace necesario resolver jurídicamente el problema de la invasión de la privacidad, así como la comisión de delitos por Internet (como la pornografía, el proxenetismo, venta ilegal de productos prohibidos, etc.).

La publicidad en Internet llega a todo el mundo, por lo que se hace necesario encontrar mecanismos para que no se viole la legislación nacional ni la de los países hacia los cuales va dirigida la publicidad. Esto debido a que los países no tienen las mismas prohibiciones.

La publicidad que se hace debe ser lícita, honesta, decente y verídica. El anunciante debe identificarse, informar sobre las razones de una posible recopilación de datos, indicar a quiénes va dirigida la publicidad, y respetar la confidencialidad así como las disposiciones particulares sobre la publicidad infantil y las sensibilidades diversas del público mundial.

6.1.1.1 Disposiciones de organismos internacionales

De acuerdo con el artículo 4 de la Directiva 1997/7/CE relativa a la protección de los consumidores en materia de contratos a distancia de la Unión Europea, antes de celebrar un contrato, el consumidor debe disponer de la siguiente información:

> "a) identidad del proveedor y, en caso de contratos que requieran el pago por adelantado, su dirección;
> b) características esenciales del bien o del servicio;
> c) precio del bien o del servicio, incluidos todos los impuestos;
> d) gastos de entrega, en su caso;
> e) modalidades de pago, entrega o ejecución;
> f) existencia de un derecho de resolución, salvo en los casos mencionados en el apartado 3 del artículo 6;
> g) coste de la utilización de la técnica de comunicación a distancia cuando se calcule sobre una base distinta de la tarifa básica;
> h) plazo de validez de la oferta o del precio;
> i) cuando sea procedente, la duración mínima del contrato, cuando se trate de contratos de suministro de productos a servicios destinados a su ejecución permanente o repetida." (Directiva 1997/7/CE, Unión Europea, p.4).

Su artículo 10 establece:

> “Articulo 10. Restricciones de la utilización de determinadas técnicas de comunicación a distancia
> 1. La utilización por un proveedor de las técnicas que se enumeran a continuación necesitará el consentimiento previo del consumidor:
> -sistema automatizado de llamada sin intervención humana (llamadas automáticas),
> -fax (telecopia).
> 2. Los Estados miembros velarán por que las técnicas de comunicación a distancia distintas de las mencionadas en el apartado 1, cuando permitan una comunicación individual, sólo puedan utilizarse a falta de oposición manifiesta del consumidor.” (Directiva 1997/7/CE, Unión Europea, p.6).

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre Comercio Electrónico), indica en su artículo 5 que los prestadores de servicios electrónicos deberán proporcionar a los usuarios y a los órganos de control una serie de informaciones referentes tanto de sus actividades como del contenido y condiciones de un eventual contrato. En concreto, según la directiva, los proveedores deberán proporcionar los datos siguientes de forma fácil, directa y gratuita:

1. El nombre del prestador de servicios,
2. La dirección geográfica donde está establecido el prestador,
3. Señas que permitan ponerse en contacto con el prestador de servicios de forma directa y efectiva, incluido su correo electrónico,
4. Si el prestador de servicios está inscrito en un registro mercantil, el nombre del registro y los datos de inscripción en ese registro.
5. Si una actividad está sujeta a una autorización (administrativa u otras), los datos de la autorización y los de identificación del órgano encargado de la supervisión.
6. Si el prestador ejerce una profesión regulada deberá indicar:
    a) el nombre del colegio profesional al que en su caso pertenezca,
    b) título profesional expedido,
    c) referencia a las normas profesionales y los medios por los cuales se puedan conocer.
7. En su caso el número de identificación fiscal.
8. El precio de los bienes o servicios debe constar de forma clara y sin ambigüedades con la indicación, en su caso de si están incluidos los impuestos y los gastos de envío.

Además, indica en su artículo 10 la información exigida al prestador de servicios antes de que el destinatario del servicio efectúe un pedido:

> "a) los diferentes pasos técnicos que deben darse para celebrar el contrato;
> b) si el prestador de servicios va a registrar o no el contrato celebrado, y si éste va a ser accesible;
> c) los medios técnicos para identificar y corregir los errores de introducción de datos antes de efectuar el pedido;
> d) las lenguas ofrecidas para la celebración del contrato." (Directiva 2000/31/CE, 2000, p.12).

También indica esta misma Directiva que debe estar disponible al consumidor los códigos de conducta a los que se acoge el proveedor y las condiciones generales de los contrato.

Su artículo 7 se refiere a las comunicaciones comerciales no solicitadas indicando que los Estados debe garantizar la identificación del prestador de servicio que envió la comunicación comercial no solicitada, y que éstos consulten regularmente las listas de exclusión voluntaria de personas que no desean recibir dichas comunicaciones.

En su artículo 16 de esta misma Directiva fomenta el uso de código de conducta a nivel comunitario para la correcta aplicación de la normativa de la Directiva.

La Directiva 2002/58/CE de la Unión Europea (art.13, incisos 3 y 4) indica que los Estados tomarán medidas para que no se permita comunicaciones no solicitadas con fines de venta directa y se prohíbe la práctica de enviar mensajes electrónicos en donde no se indique una dirección válida para que el consumidor pueda poner fin a tales comunicaciones.

La recomendación de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico indica, en relación con la publicidad, el principio de "Equidad en las prácticas empresariales, publicitarias y de mercadotecnia", refiriéndose a que:

> "Las empresas involucradas en el comercio electrónico deben respetar los intereses de los consumidores y actuar de acuerdo a prácticas equitativas en el ejercicio de sus activi dades

> empresariales, publicitarias y de mercadotecnia." (Segunda Parte, inciso II, Lineamientos de la OCDE para la protección del Consumidor, 1999, p.5).

Este principio establece que las empresas no deben realizar prácticas falsas, engañosas, fraudulentas o desleales; no deben aprovecharse de las características del comercio electrónico para ocultar su identidad y ubicación; no deben provocar riesgos en perjuicio de los consumidores; la información que presenten debe ser clara, visible, precisa y de fácil acceso; deben respetar la decisión del consumidor de recibir o no mensajes comerciales no solicitados por correo electrónico; deben tener cuidado con la publicidad dirigida a niños, ancianos, enfermos u otros grupos vulnerables.

Relacionado con el principio de "Información en Línea", establece que las empresas deben proporcionar la información de manera clara, precisa, fácil y suficiente que permita lo siguiente: identificación de la empresa, domicilio geográfico y medios de contacto; comunicación rápida, fácil y efectiva con la empresa; mecanismos efectivos de solución de disputas; servicios de atención a procedimientos legales; dirección del domicilio legal de la empresa y sus directivos. Sobre los bienes y servicios, indica:

> "Las empresas que realicen transacciones con consumidores por medio del comercio electrónico deben proporcionar información precisa y fácilmente accesible que describa los bienes o servicios ofrecidos, de manera que permita a los consumidores tomar una decisión informada antes de participar en la transacción, y en términos que les permita mantener un adecuado registro de dicha información." (segunda Parte, inciso III, Lineamientos de la OCDE para la protección del Consumidor, 1999, p.7).

Por otro lado, sobre la información que deben dar las empresas relativa a la transacción, indica que deben incluir: costos totales cobrados, impuestos, otros costos aplicados rutinariamente; términos de entrega o prestación del servicio; términos, condiciones y formas de pago; restricciones, limitaciones o condiciones de compra; instrucciones para el uso adecuado del producto; disponibilidad de servicios posventa; información sobre retractación, devolución, terminación, intercambio, cancelación, reembolso; y pólizas y garantías.

En resumen, la información y publicidad que se divulgue para ofrecer productos o servicios, debe contener al menos la siguiente información:

- Identidad del proveedor,

- domicilio geográfico del proveedor de bienes o servicios,
- medios de contacto,
- las características especiales de producto,
- el precio (si tienen los impuestos incluidos o no),
- los gastos de transporte o de entrega,
- la forma de pago,
- las modalidades de entrega o de ejecución de servicios,
- el plazo de la validez de la oferta,
- garantías,
- países a los que se dirige la publicidad,
- indicación de la posible recopilación de datos del consumidor y su justificación,
- advertencias sobre contenidos no apto y a qué tipo de población se refiere.
- procedimientos para reclamos o mecanismos efectivos de solución de disputas,

Además otra de importancia como:
-Mecanismos de comunicación rápida, fácil y efectiva con la empresa,
-servicios de atención a procedimientos legales,
-dirección del domicilio legal de la empresa y sus directivos,
- referencia en el registro mercantil,
-los diferentes pasos técnicos que deben darse para celebrar el contrato,
-si el prestador de servicios va a registrar o no el contrato celebrado, y si éste va a ser accesible,
-los medios técnicos para identificar y corregir los errores de introducción de datos antes de efectuar el pedido.

Uno de los fines principales del derecho del consumo es restablecer la asimetría que existe entre consumidor y empresario; este equilibrio sólo se logra cuando el consumidor tiene toda la información del producto disponible, y puede elegir libremente su relación de consumo.

6.1.1.2 Análisis de legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México, Perú.

En relación con la información, sólo las leyes de Chile y Ecuador sobre protección al consumidor, incluyen en su articulado la definición de la información básica comercial que debe dar los proveedores de bienes y servicios. La ley Orgánica de Defensa del Consumidor de Ecuador incluye un capítulo entero relacionado con la información básica comercial y otro referido a la publicidad y su contenido, la ley chilena 19.496 sobre protección al consumidor también incluye una serie de artículos normativos sobre la Información y publicidad, así como sobre las ofertas y promociones en su Título III.

La ley chilena 19.496 indica que en contratos por medios electrónicos o cualquier otra forma de comunicación a distancia el proveedor debe informar de forma fácil y accesible los pasos a seguir para celebrar el contrato, si el documento electrónico será archivado y si éste será accesible al consumidor. Además debe indicar su dirección electrónica o postal y los medios que pone a disposición del consumidor para identificar y corregir errores en el envío o en sus datos.

La información sobre las propiedades, características, ingredientes, materiales utilizados en la elaboración, valores nutritivos, precauciones o contraindicaciones de los productos, entre otros, hacen más transparente la adquisición de bienes y servicios; esta es una obligación a cargo de todo productor y/o proveedor establecidos en todas las legislaciones de los países analizados: Colombia (art.14 Decreto 3466), Perú (art.8, 15, 16 Decreto 716), Ecuador (art.17 Ley Orgánica de Defensa del Consumidor), Chile (art.28, 28 A, 28 B Ley 19496), México (art.7 Ley Federal de Protección al Consumidor) y Costa Rica (art.31 y 34 Ley 7472).

En la ley colombiana, a diferencia de las leyes de los demás países, la responsabilidad por la información insuficiente o engañosa está limitada al productor. Por tanto, no es posible sancionar a un proveedor que no ha informado suficientemente sobre el producto que distribuye (art.31 y 32 Decreto 3466, Colombia).

La Constitución Política de Costa Rica, en su artículo 46 (reformado por la ley 7607 del 18 de junio de 1996), establece en su párrafo quinto:

> "Los consumidores y usuarios tienen derecho a la protección de su salud, ambiente, seguridad e intereses económicos, a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo. El Estado apoyará los organismos que ellos constituyan para la defensa de sus derechos. La ley regulará esas materias." (Rivera, 2003, p.21)

También en la Ley 7472 de Promoción de la Competencia y Protección Efectiva del Consumidor, en sus artículos 29, 31 y 34, establece como un derecho del consumidor el recibir información veraz y oportuna, y la obligación del vendedor de informar, así como los requisitos de la oferta y publicidad de los bienes y servicios.

En relación a la publicidad, las legislaciones de los países analizados establecen sanciones y prohibiciones para la publicidad falsa, engañosa o abusiva. Se consideran infracciones a la norma, en general, inducir a error sobre la naturaleza del bien, sus características o componentes, precio, origen o cualquier otra información sobre el producto que no corresponda a la verdad.

En el caso de Perú existen otras leyes apartes, como el Decreto legislativo 691 que norma lo relacionado a la publicidad en defensa del consumidor y la ley 28493 que regula la publicidad enviada por correo electrónico (spam), esta ley incluye la posibilidad de que el consumidor manifieste su voluntad de no recibir mensajes, y se considera correo electrónico comercial ilegal cuando se transmita a un receptor que haya formulado el pedido de que no se envíe dicha publicidad.

La ley chilena incluye un artículo referente a la información publicitaria (art.28 B Ley 19496) enviada por medio del correo electrónico, indicando que debe contener una dirección del remitente que permita al consumidor indicar la suspensión de los envíos.

En Costa Rica, Radiográfica Costarricense S.A. (RACSA) es una empresa pública que provee servicios de telecomunicaciones, la cual tiene el "Reglamento autónomo de servicio para la regulación del correo electrónico masivo no deseado" que regula los

correos electrónico no deseado estableciendo prohibiciones y sanciones a los usuarios de los servicios que presta RACSA.

La Ley 67 de comercio electrónico, firmas y mensajes de datos de Ecuador indica que en el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos. La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo es sancionado.

La Ley Federal de Protección del Consumidor de México, incita a los comerciantes a no utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y además el comerciante debe de cuidar las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, debiendo incorporar mecanismos que adviertan cuando la información no sea apta para esa población. (Artículo 76 bis párrafo VII de la Ley Federal de Protección al Consumidor). Las disposiciones de este artículo se aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

El artículo 17 establece que en la publicidad que se envíe debe indicarse datos del proveedor como su nombre y dirección electrónica, también que el consumidor puede exigir al proveedor o empresa a no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o cualquier otro medio para ofrecerle bienes, productos o servicios, y que no le envíen publicidad.

La ley Federal de Protección al Consumidor también prevé que los comerciantes deben tener códigos de ética respecto de las transacciones que elaboren con los

consumidores a través del uso de medios electrónicos (artículo 24 IX bis de la Ley Federal de Protección al Consumidor).

La publicidad que anuncia ofertas y promociones es, en muchos casos, la que más se utiliza para inducir a error al consumidor. En este sentido, las legislaciones de los países analizados han regulado este tipo de publicidad de diferentes maneras.

En la ley de Colombia, se presume que existe inducción a error al consumidor cuando se ofrece un incentivo y éste no se entrega en la oportunidad y forma indicada, o cuando como consecuencia de la oferta o promoción se aumenta el precio del bien o se reduce su calidad (art.16 Decreto legislativo 3466).

La ley ecuatoriana, por su parte, establece que en las ofertas o promociones se debe informar el antiguo y el nuevo precio, y en caso de que se haga ofrecimiento de sorteos o rifas, se debe anunciar la cantidad de premios a repartir, y el plazo y el lugar donde se sortearán (art. 46 Ley Orgánica de Defensa del Consumidor).

También en la ley 67 de comercio electrónico, firmas y mensajes de datos de Ecuador establece un capítulo sobre los derechos de los consumidores en relación con servicios electrónicos.

La norma peruana exige a quien vaya a realizar rifas, sorteos, concursos o cualquier otro sistema de promoción de un bien, obtener una autorización previa por parte del Estado. Igualmente, en los casos de rebajas, promociones u ofertas, el proveedor está en la obligación de indicar la duración de las mismas y el número de bienes a ofertar (art.22, 23 Decreto legislativo 716).

La ley chilena exige que se informe sobre el plazo de las promociones u ofertas, e indica que el consumidor puede exigir el cumplimiento de lo ofrecido por medio de un juez competente (art. 35 Ley 19496).

La Ley Federal mexicana expresamente establece que no se requiere autorización ni avisos previos para realizar una promoción, excepto cuando se dispongan en normas oficiales, en los casos que puedan lesionarse intereses de los consumidores. También establece que el consumidor puede exigir el cumplimiento de la oferta cuando el proveedor no cumple con el ofrecimiento (art.47, 50 Ley Federal de Protección al Consumidor).

La ley costarricense indica que deben prevalecer las cláusulas estipuladas en los contratos, si son más beneficiosas que el contenido de la oferta, la promoción o la publicidad de los bienes y servicios (art.34 Ley 7472) y que toda promoción u oferta especial debe indicar el precio anterior del bien o del servicio, el nuevo precio o el beneficio que de aprovecharlas, obtendría el consumidor (art. 38 Ley 7472). Es una obligación del comerciante cumplir con la oferta publicitada, de lo contrario el consumidor puede acudir a la Comisión Nacional del Consumidor o a los órganos jurisdiccionales competentes para hacer valer sus derechos (art. 31, 43 Ley 7472).

La publicidad es la forma en que el empresario llega al consumidor y vende su producto. Si bien las normas analizadas se basan en los mismos principios de veracidad y suficiencia, existen diferencias y en especial de requisitos que hacen más oneroso al productor y/o proveedor emitir una publicidad. La necesidad de obtener autorización previa o de informar a las autoridades de un país el lanzamiento de una promoción u oferta, hace perder agilidad y eficacia al mercado perjudicando tanto al empresario como al consumidor.

6.1.1.3 Aciertos

Ecuador establece dentro de su ley de protección al consumidor un capítulo relacionado con la información básica comercial y otro con la publicidad y su contenido. Aunque Perú también norma el tema de la publicidad con decretos aparte, es conveniente que todo lo relacionado con la relación de consumo se encuentre en una sola normativa.

Por otro lado, Chile, Perú y México incluye en sus leyes artículos relacionado a la publicidad enviada por correo electrónico, lo cual no se incluye en la normativa sobre protección al consumidor de Costa Rica, Colombia y Ecuador.

México es el único que incluye la promoción del uso de códigos de ética por parte de los proveedores en transacciones celebradas por medios electrónicos u otros.
En México no se requiere autorización del Estado para emitir una promoción, un elemento importante para promover la libre competencia.

6.1.1.4 Vacíos

El Derecho a la Información es fundamental, una información clara y veraz es un imperativo ético que permite el respeto al derecho efectivo de la libertad de elección, basado en precios justos, variedad de productos y servicios de calidad.

La ley 7472 de Costa Rica establece como obligación del comerciante dar información completa sobre el producto o servicio, pero no define un contenido mínimo de información necesario. En este sentido es importante la definición del término Información Comercial Básica que debe tener las ofertas en la publicidad que se realiza, como lo establece la ley ecuatoriana. La ley 7472 tampoco establece el deber de identificarse por parte del comerciante ni tiene normado la publicidad enviada por correo electrónico.

Es conveniente determinar la información que debe resultar obligatorio dar al consumidor en el comercio electrónico. La Ley de promoción de la competencia y defensa efectiva del consumidor vincula al comerciante con la publicidad u oferta que éste realice al público. Lo que se comunique en la promoción es vinculante, relevante y exigible.

Por otro lado, la Ley no establece nada con respecto al control del cumplimiento de las obligaciones del vendedor. La Comisión Nacional del Consumidor actúa si existe

denuncia, no tiene la atribución de ejercer el control del cumplimiento de la normativa por parte de los vendedores.

6.1.1.5 Recomendación

El nuevo ambiente de comercio electrónico ha propiciado la existencia de un mercado abierto, virtual, con ventajas para el oferente como para el demandante. Junto a estas ventajas, se resalta la existencia de inconvenientes que hay que resolver, en especial en lo relativo a la salvaguarda de los derechos de los destinatarios, especialmente los consumidores.

En materia de información y publicidad, se debe resolver la problemática de la invasión a la intimidad y violación a derechos individuales básicos con motivo de acciones de comunicación o promoción.

Se requiere que la información, publicidad y promoción de los productos y servicios ofrecidos por medios electrónicos no infrinjan los derechos de los consumidores y se realicen acordes con la ley.

La publicidad debe ajustarse a unas reglas jurídicas básicas y la comunicación a unos principios éticos y jurídicos, porque esta interrelación que se suscita no solo afecta al emisor y al destinatario, sino que trasciende a terceros competidores. Por tanto, la actividad publicitaria como fenómeno social, en cuanto afecta a intereses varios, debe estar regulada por el Derecho, dado que puede poner en peligro o lesionar distintos bienes jurídicos (Vega, 2005, p.158).

Del análisis anterior, se llega a las siguientes recomendaciones:

Incluir dentro de una sola ley todo lo relacionado a la protección del consumidor, en este caso incluir la regulación de la publicidad en lo relacionado con el consumidor dentro de la ley de protección al consumidor, y que esta regulación tome en cuenta la publicidad

enviada por comercio electrónico. Considerar lo estipulado en la ley 28493 de Perú que regula el uso del correo electrónico comercial no solicitado (spam).

Se sugiere explicitar en la ley los datos de la información del producto o servicio, complementando lo establecido en el artículo 31 de la ley 7472 con el capítulo de "Información Básica Comercial" y "Publicidad y su Contenido" de la ley de Ecuador y el decreto legislativo 691 que norma la publicidad en defensa del consumidor y la ley 28493 que norma el uso del correo electrónico comercial no solicitado (spam) ambas de Perú.

Se recomienda también, incluir en la normativa de la publicidad, además de la información básica comercial indicado anteriormente, otros datos básicos que son importantes para los casos en que la relación comercial se realice por Internet, es decir, los datos de: identificación del proveedor, domicilio geográfico, y medios de contacto (teléfono, fax, e-mail, etc.), gastos de transporte, la forma de pago, las modalidades de entrega o de ejecución de servicios, el plazo de la validez de la oferta, garantías, procedimientos para reclamos, países a los que se dirige la publicidad, indicación de la posible recopilación de datos del consumidor y su justificación, advertencias sobre contenidos no apto y a qué tipo de población se dirige la publicidad, así como: mecanismos de comunicación rápida, fácil y efectiva con la empresa; mecanismos efectivos de solución de disputas; servicios de atención a procedimientos legales; dirección del domicilio legal de la empresa y sus directivos, su referencia en el registro mercantil.

El artículo 31 de la Ley 7472 establece que: "Toda información, publicidad u oferta al público de bienes ofrecidos o servicios por prestar, transmitida por cualquier medio o forma de comunicación, vincula al productor que la transmite, la utiliza o la ordena y forma parte del contrato" (Ley 7472, Costa Rica, p.14). Este precepto deja clara la idea de que la publicidad integra la oferta negocial y la misma obliga y forma parte del contrato, aunque después, a la hora de contratar no se contemple de forma expresa en las distintas condiciones que se entreguen al consumidor. El consumidor puede exigir que el contenido de la publicidad integre la oferta del proveedor, obligándolo a su

cumplimiento. Además de exigírsele su cumplimiento en virtud del ejercicio de las pertinentes acciones judiciales, es claro que también, de no cumplirse por el oferente lo ofrecido en la promoción, podría considerarse una publicidad falsa o engañosa.

En este último caso, desde el punto de vista de protección de los consumidores y usuarios, la publicidad falsa o engañosa, aparte de los efectos que pueda tener respecto a otros competidores, se debería considerar como un fraude y ser sancionado desde lo penal en los casos graves. Esto último, acogiendo la normativa española de la Ley General de Defensa de Consumidores y Usuarios, que en su artículo 8 establece que la publicidad falsa o engañosa será perseguida y sancionada como fraude, e incluso, el Código Penal español reprime conductas especialmente graves en relación con las prácticas publicitarias. El ordenamiento jurídico de España ha querido proteger de manera eficaz los intereses de los consumidores al definir como delito la publicidad falsa o engañosa, imponiendo penas de prisión de seis meses a un año o multa de seis a dieciocho meses a los comerciantes que realicen publicidad falsa o engañosa (artículo 282, Ley 10, España).

Se recomienda entonces incluir en la Ley 7472 que la publicidad falsa o engañosa se considerará como un fraude e incluir en el Código Penal su sanción. En este caso, se debe definir claramente lo que se debe entender por publicidad falsa o engañosa.

También es conveniente incluir una atribución adicional a la Comisión Nacional del Consumidor, que le permite ejercer el control y fiscalización del cumplimiento de las obligaciones del vendedor.

Se sugiere incorporar en la normativa la difusión y promoción del uso de códigos de ética en las relaciones comerciales electrónicas, como lo ha hecho México.

6.1.2 Protección de datos personales del consumidor

El aspecto de privacidad y más específicamente lo relacionado a la protección de datos personales es de gran importancia en el ambiente de comercio electrónico. Esto debido

a que en cualquier transacción comercial que el consumidor realiza a través de una página Web, el mecanismo mayormente utilizado es por medio de contratos de adhesión, que se basan en formularios prediseñados por el proveedor, y en los cuales se solicitan información personal al consumidor.

Por otro lado, también cuando el usuario accede a una página, simplemente para buscar información de algún asunto que le interese, aunque no compre nada, generalmente le piden información antes de otorgarle el permiso de ingresar a la página Web.

El usuario entrega información y no conoce ni es informado para qué ni cómo será utilizada.

El derecho fundamental de la protección de los datos persigue garantizar a la persona un poder de control sobre cualquier tipo de dato personal, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho afectado (Barriuso, 2002, p.425, citado por Vega (2005, p. 358)).

Estos y otros asuntos de importancia relevante en esta materia son desarrollados ampliamente en el capítulo de Privacidad y Protección de datos.

6.2 Protección del consumidor en el momento de la compra

Los contratos más numerosos perfeccionados por medio de una página Web son los de compra y venta (también denominados ventas "*on line*") de una infinidad de productos y en menor número le siguen los contratos de prestación de servicios, de acuerdo con Menéndez (2005). Por lo tanto, se analizará la compra y venta en línea por ser los contratos más comunes celebrados a través de Internet. Este tipo de contrato se realiza por medio de la transmisión telemática y la existencia de documentos en soporte informático.

En este apartado se analizará el momento mismo de la transacción comercial, específicamente lo relacionado al contrato de compra y venta en línea.

Se dividirá el análisis en:

-validez de los contratos vía Internet
- las cláusulas del contrato
- Identificación de las partes
- tiempo y lugar de perfección del contrato
- aspectos relacionados con el pago

El anexo 2 presenta una serie de matrices comparativas de las normas existentes en las legislaciones de los países analizados sobre los diferentes elementos que deben ser regulados en una contratación electrónica. Y el anexo 4 presenta los elementos regulados en las legislaciones y normativa sobre comercio electrónico, firmas digitales y mensajes de datos.

6.2.1 Validez de los contratos vía Internet

Con respecto a la forma del contrato, esta es solo el medio por el cual las partes escogen expresar su voluntad y darla a conocer a los destinatarios. Los contratos electrónicos o informáticos han evolucionado la forma de la escritura en papel a la digital y ya muchos países reconocen jurídicamente el documento electrónico.

El contrato vía Internet tiene como característica de que es celebrado sin la presencia física simultánea de las partes, prestando éstas su consentimiento en origen y destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, concretados por medio de cable, radio, medios ópticos o cualquier otro medio.

En el ambiente de comercio electrónico, la contratación electrónica es la forma en que los consumidores, mediante el uso de la Internet, pueden adquirir y/o vender bienes y servicios a tiempo real, realizando todo tipo de transacciones y contratos.

Es fundamental para el desarrollo del comercio electrónico el reconocimiento legal del documento electrónico, su equivalencia con el documento impreso en papel, y su admisibilidad como prueba en juicio.

Moreno (2002) indica que el fundamento último de la obligatoriedad de los contratos es el principio de la autonomía de la voluntad. Esto significa que la persona tiene libertad de contratar, elegir el tipo contractual, modificar los contratos regulados por ley, modificar el contenido legal de estos contratos, elegir la forma de contratar, entre otras cosas. Además, la tecnología ha hecho posible que el cumplimiento de las obligaciones nacidas del contrato electrónico pueda verificarse a través del mismo medio electrónico por el que se perfeccionó el contrato.

Menéndez (2005) indica que el contrato vía Internet es uno de los tipos de contrato electrónicos y que la admisión de este tipo de contratos debe ser analizada a la luz del ordenamiento jurídico vigente desde dos aspectos:

- La validez del empleo del medio electrónico en la contratación, y la existencia y eficacia teórica del contrato concluido a través de ellos.
- La prueba de la existencia de dicho contrato.

6.2.1.1 Disposiciones de Organismos Internacionales

La Ley de Utah de 1995 facilita las transacciones mediante mensajes electrónicos procurando que sean seguras y confiables mediante mecanismos de firma digital y entidades de certificación. Reconoce la validez jurídica y valor probatorio de los mensajes de datos siempre que tenga firma digital confirmada con clave pública por una entidad certificadora autorizada.

Lo más importante es que establece una regla de validez para todos los actos o transacciones celebrados por medios electrónicos, igualando los documentos en formato papel a los documentos en formato digital.

La norma general consagrada establece que ningún estatuto, regulación o principio de derecho que afecte o sea aplicable al comercio entre estados o internacional podrá negar efecto legal, validez o fuerza legal a alguna transacción o contrato por el solo hecho de que éste tenga forma electrónica.

El ámbito de aplicación de la Ley Modelo sobre Comercio Electrónico de la CNUDMI de 1996, indicado en su artículo 1, es a "todo tipo de información en forma de mensaje de datos utilizada en el contexto de las actividades comerciales" (CNUDMI, 1999, p.3), y hace la observación de que "el término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual" (CNUDMI, 1999, p.3).

Esta Ley Modelo reconoce la contratación electrónica al darle validez jurídica y fuerza probatoria a los mensajes de datos en sus artículos 5, 6 y 12. Además, en el artículo 11 establece la validez de la formación de contratos por medio de mensajes de datos. En su artículo 10 establece sobre la conservación de los mensajes de datos, indica que cuando la ley requiera que los documentos, registros o informaciones sean conservados, esto quedará satisfecho si se cumple las siguientes condiciones:

> "a) Que la información que contengan sea accesible para su ulterior consulta; y
> *b)* Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y
> *c)* Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido." (CNUDMI, 1999, p.7).

Así que la Ley Modelo reconoce, explícitamente el valor jurídico para la formación de la voluntad contractual y prueba de los negocios jurídicos, a los documentos electrónicos, siempre que su contenido sea accesible con posterioridad y se tenga disponibilidad del mismo.

La Ley Modelo sobre Firma Electrónica de la CNUDMI reconoce jurídicamente la firma electrónica en su artículo 6.

El 23 de noviembre de 2005 la Asamblea General de las Naciones Unidas adoptó la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, preparado por la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil Internacional.

El objetivo de dicha Convención es dar seguridad legal y comercial a los contratos internacionales que se concluyen por medio de comunicaciones electrónicas. La Convención da reconocimiento jurídico a los contratos establecidos por comunicaciones electrónicas y reconoce que los contratos pueden ser concluidos por sistemas automatizados de mensajes.

El artículo 9, inciso 4, establece:

> "4. Cuando la ley requiera que una comunicación o un contrato se proporcione o conserve en su forma original, o prevea consecuencias en el caso de que eso no se cumpla, ese requisito se tendrá por cumplido respecto de una comunicación electrónica:
> a) Si existe alguna garantía fiable de la integridad de la información que contiene a partir del momento en que se generó por primera vez en su forma definitiva, en cuanto comunicación electrónica o de otra índole; y
> b) Si, en los casos en que se exija proporcionar la información que contiene, ésta puede exhibirse a la persona a la que se ha de proporcionar.
> 5. Para los fines del apartado a) del párrafo 4:
> a) Los criterios para evaluar la integridad de la información consistirán en determinar si se ha mantenido completa y sin alteraciones que no sean la adición de algún endoso o algún cambio sobrevenido en el curso normal de su transmisión, archivo o presentación; y
> b) El grado de fiabilidad requerido se determinará teniendo en cuenta la finalidad para la que se generó la información, así como todas las circunstancias del caso." (CNUDMI, 2005, p. 6).

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, tiene un apartado relacionado con los contratos por vía electrónica.

Esta Directiva prevé que los Estados deben vigilar que su sistema jurídico pueda hacer posible la existencia de los contratos por vía electrónica. Esta recomendación va dirigida a que se reconozca el proceso contractual y que los contratos concluidos electrónicamente no sean privados de validez por este motivo.

También indica que los Estados Miembros pueden disponer excepciones para ciertas categorías de contratos como los siguientes: contratos de creación o transferencias de derechos inmobiliarios (excepto los derechos de arrendamientos); contratos que requieran intervención de tribunales, autoridades públicas o profesionales que ejerzan una función pública; contratos de crédito y caución y las garantías presentadas por personas que actúan por motivos ajenos a su actividad económica, negocio o profesión; los contratos en materia de Derecho de Familia o de sucesiones.

6.2.1.2 Legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México, Perú.

La legislación chilena, ley 19799, en su artículo 2, inciso d) define el concepto de documento electrónico y establece en su propia definición que el documento electrónico debe estar almacenado en medios electrónicos que permitan su uso posterior.

Por otro lado, el artículo 3 indica que los actos y contratos suscritos con firma electrónica tendrán valor jurídico como los realizados por escrito en soporte de papel, con excepción de aquellos actos que requieran alguna solemnidad que no pueden cumplirse por medio electrónico, que requieran presencia personal de las partes, y los relativos al Derecho de Familia. Los artículos 4 y 5 indican que los documentos electrónicos podrán presentarse en juicio y tendrán validez probatoria si fueron suscritos mediante firma electrónica avanzada. De lo contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.

En Colombia el artículo 14 de la Ley 527 sigue la norma del artículo 11 de la Ley Modelo sobre Comercio Electrónico en la que se establece la formación y validez de los contratos expresados por medio de mensaje de datos.

Los artículos 5, 6, 7, 8 y 10 le dan reconocimiento jurídico, admisibilidad y fuerza probatoria a los mensajes de datos. Además el artículo 28 atribuye un mensaje con firma digital a su autor. Además, el artículo 9 define el concepto de integridad de un mensaje de datos.

Igualmente, el artículo 12 de la Ley 527 sigue la norma del artículo 10 de la Ley Modelo sobre la conservación de los mensajes de datos, indica que cuando se requiera, la información contenida debe ser accesible para una consulta posterior, que sea conservado en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y la información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

En Costa Rica el artículo 4 de la Ley 8454 califica a los documentos electrónicos como públicos o privados y les reconoce fuerza probatoria en las mismas condiciones que a los documentos físicos.

El artículo 6 de la misma Ley indica que cuando se requiera que un documento sea conservado, se podrá hacerlo por medio del soporte electrónico, siempre que se garantice su inalterabilidad, su acceso o consulta posterior y se preserve la información relativa a su origen y otras características básicas.

Además, el artículo 8 indica que la firma digital asociado a un documento electrónico es aquel que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.

Por último, el artículo 9 indica que los documentos o comunicaciones suscritos con firma digital tendrán el mismo valor y eficacia probatoria que su equivalente firmado en manuscrito, y que los documentos públicos deben tener firma digital certificada.

Por otro lado, se hace la observación de que la normativa costarricense anterior a la Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, promulgada en agosto del 2005, ya tenía incorporado dentro de varias de sus leyes el término o concepto de documento electrónico: artículo 368 del Código Procesal Civil (Ley 7130); artículo 3 de la Ley del Sistema Nacional de Archivos (Ley 7202); artículo 1 de la Ley de Registro, Secuestro y Examen de documentos privados e intervención de las comunicaciones (Ley 7425); artículo 94 de la Ley de Justicia Tributaria (Ley 7535);

artículo 6 bis, 47 bis, 147 de la Ley Orgánica del Poder Judicial (Ley 7333), artículo 40 de la Ley de Contratación Administrativa y su Reglamento (Ley 7494); artículos 103 y 108 de la Ley General de Aduanas (Ley 7557).

La Ley 67 de Ecuador le da reconocimiento jurídico a los mensajes de datos en su artículo 2, y establece la validez de los contratos electrónicos instrumentados mediante mensajes de datos en su artículo 45. Además en su artículo 12 le da validez y reconocimiento jurídico a la firma electrónica, y fuerza probatoria como prueba en juicio.

Además, el artículo 8 indica sobre la conservación del mensaje de datos que ésta queda satisfecha si se cumple las siguientes condiciones: que la información sea accesible para su posterior consulta, que sea conservado en algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida, los datos para determinar origen y destino y la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado, se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Este artículo es semejante a la norma de la CNUDMI y a la colombiana agregando la condición de integridad del mensaje de datos por un tiempo establecido.

La Ley Mexicana, en el artículo 89 bis del Decreto sobre firma electrónica del 29 de agosto del 2003 indica que no se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos. Además en su artículo 93 indica que cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente. Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.

Además este artículo indica que los actos que requieran fe pública también pueden ser expresados por medio de mensajes de datos, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

El artículo 93 bis indica que cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos si se garantiza la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma. Y define que el contenido de un Mensaje de Datos es íntegro:

> "si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso." (Decreto sobre firma digital México, 2003, p.4).

En Perú el Decreto Supremo 019-2002-JUS que reglamenta la Ley 27269, en su artículo 7 indica que las firmas electrónicas, los mensajes de datos y documentos firmados electrónicamente podrán ser admitidas como prueba en toda clase de procesos o procedimientos.

En su artículo 6 reconoce otras firmas electrónicas (las generadas fuera de la Infraestructura Oficial de Firma Electrónica) siempre que sean acreditadas o reconocidas por la Autoridad Administrativa competente.

En su artículo 10 establece sobre la conservación de los mensajes de datos o documentos electrónicos que cuando el usuario o la ley lo exija deberá cumplir con lo siguiente: que sean accesibles para su posterior consulta, que sean conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido digital o electrónico, que sea conservado todo dato que permita determinar el origen, destino, fecha y hora del envío

y recepción, en concordancia con lo establecido en el Decreto Legislativo Nº 681 y sus normas complementarias.

Como puede observarse, Chile y Costa Rica hacen mención del concepto de documento electrónico. Ambos dan seguridad jurídica al reconocer como plenamente válido los actos y contratos celebrados por medios telemáticos y posibilitando que los medios electrónicos se presenten como medio de prueba en juicios si los documentos fueron suscritos mediante firma digital en el caso de Costa Rica y en el caso de Chile se requiere que sea firma electrónica avanzada.

Ecuador se refiere al término de mensajes de datos, pero también indica en otro artículo que los contratos electrónicos pueden ser instrumentados por medio de mensajes de datos.

México se refiere a la información contenida en el mensaje de datos, y le da validez jurídica siempre y cuando la información contenida en el mensaje de datos pueda ser mantenida íntegra y accesible para una consulta a posteriori.

Perú indica que los mensajes y documentos firmados electrónicamente pueden ser admitidos como prueba en toda clase de procesos o procedimientos.

Los cinco países tienen incorporadas en sus legislaciones la indicación de la validez de los contratos realizados electrónicamente, sin embargo todos ellos lo indican de manera diferente: unos se refiere al mensaje de datos, otros a la información contenida en el mensaje de datos, otros utilizan propiamente el término de documento electrónico y sólo Chile establece expresamente la validez de la contratación electrónica instrumentada en mensajes de datos.

Por otra parte, en relación a la prueba de la existencia de dichos contratos, las legislaciones de estos países se refieren a la conservación del mensaje de datos.

A diferencia de Chile, que tiene incorporado en su propia definición de Documento Electrónico el deber de estar almacenado en medios electrónicos que permitan su uso posterior.

Colombia, Ecuador y Perú siguen la norma de la ley Modelo sobre comercio electrónico de la CNUDMI, incorporando algunas condiciones adicionales como el de la integridad del mensaje en el caso de Ecuador.

En el caso de México cuando se exija que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos si se garantiza la integridad de la información y su posibilidad de accederla posteriormente. Las legislaciones de Colombia, Ecuador, México y Perú definen el concepto de Mensaje de Datos íntegro, no así Chile y Costa Rica.

Costa Rica expresa que la conservación del documento electrónica será satisfecha si se garantiza su inalterabilidad, su acceso o consulta posterior y se preserve la información relativa a su origen y otras características básicas.

6.2.1.3 Aciertos

Se considera como un acierto la indicación expresa de la validez de un documento electrónico y su fuerza probatoria sean establecidas con el hecho de que esté firmado electrónicamente y la posibilidad de garantizar su inalterabilidad y su acceso posterior, como lo ha hecho Costa Rica y Chile.

Chile incluso establece que el documento debe tener una firma electrónica avanzada para que tenga validez probatoria en juicios, de lo contrario tendrán el valor probatorio que corresponda.

La integridad del documento está implícita en el hecho de contener una firma digital o electrónica que además vincula unívocamente al autor con el documento.

También todas expresan en sus normas lo relativo a la conservación del mensaje de datos o documento electrónico, con lo que la prueba de la existencia del contrato puede ser establecida en caso de que se requiera.

6.2.1.4 Vacíos

Del análisis realizado se encuentra que los principios de seguridad jurídica necesarios para garantizar contratos electrónicos de confianza se encuentran cubiertos en la legislación costarricense, también como complemento puede ver el anexo 2. Esto significa que Costa Rica le da validez jurídica a los contratos celebrados por Internet, por lo que no se identifica vacíos en relación con otorgar validez jurídica a estos contratos electrónicos.

6.2.1.5 Recomendación

Indica Menéndez (2005, p.178) que la contratación por vía Internet resulta perfectamente válida, y que la utilización de este medio de comunicación está permitida siempre y cuando las partes no hayan prohibido expresamente su uso.

Además, la validez de este tipo de contratos y del uso de este medio de comunicación viene corroborada por todo el conjunto de normas analizadas.

La seguridad jurídica de los documentos electrónicos está garantizada por la ley 8454 de Costa Rica y su reglamento, los cuales son muy completos y abarcadores, y da validez a la contratación electrónica.

6.2.2 Las cláusulas del contrato

De manera general, una compra y venta en Internet es un contrato en línea que toma la forma de un contrato de adhesión, definido como:

> "aquel cuyas cláusulas han sido establecidas unilateralmente por el proveedor a través de contratos previamente impresos o en formularios sin que el consumidor, para celebrarlo, haya discutido su contenido." (art. 2 Ley Orgánica de Defensa del Consumidor de Ecuador, 2000, p.3)

Los principales contratos que se dan en el comercio electrónico son los de adhesión (Menéndez, 2005), aquellos en los que el consumidor no puede modificar el texto del contrato. El texto del contrato está previamente definido y diseñado por el proveedor y el consumidor simplemente lo acepta con todas las condiciones establecidas en él o no lo acepta, no tiene posibilidades de proponer cambios en el texto.

Por tal razón, la normativa debe dirigirse a regular las condiciones generales de la contratación y la presencia de cláusulas abusivas con especial atención a la tutela del consumidor.

Menéndez distingue entre cláusulas abusivas y condiciones generales de contratación. Una cláusula es condición general cuando está predispuesta e incorporada a una pluralidad de contratos exclusivamente por una de las partes, y no tiene por qué ser necesariamente abusiva. Cláusula abusiva es la que en contra de las exigencias de la buena fe causa en detrimento del consumidor un desequilibrio importante e injustificado de las obligaciones contractuales y puede tener o no, el carácter de condición general, ya que puede darse en contratos particulares cuando no existe negociación individual de sus cláusulas, esto es, en contratos de adhesión particulares. Por ello en las condiciones generales de contratación la norma jurídica debe proteger los legítimos intereses de los consumidores y usuarios, pero también de cualquiera que contrate con una persona que utilice condiciones generales de contratación en su actividad negocial con terceros (Menéndez, 2005, p.285).

6.2.2.1 Disposiciones de Organismos Internacionales

La Directiva 1993/13/CEE, de 5 abril 1993 del Consejo, sobre las cláusulas abusivas en los contratos celebrados con consumidores, aproxima disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre las cláusulas abusivas en los contratos celebrados entre profesionales y consumidores. En su artículo 3, incisos 1 y 2 indica:

> "1. Las cláusulas contractuales que no se hayan negociado individualmente se considerarán abusivas si, pese a las exigencias de la buena fe, causan en detrimento del consumidor un desequilibrio importante entre los derechos y obligaciones de las partes que se derivan del contrato.
>
> 2. Se considerará que una cláusula no se ha negociado individualmente cuando haya sido redactada previamente y el consumidor no haya podido influir sobre su contenido, en particular en el caso de los contratos de adhesión." (Directiva 1993/13/CEE, 5-04-1993, p.3).

En el anexo de esta Directiva, se presenta una lista indicativa no exhaustiva de cláusulas que pueden considerarse abusivas.

El artículo 5 de la Directiva 97/7/CE del Parlamento Europeo y del Consejo del 20 de mayo de 1997, indica que a más tardar durante la ejecución del contrato debe facilitarse al consumidor, en forma escrita o en soporte duradero y accesible a él, la información sobre: condiciones y modalidades de resolución del contrato, dirección geográfica del establecimiento del proveedor, los servicios posventa y garantías comerciales.

En la sección sobre Información y publicidad se indicó la información que debe proporcionarse al consumidor antes de celebrar un contrato electrónico indicados en las Directivas 2000/31/CE.

6.2.2.2 Legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México, Perú.

El artículo 16 de la Ley 19.496 de Protección al Consumidor de Chile establece la nulidad de las cláusulas abusivas en los contratos de adhesión. El artículo 17 indica que los contratos de adhesión deben estar claramente legibles con un tamaño de letra no inferior a 2,5 milímetros y en idioma castellano. El consumidor puede pactar en otro idioma siempre que éste así lo acepte mediante su firma en documento escrito. Inmediato a su firma, el consumidor debe tener una copia fiel al original del contrato.

La ley 7472 de Costa Rica incluye un artículo 39 sobre cláusulas abusivas en contratos de adhesión, indica que la eficacia de las condiciones generales está sujeta al conocimiento efectivo de ellas por parte del adherente o a la posibilidad cierta de haberlas conocido mediante una diligencia ordinaria, e indica cuáles son cláusulas

abusivas y absolutamente nulas. Además el artículo 1023 del Código Civil declara como nulo las cláusulas que pidan la renuncia del comprador a los preceptos nacionales y lo remiten a leyes extranjeras.

El capítulo VII de esta Ley Orgánica de Defensa del Consumidor de Ecuador se refiere a todo lo relacionado a la protección contractual. Este capítulo establece que el contrato de adhesión debe ser claramente legible, con un tamaño de fuente no menor de 10 puntos según las normas informáticas internacionales, no debe contener remisiones a textos o documentos que no se faciliten al consumidor antes de la celebración de contrato y en idioma castellano. Además el proveedor debe entregar una copia fiel del contrato al consumidor. El artículo 43 de esta Ley establece las cláusulas que están prohibidas y por lo tanto nulas para efectos legales.

La Ley Federal de Protección al Consumidor de México establece en su Capítulo X lo relacionado con los contratos de adhesión. Indica que los contratos de adhesión celebrados en territorio nacional deben ser legibles y en idioma español. Establece que estos contratos no pueden implicar prestaciones desproporcionadas a cargo de los consumidores, obligaciones inequitativas o abusivas, o cualquier otra cláusula que viole la ley. También establece que la Secretaría, mediante normas oficiales mexicanas podrá sujetar contratos de adhesión a registro previo ante la Procuraduría cuando impliquen o puedan implicar prestaciones desproporcionadas a cargo de los consumidores, obligaciones inequitativas o abusivas, o altas probabilidades de incumplimiento.

El Decreto Legislativo 716 de Protección al Consumidor de Perú y el Decreto Legislativo 3466 de Colombia no establecen nada respecto a las cláusulas en contratos de adhesión.

6.2.2.3 Aciertos

La normativa de Chile, Ecuador y México expresamente indica que los contratos de adhesión deben ser legibles y en idioma castellano, y el deber del proveedor de entregar una copia fiel al consumidor.

La normativa de Ecuador indica que el contrato de adhesión no debe contener remisiones a textos o documentos que no se faciliten al consumidor. Esto es importante, porque en las compras por Internet, generalmente el contrato de adhesión está estipulado en varias páginas Web que deben ser aceptadas por el consumidor conforme avanza en la contratación, y en ocasiones remiten a otros textos a través de enlaces siempre y cuando el consumidor acepte revisar dichos textos.

La normativa de Protección al Consumidor de México y Ecuador contiene expresamente artículos relacionados con la contratación electrónica.

6.2.2.4 Vacíos

En la Ley 7472 de Costa Rica no contiene expresamente nada relacionado a la contratación electrónica.

La Ley 8454 no contiene nada sobre cláusulas abusivas.

El Estado no puede garantizar los derechos de los consumidores en las transacciones que traspasan las fronteras nacionales. Sólo podría recurrirse a lo que establece el artículo 1023 del Código Civil, que declara como nulo las cláusulas que pidan la renuncia del comprador a los preceptos nacionales y lo remiten a leyes extranjeras.

6.2.2.5 Recomendaciones

Recogiendo el análisis de esta y otras secciones, se identifica que las cláusulas más importantes que deben estar establecidos en el contrato de adhesión se encuentran:

- La identificación de las partes;
- la dirección geográfica (domicilio social) del establecimiento del proveedor de bienes o servicios;
- las obligaciones de las partes;

- características y precio del producto o servicio pactado;
- los gastos de entrega;
- las modalidades de pago,
- forma de entrega o ejecución,
- garantías,
- la cláusula de confidencialidad de datos personales, en la cual hay un compromiso de no utilizar los datos personales de los clientes para fines diferentes a los previsto inicialmente;
- la legislación aplicable, no hay que olvidar que se pueden realizar operaciones comerciales con personas físicas o morales de diversos países en los cuales la legislación a aplicar será distinta y el consumidor no conoce forzosamente;
- si existe la posibilidad de un arbitraje y la jurisdicción competente;
- procedimientos para reclamos o mecanismos efectivos de solución de disputas,
- mecanismos de comunicación rápida, fácil y efectiva con la empresa,
- servicios de atención a procedimientos legales;
- dirección del domicilio legal de la empresa y sus directivos

Se recomienda incorporar en la normativa de Protección al Consumidor la obligación del proveedor de incluir primero, el término de contratación electrónica; y segundo, todas las cláusulas anteriores en los contratos de adhesión realizados a través de medios electrónicos.

Además de indicar los requisitos de legibilidad e idioma, la entrega de copia fiel del contrato al consumidor, y la referencia de no permitir remisiones a textos que no se faciliten al consumidor.

6.2.3 Identificación de las partes

En el comercio tradicional, el consumidor compra en un local comercial con presencia física, el propio consumidor también se encuentra físicamente en el local; por lo tanto, se da por cierto las identidades de las partes involucradas. Si el consumidor desea adquirir un bien, sólo tiene que ir al local comercial, ver el producto que desea, revisarlo y si cumple todas las características que busca lo compra.

En el comercio electrónico, el consumidor sólo tiene de referencia la información que aparece en la pantalla, y el consumidor está obligado a confiar en la información y publicidad que se muestra en la página Web del proveedor, como lo indica Monge y Murillo (2000):

> "Los contratos electrónicos se basan en la confianza que se debe establecer en forma casi inmediata de que una parte se compromete a entregar una cosa o prestación a cambio de un precio acorde con lo pactado." (Monge y Murillo, 2000, p. 193).

Por el otro lado, igualmente sucede con el vendedor, que recibe una solicitud de un comprador a través de una fórmula de pedido, y debe confiar en la veracidad y existencia del comprador, así como su capacidad contractual.

La identificación de ambas partes debe quedar claramente establecido para posteriores reclamos de incumplimientos, o más aún, para establecer la capacidad contractual de ambas, como es el caso de la participación de los menores de edad o de incapacitados mentalmente en la contratación.

En algunas ocasiones la identificación del proveedor escapa de los controles creados al efecto, sin embargo, el principal problema se va a localizar al otro lado de la relación contractual, el correspondiente al destinatario del bien o servicio. De acuerdo con Menéndez (2005), los inconvenientes se refieren: al modo de identificar correctamente al consumidor, la forma de determinar sus condiciones personales y la manera de comprobar fehacientemente el lugar desde el cual formaliza la relación contractual.

6.2.3.1 Disposiciones de Organismos Internacionales

La Ley Modelo sobre Comercio Electrónico de la CNUDMI establece, en su artículo 13, la atribución de los mensajes utilizando el hecho de que el mensaje ha sido enviado por el propio iniciador, por una persona facultada para actuar en nombre del iniciador, o por un sistema de información programado por el iniciador o en su nombre que actúe automáticamente. Y el artículo 14 establece las condiciones para presumir cuándo un mensaje de datos ha sido enviado por el iniciador.

La identificación del proveedor es exigida en el artículo 5 de la Directiva 2000/31/CE, y en el artículo 4 de la Directiva 1997/7/CE del Parlamento Europeo y del Consejo. De esta forma, la persona física o jurídica que actúa en la red, ofreciendo sus productos o servicios al público en general, debe encontrarse perfectamente determinado.

El artículo 7 de la Convención de la Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales establece:

> "Requisitos de información
> Nada de lo dispuesto en la presente Convención afectará a la aplicación de norma jurídica alguna en virtud de la cual las partes deban revelar su identidad, la ubicación de su establecimiento u otros datos, ni eximirá de consecuencias jurídicas a una parte que haya hecho a este respecto declaraciones inexactas, incompletas o falsas." (Convención de las Naciones Unidas, 2005, p.5).

Por otro lado, se tiene todo lo relacionado a la firma digital o electrónica, que como se analizó en la sección correspondiente, es la que garantiza la autoría del remitente.

6.2.3.2 Legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México, Perú.

El artículo 3 de la Ley 19799 de Chile establece la validez de los contratos suscritos por firma electrónica. En este caso, la firma electrónica es la que asocia el mensaje con su autor, y es la manera para identificar las partes en una transacción contractual.

Los artículos 16 y 17 de la Ley 527 de Colombia establecen de manera semejante a la Ley Modelo sobre Comercio Electrónico, la atribución del mensaje de datos y la presunción de su origen.

El artículo 10 de la Ley 8454 de Costa Rica establece que el documento o comunicación firmada digitalmente establece la autoría del titular de la firma.

El artículo 10 de la Ley 67 de Ecuador establece la procedencia e identidad del mensaje de datos, indica que se entiende que el mensaje proviene de quien lo envía y autoriza a

quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica.

El artículo 90 y 90 bis del Decreto sobre firma electrónica del 29 de agosto del 2003 de México establecen de manera semejante a la Ley Modelo sobre Comercio Electrónico, la atribución del mensaje de datos y su presunción del origen.

El artículo 8 del Decreto 019-2002-JUS de Perú establece que un documento o mensaje de datos firmado electrónicamente con firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, se presume que fue enviado y firmado por su titular.

Como puede verse, Chile, Costa Rica, Ecuador y Perú establecen el requisito de que el mensaje o documento electrónico debe estar firmado digital o electrónicamente para establecer la autoría de él.

Colombia y México siguen la ley Modelo sobre Comercio Electrónico para atribuir el mensaje de datos a quien lo envió.

6.2.3.3 Aciertos

Chile, Costa Rica, Ecuador, Perú establece la identificación de las partes a partir de la firma digital o electrónica que contenga el mensaje o documento electrónico.

6.2.3.4 Vacíos

Volviendo al caso de una compra y venta en Internet, el consumidor solicita un pedido llenando una fórmula accesible desde la página Web del proveedor. Muchas fórmulas de pedido no requieren de la firma digital del consumidor, por lo tanto no hay garantía para el proveedor de la identidad del consumidor ni de su capacidad contractual. Igualmente ocurre a la inversa.

El conocimiento de las circunstancias personales del consumidor dependerá de la mayor o menor diligencia con la que el proveedor confeccione su hoja de pedido y de la honestidad con la que el interesado la rellene. En la práctica, lo normal es que la hoja de pedido exija los siguientes datos personales: nombre y apellidos, dirección, ciudad, país, código postal y dirección de correo electrónico. Además de otros que no son obligatorios darlos, como número de fax, teléfono, documento nacional de identidad.

Generalmente una venta por Internet no solicita al comprador la firma digital o electrónica, y da por un hecho la capacidad contractual del adherente. Y en relación al proveedor, el consumidor confía en la existencia real de éste. En el contrato de compra y venta establecido, no existiría la prueba de su identidad si no es exigido por las normas del país. Además, generalmente el contrato no contiene la firma digital del proveedor.

6.2.3.5 Recomendaciones

De acuerdo con Menéndez (2005), en las relaciones con consumidores, se requiere de un documento electrónico de identidad seguro que sirva de forma semejante al documento de identidad nacional, o al menos se exija el empleo para la conclusión del contrato de una firma electrónica con ciertas características que permita la perfecta identificación de aquellos sujetos dotados de capacidad contractual.

Menéndez (2005) indica que las características de este tipo de firma electrónica serían las siguientes:

- para su obtención se podría requerir la capacidad general para contratar (ser mayor de edad y no hallarse incapacitado).
- El coste de su obtención debería ser nulo o al menos de reducido valor.
- Poseer un carácter internacional.
- Se trataría de una firma electrónica avanzada reconocida que viene acompañada de un certificado reconocido mediante el cual se acredita fehacientemente que la clave pública corresponde con la identidad del titular de la firma.

En el caso del proveedor, las normas relativa a la protección al consumidor de los países analizados, no exigen expresamente la identificación del proveedor en la Información o Publicidad que realizan. Es necesario incluir, como una obligación del proveedor, que su identificación conste en el contrato de adhesión, y además que debe ser firmado electrónicamente para acreditar su identidad real en el contrato.

De acuerdo con el análisis realizado, se presentan las siguientes recomendaciones:

Incluir en la normativa de protección al consumidor la exigencia de que la información y publicidad realizada por Internet se incluya, como se dijo anteriormente, entre otras cosas, la identificación del proveedor, su dirección geográfica, su referencia en el registro mercantil, dirección del domicilio legal de la empresa y sus directivos, esto con el fin de que el consumidor pueda tener plenamente identificado al proveedor en casos de reclamos.

Además, el consumidor debe tener una forma fácil de verificar la veracidad y existencia real de un proveedor que realiza comercio a través de Internet, antes de establecer una compra y venta electrónica. Un ejemplo sería que exista un sitio oficial del Estado de donde pertenece el proveedor, en donde el consumidor pueda consultar fácilmente sobre la identidad y existencia de una empresa o proveedor que ofrece bienes o servicios a través de la página Web. Una especie de Registro Mercantil de comerciantes electrónicos o certificaciones de confianza otorgadas por organismos de consumidores que verifican la honorabilidad de los sitios, lo cual incluye la identificación exacta de los proveedores certificados (Burgos, 2003)

La firma digital o electrónica es la que vincula al firmante con el documento electrónico o mensaje de datos, además de que permite determinar su integridad. Por tal motivo, es importante incluir en los formularios de pedidos (o contratos electrónicos) las firmas digitales de ambas partes (proveedor y consumidor). Para protección del consumidor, es importante que el proveedor firme digitalmente el contrato electrónico.

Sería conveniente que para comprar por Internet se exija poseer una firma digital, y que para compras que exija cierta capacidad contractual u otros requisitos personales, sea necesario para realizarla utilizar firmas digitales certificadas o avanzadas. En estos casos, el otorgamiento de una firma digital certificada se requiera al menos la condición de mayoría de edad y de capacidad contractual, y éstas sean exigidas por la entidad certificadora.

Otra recomendación es que las empresas incluya la petición de la firma digital certificada para que un consumidor pueda acceder a ciertas páginas de contenidos no aptos, por ejemplo, a menores u otro tipo de población (incapaces).

Ciertamente, la exigencia de una firma digital al consumidor para poder comprar por Internet va a restringir el comercio, sin embargo, para protección del proveedor, este es el mecanismo que podría garantizar la identidad y capacidad contractual del consumidor. Y a la inversa, la firma digital por parte del proveedor en los contratos de adhesión, respalda al consumidor para ejercer cualquier acción legal en caso de controversias.

6.2.4 Tiempo, lugar de perfección del contrato

Un elemento determinante en relación a la contratación electrónica consiste en determinar cuándo y dónde el consentimiento de las partes se entiende formado, ya que generalmente será la formación del consentimiento de las partes lo que determinará el momento en que un contrato ha sido perfeccionado, de lo cual se producirán múltiples efectos jurídicos.

Determinar el momento en que se formó el consentimiento permite conocer el momento exacto en que:

> "i) los derechos y obligaciones que nacen de un contrato pueden ser ejercidos o demandados por la otra parte del contrato; ii) el oferente ya no podrá retractarse de su oferta; y iii) se inicia el plazo de prescripción o caducidad de las acciones que correspondan." (Magliona, 2001, p.4).

En relación con el lugar de perfección del contrato, esto es importante para establecer el tribunal competente de conocer las controversias que se deriven de la aplicación de dicho contrato y la legislación aplicable al mismo, siempre que en el texto del contrato no se establezca la legislación aplicable expresamente.

El contrato queda concluido desde el momento en que hay coincidencia de voluntades y se perfecciona con la simultaneidad de las declaraciones de voluntad. En el caso de una transacción electrónica, cuándo ocurre esta simultaneidad de las declaraciones de voluntades? La Ley Modelo sobre Comercio Electrónico establece normas que pueden facilitar la determinación del lugar y momento de formación del consentimiento.

Es decir, el consentimiento se forma con la existencia de una oferta y su aceptación. Para que un pedido electrónico sea considerado como válido es necesario el consentimiento de las partes y el contrato electrónico, ambos elementos podrán servir de prueba para demostrar la existencia y las condiciones de la transacción en caso de conflicto.

Se puede ver que existe una similitud entre la compra en un sitio Web y la compra en una tienda física: El consumidor luego de decidir comprar, lo paga mediante su tarjeta de crédito.

6.2.4.1 Disposiciones de Organismos Internacionales

El artículo 2 de la Directiva 97/7/CE del Parlamento Europeo y del Consejo del 20 de mayo de 1997 define:

> "1) «contrato a distancia»: todo contrato entre un proveedor y un consumidor sobre bienes o servicios celebrado en el marco de un sistema de ventas o de prestación de servicios a distancia organizado por el proveedor que, para dicho contrato, utiliza exclusivamente una o más técnicas de comunicación a distancia hasta la celebración del contrato, incluida la celebración del propio contrato;" (Directiva 97/7/CE del Parlamento Europeo y del Consejo, 1997, p.4)
>
> "4) «técnica de comunicación a distancia»: todo medio que permita la celebración del contrato entre un consumidor y un proveedor sin presencia física simultánea del proveedor y del consumidor. En el Anexo I figura una lista indicativa de las técnicas contempladas en la presente Directiva;" (Directiva 97/7/CE del Parlamento Europeo y del Consejo, 1997, p.4)

Indica el Anexo I de esta Directiva, que las técnicas de comunicación a distancia son las siguientes: Impreso sin destinatario, Impreso con destinatario, Carta normalizada, Publicidad en prensa con cupón de pedido, Catálogo, Teléfono con intervención humana, Teléfono sin intervención humana (llamadas automáticas, audiotexto), Radio, Visiófono (teléfono con imagen), Videotexto (microordenador, pantalla de televisión) con teclado o pantalla táctil, Correo electrónico, Fax (telecopia), Televisión (compras y ventas a distancia).

Se deriva de esta Directiva que una compra realizada por medio de la página Web es una compra a distancia, esto es así para la protección al consumidor, aunque en la lista de los medios de comunicación a distancia no aparezca expresamente el de Internet.

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo, indica en su artículo 11 sobre la realización de un pedido, que el prestador de servicios debe acusar el recibo del pedido sin demora y por vía electrónica, y se considera que se ha recibido el pedido y el acuse de recibo cuando las partes a las que se dirigen puedan tener acceso a los mismos. Es en este momento en que se considerará perfeccionado el contrato.

Respecto al momento en que debe entenderse que un mensaje de datos fue enviado, la Ley Modelo sobre Comercio Electrónico de la CNUDMI señala en su artículo 15 que:

> "1) de no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos a nombre del iniciador". (CNUDMI, 1999, p.18)

Respecto al momento de la recepción de mensaje de datos, el mismo artículo 15 señala que:

> "2) de no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue: a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar: i) En el momento en que entre el mensaje de datos en el sistema de información designado; o ii) De enviarse el mensaje de datos a un sistema de información destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos; b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar al entrar el mensaje de datos a un sistema de información del destinatario". (CNUDMI, 1999, p.18).

Con respecto al lugar, la Ley Modelo, artículo 15 señala que:

> "4) 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 párrafo: a) Si el iniciador o el 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 tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual". (CNUDMI, 1999, p.18).

La Ley Modelo no dice el lugar y el momento en que debe entenderse perfeccionado el consentimiento, a fin de no interferir con el derecho interno de cada país en esta materia, pero si da normas que pueden facilitar la determinación del lugar y momento de formación del consentimiento por cada derecho interno, como el expuesto del artículo 15.

6.2.4.2 Legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México, Perú.

El artículo 12 A de la Ley 19496 de protección al consumidor de Chile establece que el consentimiento no se entenderá formado si el consumidor no ha tenido previamente acceso claro, comprensible e inequívoco de las condiciones generales del contrato celebrado por medios electrónicos, y la posibilidad de almacenarlos o imprimirlos. Se requiere que el consumidor acepte en forma inequívoca las condiciones ofrecidas por el proveedor. Una vez perfeccionado el contrato, el proveedor debe enviar confirmación escrita del mismo que puede ser por medio electrónico. La confirmación debe contener una copia íntegra, clara y legible del contrato.

Los artículos 23, 24 y 25 de la Ley 527 de Colombia establecen de manera semejante a la Ley Modelo sobre Comercio Electrónico, lo relacionado al tiempo y lugar de envío y recepción del mensaje de datos.

El artículo 14 indica que la formación de contratos, la oferta y aceptación pueden ser expresadas por medio de mensajes de datos.

El Código de Comercio costarricense, la Ley 7472 de promoción de la Competencia y Defensa Efectiva del Consumidor no contemplan expresamente la compra y venta realizada por medio de Internet.

Sin embargo, el Código Civil de Costa Rica indica:

> **"ARTÍCULO 1012.-** Si las partes no estuvieren reunidas, la aceptación debe hacerse dentro del plazo fijado por el proponente para este objeto. Si no se ha fijado plazo, se tendrá por no aceptada la propuesta, si la otra parte no respondiere dentro de tres días cuando se halle en la misma provincia; dentro de diez, cuando no se hallare en la misma provincia, pero sí en la República; y dentro de sesenta días, cuando se hallare fuera de la República.
>
> **ARTÍCULO 1013.-** El proponente está obligado a mantener su propuesta, mientras no reciba respuesta de la otra parte en los términos fijados en el artículo anterior." (Ley 63 Código Civil de Costa Rica, 1887, p.107).

Esto indica que el contrato no queda perfeccionado si no hay respuesta de aceptación por parte del consumidor, y define ciertos plazos para que éste responda.

La Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos es la que reconoce la validez jurídica de los documentos electrónicos y su equivalencia funcional con los documentos en medios físicos (artículos 3 y 4), sin embargo no establece, para los casos de contratos electrónicos, el momento y lugar de perfección del contrato.

El artículo 442 del Código de Comercio de Costa Rica establece que cuando se trata de viva voz, ya sea reunidas o por teléfono, el contrato de compra y venta se perfecciona desde que se convenga en cosa y precio.

El artículo 443 establece que si la compra y venta se negocia por correspondencia, se siguen las siguientes reglas:

> "a) Si el proponente fija un término de espera, estará obligado a mantener su oferta hasta ese día; y
> b) Si no fija fecha de espera, estará obligado a mantener su oferta cinco días, si se trata de la misma plaza; si se trata de otra plaza dentro del territorio nacional, diez días; y si es en el exterior, un mes. Estos términos se contarán desde el día en que el proponente deposite la oferta en las oficinas de correos." (Código de Comercio de Costa Rica, 1964, p. 74).

El artículo 444 indica:

> "El contrato quedará perfecto desde el momento en que, dentro de los términos indicados en el artículo anterior, el proponente reciba comunicación de la otra parte aceptando pura y simplemente. Si la contestación contuviere algunas modificaciones o condiciones, el contrato no se perfeccionará hasta tanto el proponente original no acepte los cambios y así lo haga saber. Esa contestación, por su parte, producirá el perfeccionamiento del contrato, cuando llegue a poder del posible comprador." (Código de Comercio de Costa Rica, 1964, p.74).

Estos artículos indican, sobre la compra y venta por correspondencia, que el contrato quedará perfecto si el proponente recibe la aceptación del consumidor y el consumidor reciba del proponente también su aceptación. Esto podría aplicarse para la compra y venta por Internet, definiéndose lo relacionado con la recepción de la aceptación por ambas partes.

Por otro lado, se presentó el Proyecto de Ley de Comercio Electrónico, expediente 16081, que pasó a estudio de la Comisión Permanente de Asuntos Jurídicos el 6 de diciembre de 2005, en este proyecto se establece que:

> "Artículo 5º—Formalización. Se entenderá por contrato formalizado por vía electrónica el celebrado sin la presencia simultánea de las partes, prestando su consentimiento en origen y en destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, conectados por medio de cable, radio o medios ópticos o electromagnéticos.
> El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes civiles y comerciales y se tendrá como lugar de perfeccionamiento el que acordaren las partes, en su defecto el domicilio de quien recibió el servicio." (Proyecto de Ley de Comercio Electrónico de Costa Rica, 2005, p.3).
>
> "Artículo 6º—Consentimiento. La validez del consentimiento del contrato electrónico estará sujeta a la existencia de mecanismos tecnológicos que indubitablemente tengan tal finalidad. La recepción, confirmación de recepción o apertura de mensajes de datos o telecomunicaciones en general, salvo acuerdo previo en contrario, se considerarán como propuestas o tratativas y no implican aceptación del contrato electrónico." (Proyecto de Ley de Comercio Electrónico de Costa Rica, 2005, p.3).

Este proyecto establece que el lugar de perfeccionamiento del contrato será el que acuerden las partes, en su defecto el domicilio de quien recibió el servicio.

Además el proyecto agrega que la apertura de mensajes de datos en general, se considerará como propuestas o tratativas y no implican aceptación del contrato electrónico.

El artículo 11 de la Ley 67 de Ecuador establece el momento y lugar de envío y recepción del mensaje de datos de manera similar a la Ley Modelo.

Por otro lado, el artículo 46 indica que el perfeccionamiento del contrato electrónico se someterá a los requisitos y solemnidades previstos en las leyes, y que el lugar de perfección es el que acuerden las partes. Además indica que la recepción, confirmación de recepción, o apertura del mensaje de datos no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

El artículo 93 de la Reforma al Código de Comercio en materia de Firma Electrónica de México, del 29 de agosto del 2003, indica que los actos o contratos pueden ser establecidos por medio de mensajes de datos, los artículos 91 y 91 bis establece el momento de recepción de un mensaje de datos; el artículo 92 sobre el acuse de recibo y el artículo 94 establece el lugar de emisión y recepción del mensaje de datos; todos éstos de manera similar a la Ley Modelo de Comercio Electrónico.

Por otro lado, la Ley Federal de Protección al Consumidor de México, en su artículo 51 define la venta a domicilio, mediata o indirecta, como aquella que se proponga o lleve a cabo fuera del local o establecimiento del proveedor; el artículo 53 establece que el proveedor que realice este tipo de ventas, donde no es posible el trato directo con el comprador, debe permitir al consumidor hacer reclamaciones y devoluciones por medios similares a los utilizados para la venta; y en su artículo 56 indica que el contrato se perfeccionará a los cinco días hábiles contados a partir de la entrega del bien o de la firma del contrato, lo último que suceda.

Podría incluirse aquí que la venta realizada por Internet es una venta que cae dentro del tipo establecido en el artículo 51, y por lo tanto se perfeccionará cinco días hábiles después de entregado el bien o firmado el contrato (lo último que suceda).

La Ley 27.291 de Perú modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de la voluntad y la utilización de la firma electrónica. Establece en su artículo 1 la modificación al artículo 1374 del

Código Civil indicando que en una contratación por medios electrónicos, se presume la recepción de la declaración contractual (oferta, revocación o aceptación) cuando el remitente reciba el acuse de recibo.

6.2.4.3 Aciertos

Se considera como acierto la inclusión en la normativa peruana de normas que permita establecer el momento en que se perfecciona un contrato electrónico: con la recepción por parte del consumidor del acuse de recibo de su declaración contractual. Perú establece estas normas en una norma aparte que modifica su Código Civil.

También la norma chilena en la que se indica que el proveedor debe enviar una copia íntegra del contrato al consumidor. Esta norma está dentro de la Ley 19496 de Protección al Consumidor.

Se resalta la norma Ecuatoriana que establece que el lugar de perfección es el que acuerden las partes, y que la recepción, confirmación de recepción, o apertura del mensaje de datos no implica aceptación del contrato electrónico, salvo acuerdo de las partes. Esta norma se encuentra en la Ley 67 de Comercio Electrónico, firmas y mensajes de datos.

Colombia y México establecen el tiempo y lugar de envío y recepción de mensajes de datos semejante a las normas de la Ley Modelo sobre Comercio Electrónico, e indican que los contratos pueden ser establecidos por medio de estos mensajes. Por lo tanto, tienen una guía bien detallada para determinar el tiempo y lugar de perfección del contrato. Colombia incluye estas normas en la Ley 527 que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones; y México incluye estas normas en una reforma al Código de Comercio.

6.2.4.4 Vacíos

El Código de Comercio y la Ley 7472 costarricense no contemplan la compra y venta realizada por medio de Internet, por lo tanto no establece el tiempo y lugar de perfección de un contrato realizado por este medio.

La Ley 8454 establece la validez de los documentos electrónicos pero no indica nada al respeto de cuándo y dónde se considera la perfección de un contrato realizado por medios electrónicos.

Podría establecerse que la perfección del contrato es de acuerdo con el artículo 444 del Código de Comercio, considerando la compra y venta por Internet como una compra por correspondencia, y por lo tanto la perfección se da cuando el proponente reciba comunicación de la otra parte aceptando pura y simplemente, y el consumidor reciba la aceptación por parte del proponente devuelta.

El proyecto de Ley de Comercio Electrónico, expediente 16081, remite al código civil y comercial en lo referente al momento de perfeccionamiento del contrato electrónico, e indica que el lugar de perfección es el que acuerden las partes, en su defecto el del domicilio del consumidor. Y que la validez del consentimiento del contrato electrónico depende de la existencia de mecanismos tecnológicos que lo puedan probar.

Puede observarse que el proyecto de Ley tampoco resuelve de forma explícita y simple el problema del tiempo de perfección del contrato.

6.2.4.5 Recomendaciones

La tendencia hacia sistemas de comunicación cada vez más instantáneos, hacen posible que se consideren las contrataciones electrónicas como contrataciones celebradas entre presentes, pues la velocidad de las comunicaciones hacen desaparecer el tiempo y la distancia, y por lo tanto es posible considerar que la aceptación de la oferta llega inmediatamente a conocimiento del oferente, lo que perfecciona el contrato.

Cuando se emplee una tecnología que permita la comunicación instantánea de las partes (videoconferencia o sistemas similares), la contratación se producirá de manera instantánea o interactiva, y estaría ante un caso muy similar a la contratación telefónica (en la que existe distancia física entre las partes, pero no existe distancia temporal), por lo que cabría admitir la aplicación a aquellos contratos de las reglas que gobiernan la contratación entre presentes.

El uso de la comunicación telefónica, el módem y el computador como elementos técnicos permite la comunicación instantánea. Para estos casos, el artículo 442 del Código de Comercio de Costa Rica determina que cuando las partes traten por teléfono se está en presencia de un contrato entre presentes:

> **"ARTÍCULO 442.-** Cuando las partes traten de viva voz, ya sea reunidas o por teléfono, el contrato de compra-venta que de ahí resulte quedará perfecto desde que se convenga en cosa y precio, y demás circunstancias de la negociación." (Código Comercio de Costa Rica, 1964, p.79).

Aunque una compra-venta por Internet no es exactamente un trato que se realiza a viva voz (como una hecha por teléfono), posee la característica de una comunicación instantánea (la velocidad de la comunicación es tan alta que casi no se percibe un tiempo de espera por respuesta).

Sin embargo, esta consideración depende de aspectos puramente tecnológicos. De acuerdo con Guisado (2004), a pesar de la tendencia del desarrollo de las comunicaciones, la mayoría de los contratos electrónicos que se celebran en Internet son contratos a distancia y no instantáneos, pese a la rapidez que pueden proporcionar los contextos virtuales. Esto es debido a que los equipos y sistemas tecnológicos que habitualmente se emplean en Internet son incapaces de proporcionar a los contratantes el mismo grado de inmediatez que éstos alcanzan en la contratación oral (física o telefónica). Esto es congruente también con lo establecido en el artículo 2 de la Directiva 97/7/CE.

Indica Guisado (2004) que puede haber excepciones cuando se proporcione a las partes una comunicación instantánea, en cuyo caso se equipararía con la contratación entre presentes.

Por lo tanto, la aceptación del contrato se hace pulsando el botón aceptar de la página de Internet, por parte del consumidor; inmediatamente después el consumidor recibe la confirmación del proveedor, generalmente a través de un mensaje por correo electrónico, concluyendo la formación del contrato. El requisito de que ambas partes tengan conocimiento de la aceptación es congruente con el artículo 11 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo.

También Álvarez y otros (2005) indican que en "los contratos electrónicos, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, en la Ley Modelo para el Comercio Electrónico y el derecho comparado, en general, aceptan pacíficamente que el contrato queda perfeccionado en el momento en que la aceptación ingresa al sistema informático del oferente. No es necesario que el oferente tenga conocimiento de la aceptación. Basta que ingrese a su esfera de control. Se establece además, la obligación a cargo del oferente de emitir un "acuse de recibo" de la aceptación para dar seguridad a las transacciones comerciales."

Por otro lado, menciona Vega (2005) que la LSSICE (Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, España) establece en su artículo 29,1, que en el caso de una contratación electrónica celebrada con un consumidor, se presumirá celebrado en el lugar en que éste tenga su residencia habitual.

En cuanto al lugar de perfección, para protección del consumidor, se recomienda que el lugar de perfección sea el de residencia de éste, como lo establece la LSSICE.

Recogiendo el análisis realizado se recomienda incluir en una sola normativa, que puede ser la de Promoción de la Competencia y Protección efectiva del Consumidor,

una sección relacionada con la contratación electrónica que incluya los siguientes elementos:

-Indicación de que la recepción, por parte del consumidor, del acuse de recibo de su declaración contractual y del texto del propio contrato, perfecciona el contrato.
-Indicar que el lugar de perfeccionamiento del contrato sea, salvo acuerdo de las partes, el lugar de residencia del consumidor, para su mejor protección.
-Indicar que la recepción, confirmación de recepción, o apertura del mensaje de datos no implica aceptación del contrato electrónico, salvo acuerdo de las partes.
-Indicar claramente el momento y lugar de envío o recepción del documento electrónico de acuerdo con lo establecido en el artículo 15 de la ley Modelo sobre Comercio Electrónico.
-Exigir que las compras y ventas que requieran capacidad contractual se realice con respaldo de firma digital o electrónica certificada de ambas partes.

Incluir en el Código de Comercio lo relacionado con la compra y venta por medios electrónicos, indicando que la perfección del contrato se da en el momento en que el proponente recibe la aceptación del consumidor y éste reciba también la aceptación del proponente junto con el documento electrónico firmado por ambas partes.

También explicitar en el Proyecto de Ley de Comercio Electrónico, expediente 16081, el tiempo y lugar de perfección del contrato electrónico como se indicó anteriormente, y no remitir a los códigos Civil y Comercial, porque éstos tampoco establece de manera explícita lo relacionado al perfeccionamiento en contratos electrónicos para compra y ventas por Internet.

6.2.5 Aspectos relacionados con el pago

Con relación al pago de una compra y venta realizada por Internet, se considera que el sistema tecnológico utilizado, ya sea tarjeta de crédito, monedero o dinero electrónico, provee los mecanismos de seguridad necesarios para realizar la transacción con toda

confianza. Se analiza en esta sección lo relacionado con el uso indebido del medio de pago por un tercero, específicamente se considerará el uso de tarjetas de crédito, por ser el medio más utilizado en las compras electrónicas realizadas por los consumidores (Menéndez, 2005).

En relación con el pago, la mayoría se realiza a través del uso de tarjetas de crédito o débito, como también lo indica Carvajal y Jiménez (2002):

> "Sobre la forma de pago, este es generalizado mediante el uso de tarjetas de crédito o débito, por lo que los oferentes obvian la necesidad de mostrarla ya que por costumbre y por idoneidad es la única forma de pago en Internet" (Carvajal y Jiménez, 2002, p.212).

La desconfianza del consumidor sobre los aspectos relacionados con la seguridad en los pagos, el reembolso de pagos efectuados son asuntos que limitan el crecimiento del comercio electrónico. La posibilidad de revocar los pagos realizados por vía electrónica es indudablemente uno de los elementos que aumentarían la confianza de los consumidores en el comercio electrónico, además de la confianza de la existencia real del proveedor, y de que no usarán indebidamente su tarjeta de pago.

En las estadísticas de la Red Internacional de Protección al Consumidor y Aplicación de la Ley indicado eConsumer.gov (2005), se observa que de la quejas presentadas por los consumidores con relación a los pagos, el 36% se realizaron por medio de tarjeta de crédito y corresponde al porcentaje más alto con relación a las otras formas de pago (estadísticas del 1 de enero al 31 de diciembre del 2005).

6.2.5.1 Disposiciones de Organismos Internacionales

El artículo 8 de la Directiva 97/7/CE del Parlamento Europeo y del Consejo establece que los Estados miembros deben velar por que existan medidas apropiadas para que el consumidor pueda anular una pago en caso de uso fraudulento de su tarjeta de pago en contratos a distancia, y en este mismo caso, tiene derecho a que se le restituya, por parte de la entidad, las sumas cobradas ilícitamente.

Por supuesto, al titular de la tarjeta se le exige el deber de diligencia en caso de extravío o pérdida de la tarjeta, esto es, el deber de poner en conocimiento a la entidad emisora sobre el extravío.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, sobre privacidad y comunicaciones electrónicas, establece en su artículo 4 que:

> "el proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de comunicaciones por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente." (Directiva 2002/58/CE, 2002, p.7).

En el caso de que exista algún riesgo de violación de la seguridad, el proveedor así debe informarlo a los abonados.

El artículo 5 de esta misma directiva recuerda, como principio de base, que los Estados miembros deben garantizar, a través de la legislación nacional, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de comunicaciones electrónicas. En particular, han de prohibir que personas distintas de los usuarios escuchen, intercepten o almacenen comunicaciones sin el consentimiento de los usuarios.

6.2.5.2 Legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México, Perú.

El artículo 76 bis de la Ley Federal de Protección al Consumidor de México establece que en transacciones realizadas por medios electrónicos, el proveedor debe utilizar alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor y le informará sobre las características de dichos elementos.

Las legislaciones de protección al consumidor de los 6 países no contemplan nada respecto a la posibilidad de anular un pago en caso de uso fraudulento de su tarjeta de tarjeta de crédito en contratos electrónico.

6.2.5.3 Aciertos

Las Directivas Europeas 97/7/CE y la 2002/58/CE establecen el deber de los Estados miembros de velar por que existen medidas adecuadas para anular un pago en caso de uso fraudulento de su tarjeta de crédito, así como la garantía y la seguridad de los datos en una comunicación electrónica.

6.2.5.4 Vacíos

La Ley costarricense no tiene establecido la protección del consumidor en el caso de uso fraudulento de su tarjeta de crédito. Es responsabilidad del consumidor resguardar la seguridad de su uso. En caso de pagos de compras por Internet, no hay manera de que el consumidor anule un pago si ya ha consentido el pago con su tarjeta y digitado la información de ella en la página Web del proveedor o si un tercero usó de manera fraudulenta su tarjeta de crédito. El consumidor puede recurrir al sistema judicial planteando su denuncia de uso indebido o robo de su tarjeta de crédito. Pero por parte de la empresa comercial, no hay ninguna posibilidad de devolución del dinero al consumidor.

Las instituciones financieras que proveen el servicio de tarjeta de crédito, lo más que han ofrecido es la póliza contra robo de la tarjeta, en la que asegura al consumidor que la entidad aseguradora se hará cargo de la pérdida que sufra el consumidor en caso de robo de su tarjeta y así se demuestre. Es deber del consumidor dar aviso inmediato del robo de la tarjeta.

No existe una obligación del proveedor de proveer seguridad en la transacción electrónica, que incluya mecanismos de protección de la información que se transmite a través de la Red, así como seguridad en el pago por medio de tarjetas de crédito.

Por otro lado, el Estado debe ofrecer al consumidor un medio fácil y ágil de consulta de la existencia real de una empresa con presencia en Internet. Esto con el fin de proteger al consumidor previniéndolo de realizar una transacción con una empresa falsa o inexistente.

6.2.5.5 Recomendaciones

Indica Suárez (2001, p. 122), citado por Vega (2005, p. 301), “la seguridad en el comercio es una de las cuestiones que más preocupa al consumidor”, y entre ellas la del medio de pago. “El éxito del comercio electrónico pasa, pues, por la adopción de medios técnicos y normas jurídicas que tiendan a garantizar la seguridad del tráfico” (Gourion y Ruano, 2003, p.85) citado por Vega (2005, p. 301).

De acuerdo con Vega (2005), a nivel legal no existe una regulación que de forma general acometa los problemas y soluciones por los conflictos que en la práctica se vienen produciendo por la utilización de las tarjetas.

Además indica que, cuando el pago con tarjeta se produce de forma directa o a través de la red (lo que suele denominarse pago *on line*) se impone la necesidad de adoptar ciertas medidas para garantizar la seguridad de la operación, tanto en lo que se refiere al propio proveedor pero especialmente al consumidor.

El proveedor deberá mirar la efectividad e integridad del pago así como una identificación segura del sujeto que lo realiza para evitar utilizaciones fraudulentas de dichas tarjetas, en tanto que el consumidor deberá velar porque dicho pago quede perfectamente reflejado bajo su identidad, con total confidencialidad y en lo que afecta al medio probatorio.

Vega (2005) indica que la solución se arbitra mediante sistemas técnicos consistentes en criptosistemas de clave pública y protocolos comunes, que amplían y modifican los tradicionales sistemas de registro de datos en las operaciones con las distintas tarjetas bancarias o financieras.

El sistema de pago a través de redes de comunicación requiere métodos seguros, para poder dar confianza a los consumidores. Existen distintos mecanismos utilizados por las entidades financieras privadas tendiente a garantizar la seguridad, confidencialidad y efectividad del pago con tarjeta, entre los que se encuentran: los protocolos *Secure Sokets Layes* (SSL) y *Secure Electronic Transaction* (SET).

Concluye Vega (2005) que la seguridad nunca podrá ser absoluta, y que se están detectando fallos en a práctica. Indica que se requiere de una regulación específica para el uso de tarjetas como medio de pago electrónico, sobre todo de cara a determinar las responsabilidades de los prestadores de servicios de la sociedad de la información en los mecanismos de pago electrónico.

Del análisis realizado, y con el fin de dar mayor seguridad a los consumidores, se presentan las siguientes recomendaciones.

El Estado debe tener un sitio oficial con la lista de empresas autorizadas y con presencia en Internet (para el caso de empresas nacionales), en el caso de empresas extranjeras, debe haber un mecanismo similar en el Estado donde radica esa empresa; es decir, es necesario ofrecer al consumidor una especie de directorio de empresas con presencia en Internet, claramente identificados y ubicados (en espacio físico y geográfico).

En el mismo sentido, el Estado debe coordinar a nivel internacional para obtener una lista de las personas físicas y jurídicas debidamente identificadas, de otros países que venden por Internet con operaciones en Costa Rica, y ofrecer esta lista en una página oficial del Estado. O tener un sitio Oficial del Estado, y con un mecanismo fácil, en donde el consumidor pueda consultar por la existencia real de una empresa que vende por Internet.

Mejor aún, debe haber un organismo de ámbito internacional donde tenga el control de todas las empresas con presencia en Internet. Esto pareciera limitar el comercio

electrónico, pero para protección del consumidor se debe buscar el mecanismo para que éste no sea presa fácil de acciones fraudulentas por parte de proveedores inescrupulosos.

Se debe exigir a los proveedores que incluyan mecanismos de transmisión de datos que garanticen la seguridad en las transacciones electrónicas, por ejemplo, exigir al proveedor la utilización de servidores y mecanismos seguros para realizar las transacciones de comercio electrónicas, confirmar las órdenes de compra por e-mail o por teléfono cuando son por grandes cantidades de dinero.

También es conveniente incluir la obligación de los proveedores de establecer cláusulas de protección al consumidor en los contratos de adhesión, que garanticen que el proveedor se hará responsable de las pérdidas que sufra el consumidor por violación de la seguridad de los datos durante la transmisión en la Red.

Las medidas de seguridad en el pago las debe tomar propiamente el consumidor realizando al menos las siguientes comprobaciones o tomar las siguientes precauciones:

- Verificar la existencia real del proveedor a través de listas oficiales dado por el Estado de las empresas vigentes y activas o por otros medios.
- Comprar sólo en sitios de reconocido prestigio.
- Comprobar que el sitio utiliza medios seguros para realizar las transacciones electrónicas.
- Utilizar dinero electrónico justo en la cantidad necesaria.
- Revisar los términos del contrato electrónico y comprobar que las cláusulas no viole sus derechos y tenga establecido que la legislación aplicable y jurisdicción competente sea la de su propio país para su mejor protección.

Por lo tanto, en el caso de Costa Rica donde es deber del Estado la educación del consumidor, se recomienda crear estos programas o, si existen, incorporar en los

programas de información, divulgación, capacitación y educación al consumidor, el tema de “comercio electrónico seguro”.

6.3 Protección del consumidor después de haber realizado la compra

Una compra en el que el consumidor está satisfecho, no sería necesario recurrir a este momento. Pero si al contrario quiere devolver el bien o el servicio o existe un defecto de los mismos, ¿qué posibilidades tiene con respaldo a sus derechos y las obligaciones del vendedor?, y por otro lado, ¿cuál es la legislación aplicable y la jurisdicción competente?

Cuando el comprador da su aceptación, el comerciante confirma el pedido por escrito. En esta confirmación la identificación y referencias del comerciante deben quedar en el documento electrónico, como también las características esenciales del bien o servicio, el precio, los costos de envío, los servicios de garantía, y toda la información que se indicó en la sección sobre Las Cláusulas del Contrato.

El análisis se hará desde la problemática de los siguientes aspectos:

- Resolución del contrato
- Reclamos, legislación aplicable y jurisdicción competente.

6.3.1 Resolución del contrato

En una compra y venta en Internet se puede distinguir entre productos y servicios tangible o no tangible.

Entre los productos y servicios tangibles están: libros, CDROM, DVD, juguetes, ropa; y entre los no tangibles: programas de computación, libros electrónicos, información contenida en bases de datos, música, películas, videojuegos.

La compra de productos no tangibles es instantánea, en cambio la compra de productos tangibles no lo es, pues requiere de un período de tiempo entre el momento del pedido y la entrega. En este último caso, un pedido por Internet es similar a un pedido realizado por teléfono, y el contrato de compra venta se ejecuta sin ninguna diferencia. En cambio la compra de un producto no tangible, la entrega es instantánea y se realiza a través de la Red, en este caso, se debe tomar en cuenta algunos aspectos de protección del consumidor, como es la ausencia del plazo de reflexión del consumidor, pues la venta del bien o servicio se ejecuta de inmediato.

En cualquier caso, las normativas de protección al consumidor debe considerar la posibilidad de la resolución del contrato sin responsabilidad del consumidor por un período establecido.

6.3.1.1 Disposiciones de Organismos Internacionales

La Directiva 97/7/CE del Parlamento Europeo y del Consejo, en su artículo 6 establece el derecho a la resolución del contrato celebrado a distancia por parte del consumidor, hasta 7 días laborables después de haber recibido el bien o servicio sin necesidad de justificar y sin penalización, sólo el costo de devolución.

La Directiva establece los casos en que no es posible ejercer el derecho de resolución: a) prestación de servicios cuya ejecución haya comenzado, con el acuerdo del consumidor, antes de finalizar el plazo de siete días laborables; b) suministro de bienes o servicios cuyo precio esté sujeto a fluctuaciones de coeficientes del mercado financiero que el proveedor no pueda controlar; c) suministro de bienes confeccionados conforme a las especificaciones del consumidor o claramente personalizados, o que, su naturaleza, no puedan ser devueltos o puedan deteriorarse o caducar con rapidez; d) suministro de grabaciones sonoras o de vídeo, de discos y de programas informáticos, que hubiesen sido desprecintados por el consumidor; d) suministro de prensa diaria, publicaciones periódicas y revistas; f) servicios de apuestas y loterías.

No hace diferencia entre productos tangibles o no tangibles.

6.3.1.2 Análisis de legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México y Perú

Chile establece en su Ley 19496 de Protección al Consumidor, artículo 3 bis, que el consumidor puede poner término a un contrato unilateralmente en un plazo de 10 días a partir de la recepción del producto o servicio, en compras celebradas por medio electrónico entre otras.

El artículo 2 de la ley Orgánica en Defensa del Consumidor de Ecuador, define el derecho a la devolución, y que se aplica para ventas por correo, catálogo, teléfono, Internet y otros medios similares. Y en su artículo 45, establece 3 días posteriores a la recepción del bien o servicio para ejercer el derecho de devolución en compras realizadas por Internet entre otras.

Artículo 31, inciso j) de la Ley 7472 de Promoción de la Competencia y Protección efectiva del Consumidor de Costa Rica, indica, como una obligación del comerciante, fijar plazos prudenciales para formular reclamos.

Sobre el derecho de devolución, el artículo 37 establece, para las ventas a domicilio que se llevan a cabo fuera del local comercial, que el consumidor puede rescindir el contrato sin responsabilidad, en un plazo de ocho días contados a partir del perfeccionamiento. Interpretando que las ventas por Internet caen dentro de esta categoría de venta a domicilio, el consumidor podría rescindir el contrato.

El artículo 469 del Código de Comercio de Costa Rica, le da potestad al vendedor de aceptar o no la devolución de alguna cosa comprada por el consumidor. El vendedor tiene 5 días siguientes para manifestar judicialmente su desacuerdo en la devolución. Y su artículo 477 protege más bien al vendedor al permitir que reclame indemnización cuando el comprador no quiera recibir los efectos comprados. Claramente estos artículos protegen al vendedor y no al consumidor.

Ley Federal de Protección al Consumidor de México, en su artículo 56 indica en ventas a domicilio, mediatas o indirectas, que el contrato se perfeccionará a los cinco días hábiles contados a partir de la entrega del bien o de la firma del contrato, lo último que suceda. Plazo en el cual el consumidor puede revocar su consentimiento sin responsabilidad alguna, avisando o devolviendo el bien, y el proveedor debe reintegrar el precio pagado al consumidor. En este caso, los costos de flete y seguro corren a cargo del consumidor.

6.3.1.3 Aciertos

Chile y Ecuador establecen explícitamente el plazo (diez días y tres días respectivamente, después de haber recibido el bien) que tiene el consumidor de rescindir el contrato de compra y venta realizado por Internet o en forma electrónica.
México también lo establece de manera no explícita, se interpreta que la venta por Internet caen dentro de la categoría de venta a domicilio, mediata o indirecta, y por lo tanto se aplica su artículo 56 del plazo de 5 días para perfeccionar el contrato y por lo tanto la posibilidad de devolución del bien sin responsabilidad del consumidor.

6.3.1.4 Vacíos

Actualmente la Ley 7472 y el Código de Comercio de Costa Rica no tienen nada establecido en relación al derecho de devolución en compras realizadas por Internet, pues no tienen nada incluido con respecto a compras por este medio. Sin embargo, si se asimila las venta por Internet como una venta a domicilio, el artículo 37 de la Ley 7472 permite la devolución hasta 8 días después de perfeccionado el contrato.

Y el Código de Comercio protege más al vendedor que al comprador, no permitiendo el derecho a la devolución al consumidor, como sí lo tienen establecidos las legislaciones de Chile, Ecuador y México.

El Código de Comercio de Costa Rica tiene indicado la posibilidad de que el vendedor acepte o no una devolución de mercadería vendida a un consumidor; se podría interpretar que es para una venta realizada por cualquier medio, pero también indica

que si el vendedor no acepta la devolución puede plantear la indemnización ante la autoridad jurisdiccional competente. Este Código protege al vendedor al no permitir que el comprador se niegue a recibir los bienes comprados sin justificación. Para compras por Internet, es necesario incorporar el derecho a la devolución de lo comprado hasta transcurrido un tiempo determinado después de recibido el bien o servicio, como sí lo tienen las legislaciones de Ecuador, Chile y México, para proteger al consumidor y darle el período de reflexión que requiere y determinar su propia necesidad de la compra.

6.3.1.5 Recomendaciones

El derecho a la resolución del contrato sin penalización alguna para el comprador responde a una política comunitaria de protección de los consumidores, permitiendo la tutela de situaciones de arrepentimiento y que obedecen a la simple percepción del consumidor en el plazo establecido de que no se cumplen las expectativas que inclinaron al mismo a efectuar la compra (Vega, 2005). Este plazo permite al consumidor reflexionar sobre la compra, comparar el producto, observar la veracidad de las calidades argumentadas, reflexionar sobre la importancia de adquirirlo y la conveniencia de contratar por medios electrónicos, permitiendo que el consumidor desista del contrato, aun cuando este ya haya sido perfeccionado y sin que este incurra en responsabilidad alguna (Burgos, 2003). Aunque pareciera criticable este ejercicio tan libre y arbitrario de un derecho ya que puede dar lugar abusos en la práctica, tiene como designio la promoción de este tipo de contratos celebrados electrónicamente.

Por lo tanto, y siguiendo el espíritu de la Directiva comunitaria, se recomienda incluir en la Ley 7472 la mención expresa y explícita de que el consumidor tiene un plazo prudencial para ejercer su derecho a la devolución de un bien o servicio adquirido a través de Internet, contados a partir de la recepción del bien o servicio, y sin responsabilidad para él. En el caso de los bienes intangibles, en que la entrega se realiza inmediatamente a través de la red, este plazo servirá para que el consumidor reflexione y decida si al final desea o no el bien o servicio.

Para la definición del plazo para la devolución del bien, o resolución del contrato, debe tomarse en cuenta el tiempo de entrega del bien al domicilio del consumidor, y tomar en consideración de que la compra puede ser en un sitio en el extranjero.

6.3.2 Reclamos, legislación aplicable, jurisdicción competente.

Después que el consumidor ha recibido el bien o servicio, y no esté satisfecho en razón de incumplimiento de las características del bien o servicio, o de la garantía establecida, debe, en primera instancia, recurrir directamente al propio proveedor y plantear su reclamo. Si el proveedor le resuelve su inconformidad no habría ningún problema. Si por el contrario, el proveedor no es capaz de resolver su situación de inconformidad o no está de acuerdo con el reclamo, el consumidor debe recurrir a otras instancias.

En el caso de una compra venta en Internet, el procedimiento y el plazo para reclamos debieron quedar establecidos en el contrato electrónico, y el consumidor debe iniciar este procedimiento para reclamar sus derechos.

La mayoría de los reclamos de los consumidores se refiere al incumplimiento por parte del proveedor de los aspectos de la garantía del producto o del servicio, o por productos o servicios defectuosos.

El proveedor debe describir de manera correcta los productos o servicios para evitar inducir a error de interpretación al consumidor final y facilitar la información necesaria para su plena utilización y aprovechamiento por parte del usuario. Por otro lado, el proveedor tiene la obligación de garantizar los productos que vende o los servicios que presten.

6.3.2.1 Disposiciones de Organismos Internacionales

La Convención de Roma de 1980, establece algunas reglas básicas que comienzan por el principio de libertad de elección de fuero (artículo 3), así como la normativa aplicable en caso de que no se haya pactado nada al respecto (artículo 4), y garantiza al consumidor, bajo ciertas circunstancias, la protección de las reglas imperativas del país donde resida habitualmente (artículo 5).

El artículo 5 establece la ley aplicable a los contratos transnacionales con los consumidores; según este artículo, para decidir si el consumidor merece o no una protección especial, es necesario referirse a un momento en el tiempo o en el espacio. En general el consumidor estaría protegido mediante la aplicación de la ley de su país de residencia sólo si se da alguna de estas condiciones: a) en ese país se hayan llevado a cabo todos los pasos de cara a la celebración del contrato (publicidad, oferta, conclusión) o b) si el oferente recibe el pedido del consumidor en el país de residencia de éste último o c) si el consumidor realizó su pedido en otro país siempre que el viaje haya sido organizado por el oferente con la finalidad de concluir el contrato. Es evidente que estas normas no se ajustan al comercio electrónico, donde el tiempo y el lugar no son relevantes.

La Resolución del Consejo, de 25 de mayo del 2000, relativa a una red comunitaria de órganos nacionales encargados de la solución extrajudicial de litigios de consumo, creó una red que ayuda a los consumidores a resolver los litigios transfronterizos que los enfrentan a las empresas que suministran bienes o servicios defectuosos, dirigiéndolos hacia los organismos de resolución alternativa de litigios (RAL).

Actualmente esta red comprende 17 puntos de contacto nacionales: uno por Estado miembro, uno en Noruega y otro en Islandia.

Cada Estado miembro designa, para la conexión en red de los órganos nacionales de solución extrajudicial de litigios, un punto central (centro de intercambio de información) como punto de contacto para los consumidores que deseen iniciar un procedimiento extrajudicial en otro Estado miembro. Estos puntos constituyen una red extrajudicial destinada a facilitar la solución de litigios de consumo transfronterizos.

Por otro lado, en la Unión Europea, la norma aplicable a la cuestión de la competencia judicial en los litigios con consumidores es el reglamento Bruselas I (44/2001). Este regula la jurisdicción y la ejecución de resoluciones judiciales en materia civil y

mercantil. Contiene reglas de protección de los consumidores en los artículos 13, 14 y 15.

El artículo 16 establece que los consumidores pueden interponer acciones contra la otra parte contratante o en el país donde estuviese domiciliado el consumidor, o en el país de domicilio de la otra parte contratante. Pero si se trata de acciones entabladas contra el consumidor, éstas sólo podrán interponerse ante los tribunales del domicilio del consumidor.

“Los Protocolos que acompañan al Convenio de Bruselas otorgan a los tribunales nacionales de apelación la posibilidad de elevar cuestiones prejudiciales al Tribunal de Justicia de las Comunidades Europeas, cuando exista alguna duda interpretativa” (Vega, 2005, p. 449).

También el artículo 17 de la Directiva 2000/31/Ce, sobre comercio electrónico, alude a la solución extrajudicial de litigios con ciertas recomendaciones, en el sentido de que los Estados miembros velen porque, en caso de desacuerdo entre un prestador de servicios de la sociedad de la información y el destinatario del servicio, su legislación no obstaculice la utilización de mecanismos de solución extrajudicial, incluso utilizando vías electrónicas adecuadas. En el caso específico de los litigios en materia de consumo, se ordena que los Estados alienten a los órganos responsables a que actúen de modo tal que proporcionen garantías de procedimientos adecuados a las partes afectadas.

El artículo 18 de esta misma Directiva, impone a los Estados miembro la obligación de velar porque las actividades de servicios de la sociedad de la información puedan ser objeto de recursos judiciales eficaces, que permitan adoptar, en el plazo más breve y por procedimiento sumario, medidas dirigidas a solucionar la trasgresión alegada y evitar que se produzcan nuevos perjuicios contra los intereses de los afectados.

6.3.2.2 Análisis de legislación comparada: Chile, Colombia, Costa Rica, Ecuador, México y Perú

Chile

Servicio Nacional del Consumidor

El título V de la Ley 19496 de Chile establece que el Servicio Nacional del Consumidor será un servicio público funcionalmente descentralizado y desconcentrado territorialmente en todas las regiones del país, con personalidad jurídica y patrimonio propio, sujeto a la supervigilancia del Presidente de la República a través del Ministerio de Economía, Fomento y Reconstrucción.

El Servicio Nacional del Consumidor le corresponde velar por el cumplimiento de las disposiciones de la ley 19496 y demás normas en relación con el consumidor, difundir los derechos y deberes del consumidor y realizar acciones de información y educación del consumidor. Sus funciones están establecidas en el artículo 58, y entre otras tiene la de:

> "recibir reclamos de consumidores que consideren lesionados sus derechos y dar a conocer al proveedor respectivo el motivo de inconformidad a fin de que voluntariamente pueda concurrir y proponer las alternativas de solución que estime convenientes. Sobre la base de la respuesta del proveedor reclamado, el Servicio Nacional del Consumidor promoverá un entendimiento voluntario entre las partes. El documento en que dicho acuerdo se haga constar tendrá carácter de transacción extrajudicial y extinguirá, una vez cumplidas sus estipulaciones, la acción del reclamante para perseguir la responsabilidad contravencional del proveedor" (inc. F, Art.58, Ley 19496 de Chile, 2004, p.32)

El Servicio Nacional del Consumidor puede denunciar los posibles incumplimientos ante los organismos o instancias jurisdiccionales respectivas y de hacerse parte en las causas en que estén afectados los intereses generales de los consumidores.

Procedimiento jurisdiccional

El artículo 50 A de la Ley 19496 indica que en los contratos celebrados por medios electrónicos el juez competente para conocer de la infracción es el de la comuna en que resida el consumidor. Y la denuncia o demanda debe ser presentada por escrito y no requiere de un abogado. Las partes pueden comparecer personalmente sin intervención de letrado, salvo en los casos de intereses colectivos o difusos.

El párrafo 2 del título IV de la Ley 19496 establece el procedimiento cuando al interés colectivo o difuso de los consumidores se vean afectados. Son de interés colectivo las acciones que se promueven en defensa de derechos comunes a un conjunto determinado o determinable de consumidores, ligados con un proveedor por un vínculo contractual. Son de interés difuso las acciones que se promueven en defensa de un conjunto indeterminado de consumidores afectados en sus derechos.

Colombia

La Superintendencia de Industria y Comercio (SIC)

En Colombia, la competencia para conocer de las violaciones a las normas de protección al consumidor está dada a la Superintendencia de Industria y Comercio (SIC) de acuerdo con el artículo 2 del Decreto 2153 de 1992. Además tiene otras funciones que están establecidas en el artículo 43 del Decreto 3466 y el artículo 145 de la Ley 446.

La Superintendencia de Industria y Comercio (SIC) es un organismo de carácter técnico adscrito al Ministerio de Desarrollo Económico, que goza de autonomía administrativa, financiera y presupuestal. En materia de protección al consumidor, es la encargada de velar por la observancia de las disposiciones que regulan la materia, y dar trámite a las reclamaciones o quejas que se presenten, cuya competencia no haya sido asignada a otra autoridad, e imponer, de acuerdo con el procedimiento aplicable, las sanciones que sean pertinentes por violación de las normas sobre protección al consumidor, así como por la inobservancia de las instrucciones impartidas por la Superintendencia. La SIC tiene facultades para investigar, requerir, inspeccionar, interrogar, etc., para verificar el cumplimiento de las disposiciones legales y adoptar las medidas que correspondan para el esclarecimiento de los hechos durante el desarrollo de sus funciones.

La SIC tramita las denuncias que se presentan e inicia investigaciones de oficio. Puede suspender conductas ilegales, sancionar a los infractores y resolver sobre la efectividad de la garantía a los consumidores.

Procedimiento jurisdiccional

La competencia para conocer de los procesos denunciados por un consumidor contra un proveedor o productor para solicitar la efectividad de garantía, la tiene los Jueces Civiles, o la Superintendencia de Industria y Comercio de acuerdo con el artículo 145 de la Ley 446.

Para las acciones indemnizatorias en las que participan más de 20 consumidores como reclamantes, el procedimiento será el establecido en la Ley 472 de 1998, para las acciones de grupo.

Costa Rica

Comisión Nacional del Consumidor

La Comisión Nacional del Consumidor, es un órgano de máxima desconcentración, adscrita al Ministerio de Economía, Industria y Comercio. Le corresponde velar por el cumplimiento de las disposiciones de los capítulos V y VI de la ley 7472 y las demás normas que garanticen la defensa efectiva del consumidor, que no se le hayan atribuido, en forma expresa, a la Comisión para Promover la Competencia.

Las potestades de la Comisión Nacional del Consumidor están establecidas en el artículo 50 de la Ley 7472 entre las cuales se encuentran: sancionar incumplimiento de obligaciones establecidas en el capítulo V de la ley 7472; ordenar reparación o sustitución del bien o devolución de dinero; ordenar medida cautelares entre otras.

La Comisión Nacional del Consumidor no tiene competencia para conocer de la anulación de cláusulas abusivas en los contratos de adhesión, conforme al artículo 39 de esta ley, ni del resarcimiento de daños y perjuicios. Estos casos deben ser conocidos solo por los órganos jurisdiccionales competentes.

Procedimiento jurisdiccional

El incumplimiento de alguna de las obligaciones enumeradas en el artículo 31 de la Ley 7472, faculta al interesado para acudir a la Comisión Nacional del Consumidor, o a los

órganos jurisdiccionales competentes, para hacer valer sus derechos, en los términos que señala el artículo 43 de esta misma ley.

El artículo 43 establece que para hacer valer sus derechos, el consumidor puede acudir a la vía administrativa o a la judicial, sin que estas se excluyan entre sí, excepto si se opta por la vía judicial. En la vía judicial debe seguirse el proceso sumario establecido en los artículos 432 y siguientes del Código Procesal Civil. El juez, en los procesos por demandas de los consumidores para hacer valer sus derechos, una vez contestada la demanda y siempre que se trate de intereses exclusivamente patrimoniales, realizará una audiencia de conciliación con el fin de procurar avenir a las partes a un acuerdo. De no lograrse, se continuará con el trámite del proceso.

Los procesos que se entablen para reclamar la anulación de contratos de adhesión o el resarcimiento de daños y perjuicios en virtud de violaciones a esta ley, para los cuales la Comisión Nacional del Consumidor no tiene competencia, serán conocidos solo por los órganos jurisdiccionales competentes, de conformidad con el artículo 43.

Ecuador

La Defensoría del Pueblo

El artículo 81 de la Ley Orgánica de Defensa del Consumidor de Ecuador, le asigna la facultad a la Defensoría del Pueblo de conocer y pronunciarse motivadamente sobre los reclamos y las quejas, que presente cualquier consumidor, nacional o extranjero. La Defensoría del Pueblo podrá promover la utilización de mecanismos alternativos para la solución de conflictos, como la mediación, siempre que dicho conflicto no se refiera a una infracción penal. Sin perjuicio de lo dispuesto en el presente artículo, el consumidor podrá acudir, en cualquier tiempo, a la instancia judicial o administrativa que corresponda.

Dentro del trámite administrativo la Defensoría del Pueblo podrá convocar a audiencia pública para que las partes involucradas formulen los alegatos pertinentes, y si no se ha llegado a una solución de mutuo acuerdo, el funcionario competente deberá emitir resolución motivada sobre la queja.

A la comprobación de una violación de las normas de protección al consumidor, la Defensoría del Pueblo o el interesado deben solicitar a las autoridades judiciales respectivas que se inicien las acciones civiles o penales a que hubiere lugar.

A pesar de existir resolución administrativa en contra de un proveedor, el juez competente no tiene la obligación de acoger los argumentos expuestos de la Defensoría.

También las asociaciones de consumidores pueden representar los intereses de estos ante las autoridades judiciales por solicitud expresa de los consumidores.

Procedimiento Jurisdiccional

Son competentes para conocer y resolver sobre las infracciones a las normas de protección al consumidor, en primera instancia, el Juez de Contravenciones de la respectiva jurisdicción, y, en caso de apelación, el Juez de lo Penal de la respectiva jurisdicción de acuerdo con el artículo 84 de la Ley Orgánica de Defensa del Consumidor.

El procedimiento se inicia mediante denuncia, acusación particular o excitativa fiscal, y se adelanta mediante un proceso oral, en audiencia pública en que se deben presentar las pruebas de cada una de las partes. En caso necesario, el artículo 85 de la Ley Orgánica de Defensa del Consumidor indica que el juez puede requerir intervención de peritos o informes técnicos para resolver de fondo el asunto.

De la sentencia que dicte el juez de contravenciones se podrá interponer el recurso de apelación, según el artículo 86 de la Ley Orgánica de Defensa del Consumidor, que debe ser resuelto por el respectivo juez penal. La sentencia que dicte el juez penal si ésta es favorable al consumidor, va implícita la obligación del sentenciado de pagar daños y perjuicios al afectado, costas y honorarios como lo establece el artículo 87 de la Ley Orgánica de Defensa del Consumidor.

Por otro lado, solo Ecuador establece en su Ley 67 de comercio electrónico, firmas y mensajes de datos un artículo sobre jurisdicción:

> "Art. 47.- Jurisdicción.- En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario.
>
> Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta ley y demás normas legales aplicables.
>
> Cuando las partes pacten someter las controversias a un procedimiento arbitral en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje." (Ley 67de Ecuador, 2002, p.9).

México

Procuraduría Federal del Consumidor

El artículo 20 de la Ley Federal de protección al consumidor de México establece que la Procuraduría Federal del Consumidor es un organismo descentralizado de servicio social con personalidad jurídica y patrimonio propio. Tiene funciones de autoridad administrativa y está encargada de promover y proteger los derechos e intereses del consumidor y procurar la equidad y seguridad jurídica en las relaciones entre proveedores y consumidores.

El artículo 24 de esta misma ley indica las atribuciones de la Procuraduría, entre las cuales están: procurar la solución de las diferencias entre consumidores y proveedores y, en su caso, emitir dictámenes en donde se cuantifiquen las obligaciones contractuales del proveedor, conforme a los procedimientos establecidos en esta ley; y denunciar ante el Ministerio Público los hechos que puedan ser constitutivos de delitos y que sean de su conocimiento y, ante las autoridades competentes, los actos que constituyan violaciones administrativas que afecten los intereses de los consumidores.

La Procuraduría puede ejercer ante los tribunales competentes acciones en representación de los consumidores.

Procedimiento jurisdiccional

El artículo 99 establece que la Procuraduría recibirá las quejas o reclamaciones de los consumidores con base en esta ley, las cuales podrán presentarse en forma escrita, oral, telefónica, electrónica o por cualquier otro medio idóneo.

El artículo 100 indica que las reclamaciones podrán desahogarse a elección del reclamante, en el lugar en que se haya originado el hecho motivo de la reclamación; en el del domicilio del reclamante, en el del proveedor, o en cualquier otro que se justifique, tal como el del lugar donde el consumidor desarrolla su actividad habitual o en el de su residencia. En caso de no existir una unidad de la Procuraduría en el lugar que solicite el consumidor, aquélla hará de su conocimiento el lugar o forma en que será atendida su reclamación.

Art. 110 indica que los convenios aprobados y los laudos emitidos por la Procuraduría tienen fuerza de cosa juzgada y traen aparejada ejecución, lo que podrá promoverse ante los tribunales competentes en la vía de apremio o en juicio ejecutivo, a elección del interesado.

Las infracciones a lo dispuesto en ley Federal de Protección al Consumidor serán sancionadas por la Procuraduría quien podrá establecer sanciones que van desde multas hasta clausura total o destrucción de bienes o productos.

La Procuraduría puede realizar procedimientos conciliatorios o arbitrales establecidos detalladamente en las secciones II y III respectivamente, del Capítulo XIII de la Ley Federal de Protección al Consumidor.

Perú

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) fue creado por el Decreto 25868 en 1992 como organismo dependiente del Ministerio de Industria Turismo, Integración y Negociaciones

Comerciales Internacionales. Tiene personería jurídica de derecho público y goza de autonomía técnica, económica, presupuestal y administrativa.

Artículo 38 del Decreto 716 de Perú indica que la Comisión de Protección al Consumidor, en coordinación con el Directorio del INDECOPI, establecerá, directamente o mediante convenios con instituciones públicas o privadas, mecanismos alternativos de resolución de disputas del tipo de arbitraje, mediación, conciliación o mecanismos mixtos, que, mediante procedimientos sencillos y rápidos, atiendan y resuelvan con carácter vinculante y definitivo para ambas partes las quejas o reclamaciones de los consumidores o usuarios, sin perjuicio de las competencias administrativas.

Tiene siete comisiones, una de las cuales es la Comisión de Protección al Consumidor encargada de velar por el cumplimiento de la Ley de Protección al Consumidor aprobada por el Decreto Legislativo 716. Para el efecto, asume las funciones que se refieren los artículos 38 y 42 de dicha norma legal. A través de la Comisión de Protección al Consumidor se protege el cumplimiento de los derechos fundamentales de los consumidores.

El artículo 40 del Decreto 716 indica que el trámite de las investigaciones, por posible violación de normas de protección al consumidor, se pueden iniciar de oficio o a petición de la parte afectada.

Procedimiento Jurisdiccional

El artículo 39 del Decreto 716 establece que la investigación está a cargo de la Comisión de Protección al Consumidor, único órgano administrativo competente para conocer de las presuntas infracciones a las normas de protección al consumidor, así como para imponer sanciones administrativas y medidas correctivas.

El artículo 42 del Decreto 716 establece que la Comisión, además de imponer sanciones, cuenta con facultades para decomisar y destruir mercadería, clausurar

temporalmente establecimientos de comercio y ordenar publicaciones de rectificación de información.

El Decreto 807 de Perú establece el procedimiento a seguir ante la Comisión de Protección del Consumidor. La desobediencia a medidas cautelares se castiga con multa, de persistirse el incumplimiento, la Comisión podrá imponer una nueva multa sin perjuicio de poder denunciar al responsable ante el Ministerio Público para que éste inicie el proceso penal que corresponda.

El INDECOPI ha creado mecanismos para sancionar las prácticas que atenten contra los derechos del consumidor, e instancias donde los consumidores pueden conciliar con los empresarios soluciones satisfactorias para ambas partes. Pero si el consumidor tiene que exigir la devolución de su dinero o el cambio de un producto tiene que recurrir al Poder Judicial.

Cuando no se llega a un acuerdo conciliatorio, se declara fundado el reclamo, los órganos funcionales competentes del INDECOPI sólo podrán imponer una sanción administrativa al proveedor pero no ordenarle realizar una acción en favor del denunciante (como podría ser la devolución de su dinero o el cambio del producto). Es decir, si no hay conciliación, el consumidor deberá recurrir a los procedimientos jurisdiccionales para lograr su indemnización o garantía ante el Juzgado Civil en proceso ordinario de acuerdo con el Código Procesal Civil.

6.3.2.3 Aciertos

El caso de Colombia, el hecho de que a una institución administrativa como la Superintendencia de Industria y Comercio, se le hayan otorgado facultades jurisdiccionales para ordenar la efectividad de garantías, es un gran progreso a favor del consumidor. El que el SIC pueda ordenar la reparación del bien, el cambio por uno nuevo o la devolución del dinero, hace que el proceso sea más ágil y económico para el consumidor que en el caso de recurrir al Juez Civil. Sin embargo, la indemnización de perjuicios causados por el defecto del bien sigue siendo reservada a los jueces.

En Colombia, los consumidores tienen las dos alternativas para reclamar sus derechos, a través de la instancia administrativa de la Superintendencia de Industria y Comercio, y a través de los Jueces Civiles.

En el caso de Costa Rica con la Comisión Nacional del Consumidor tiene la atribución de ordenar, cuando proceda, la devolución del dinero o del producto. Puede fijar, asimismo, un plazo para reparar o sustituir el bien, según corresponda. También se establece en la ley los procedimientos para realizar una conciliación y arbitraje, ambas le corresponden a esta Comisión llevarlas a cabo.

De los artículos 29 y 30 de la Ley 7472 se interpreta que corresponde al Estado:
-Fortalecer los órganos existentes o crear nuevos con amplias facultades para conocer y perseguir los atentados a los derechos de los consumidores, incluidos los que ocurren en el ambiente de comercio electrónico, y
-Crear efectivos mecanismos de solución de controversias originados entre proveedores y consumidores.
Por lo tanto debe implementarse los mecanismos y procedimientos para cumplir con estas funciones.

El reciente proyecto de Ley de Comercio Electrónico de Costa Rica, que pasó a estudio e informe de la Comisión Permanente de Asuntos Jurídicos, el 6 de diciembre del 2005, incluye un artículo sobre jurisdicción, indicando que en casos de controversias, la jurisdicción costarricense será competente si al menos uno, el receptor o prestador, tiene su domicilio en Costa Rica. En el supuesto de que alguna de las partes no tenga domicilio nacional deberá notificársele por vía consular la articulación o demanda interpuesta.

La Ley Federal de Protección al Consumidor de México establece en detalle los procedimientos a seguir en caso de reclamo por parte del consumidor, permitiendo procesos conciliatorios o arbitrales y presentados ante Procuraduría Federal del Consumidor.

Chile establece expresamente en su norma el caso de los contratos celebrados electrónicamente, indicando que el juez competente para conocer la infracción es el de donde resida el consumidor.

Ecuador establece en su ley 67 de Comercio Electrónico, firmas y mensajes de datos un artículo sobre jurisdicción, y resalta en él que en materia con consumidores, la jurisdicción será la del domicilio del consumidor. Además permite el arbitraje a través de medios electrónicos. Esto último es un aspecto novedoso a considerar.

6.3.2.4 Vacíos

En Ecuador, la autoridad administrativa competente, la Defensoría del Pueblo, no cuenta con facultades suficientes para hacer una efectiva vigilancia y control de los proveedores. No tiene capacidad de practicar pruebas más allá de las aportadas, ni tampoco puede sancionar las conductas violatorias. Al parecer, la función principal de la Defensoría del Pueblo se limita a promover los mecanismos alternativos de solución de conflictos, y de practicar audiencias de conciliación.

En Perú, a pesar de haberse creado toda una Institución y una Comisión dentro de ella encargada de los asuntos de los consumidores, ésta tampoco tiene potestad de ordenar la devolución del dinero o el cambio del producto. Si no se logra la conciliación, el consumidor deberá recurrir a los procedimientos jurisdiccionales para lograr su indemnización o garantía ante el Juzgado Civil en proceso ordinario de acuerdo con el Código Procesal Civil.

En el caso de Costa Rica si no se logra una conciliación a nivel de la Comisión Nacional del Consumidor, el consumidor debe acudir a las instancias judiciales para hacer valer sus derechos. Y en los casos de anulación de contratos de adhesión o el resarcimiento de daños y perjuicios la Comisión Nacional del Consumidor no tiene competencia, sólo pueden ser conocidos por los órganos jurisdiccionales competentes, de conformidad con el artículo 43.

En casos de transacciones que traspasan fonteras, se puede recurrir al artículo 1023 del Código Civil, incisos 2 d) y 2 e) el cual indica la imposibilidad del consumidor de renunciar a la jurisdicción nacional en el caso de preceptos que protegen sus derechos y de acudir vía judicial para plantear su reclamo, y los artículos del 23 al 30 de este mismo Código, que se refieren a las Normas del Derecho Internacional Privado.

El artículo 26 establece que la prescripción y todo lo que concierna al modo de cumplir o extinguir las obligaciones de un contrato que haya de ejecutarse en Costa Rica, se regirá por las leyes costarricenses, aunque los otorgantes sean extranjeros, y aunque el acto o contrato no se haya ejecutado o celebrado en el país. Y el artículo 27 indica que para la interpretación de un contrato y para fijar los efectos mediatos o inmediatos que resulten de él, se recurrirá a las leyes del lugar donde se celebró el contrato; pero si los contratantes tuvieran una misma nacionalidad, se recurrirá a las leyes de su país.

Como puede observarse, las normas 26 y 27 del Código Civil no indica la legislación aplicable o la jurisdicción competente para resolver conflictos derivados de los contratos de compra y venta celebrados entre un proveedor extranjero con un consumidor costarricense. Al menos se tiene el artículo 1023 que protege al consumidor de renunciar a la jurisdicción nacional.

Aunque los artículos 29 y 30 de la Ley 7472 se pueda interpretar que entre las funciones del Estado están:
-Fortalecer los órganos existentes o crear nuevos con amplias facultades para conocer y perseguir los atentados a los derechos de los consumidores, incluidos los que ocurren en el ambiente de comercio electrónico, y
-Crear efectivos mecanismos de solución de controversias originados entre proveedores y consumidores.

No existe aún en el país nada establecido al respecto, sólo lo indicado en el Código Civil. Y lo que se establece como derecho constitucional sobre la justicia pronta y cumplida, artículo 41 de la Constitución Política, en Costa Rica es irreal para los casos

en el propio territorio nacional, sin contar que en el comercio electrónico, esto podría agravarse para los casos a nivel internacional.

6.3.2.5 Recomendaciones

Cuando un contrato internacional se celebre por vía electrónica y las partes expresamente no determinen el régimen jurídico aplicable, para la determinación de la ley aplicable y la jurisdicción competente, se seguirán las disposiciones de los convenios y tratados internacionales, en los que Costa Rica sea parte y en su defecto, las normas de derecho internacional privado.

El principio de la autonomía de la voluntad en materia de controversias contractuales, ha sido reconocido por el derecho internacional privado. Como principio general de contratación por medios electrónicos, las partes contratantes tienen la libertad y la posibilidad de escoger la ley que quieran aplicar a su relación jurídica, lo anterior dentro de los límites previstos por la ley y las normas imperativas internacionales que se proyectan directamente en la relación comercial. Existen límites a la autonomía de la voluntad entre los cuales se encuentran: la violación de derechos o desconocimiento de derechos de terceros o fraude a la ley.

En caso de no elección, se aplicarán los principios de proximidad y prestación característica, tomados como referente de la Convención de Roma de 1980, de acuerdo con el artículo 4.1, apartado 2, según el cual, se presume que el contrato presenta los vínculos más estrechos con el país en el que la parte que deba realizar la prestación característica, tenga su residencia habitual o la administración de sus negocios.

En el caso de una contratación en la que interviene un consumidor, la ley aplicable será la de la residencia habitual del consumidor.

Para que un Estado pueda juzgar a un individuo, deben existir elementos suficientes que permitan ejercer jurisdicción. En los casos de actividades en Internet, el principio

de universalidad es la excepción, pues aunque no existan elementos que relacionen al Estado con los hechos, cualquier país pueda aplicar su normativa y juzgar a quienes amenacen la dignidad humana con sus manifestaciones. El juez deberá tomar en cuenta, los contactos relevantes, en los contratos, siendo estos, el lugar de contratación, el lugar de la negociación o perfección del contrato, el lugar de la creación del punto central del contrato, el domicilio, residencia, nacionalidad, lugar de incorporación o trabajo de las partes. Todos estos criterios ayudarán a los jueces para considerar que se tiene jurisdicción para juzgar un caso específico que se presente respecto a una contratación por Internet.

Los Estados requieren la autorización de otras naciones para poder realizar actividades de policía fuera de su territorio, por lo que además de tener jurisdicción para crear las leyes que aplicará, deberá contar con el permiso de otros Estados en donde pretenda efectuar operaciones para ejecutar su ley. En cuanto a las ejecuciones de sentencias, cada caso particular se resolverá de acuerdo a sus circunstancias. Si el sujeto cometiera un delito en Internet, y se encuentra en el mismo territorio del país que lo juzgó, no existirá ningún problema, y si el sujeto se encontrara fuera de éste se requeriría un acuerdo entre los Estados para la extradición del individuo. Por lo tanto los principios de territorialidad, nacionalidad, universalidad, efectos del acto y seguridad nacional, son importantes bajo el ámbito de la jurisdicción ejecutoria, en las actividades realizadas por los individuos en Internet.

Para resolver un conflicto en un caso de compraventa en Internet, será importante para cada compraventa que se presente, el análisis en primer lugar de si las partes han elegido un foro para la aplicación de las leyes y resolución de posibles conflictos. Ante la ausencia de dicho acuerdo, las reglas de derecho internacional público y privado, crean una posibilidad para regular por lo menos las compraventas en Internet. No importa, para el derecho, en dónde se hayan ejecutado los actos, sino en dónde surten éstos efectos. Dependiendo de esto, el foro de un Estado u otro será el competente para aplicar su legislación y juzgar el caso.

El hecho de que un acto se presente en el espacio virtual de la Internet, no implica que se encuentre ante hechos de otro mundo o algo similar. En el caso de compraventas de inmuebles, podemos ver que la aplicación de criterios de territorialidad, demuestran que la ley aplicable será la del lugar en donde se encuentre el inmueble. Por más que la operación se realice en la Internet, o en dos distintos países, lo esencial es que los efectos se producirán en un Estado. En caso de compraventas de bienes, será determinante analizar todos lo aspectos que rodeen la transacción, como nacionalidad de las partes, aspectos territoriales, localización del bien y otros, para definir cual será el foro más apropiado.

Sin embargo, las normas analizadas protegen al consumidor y establecen como regla general que en los casos de contrataciones en las que intervienen un consumidor, la ley aplicable y la jurisdicción competente será la del propio domicilio del consumidor.

En el caso de las compraventas en Costa Rica, si las partes se encuentran en el país, la ley aplicable será la costarricense. No importa que los actos de oferta y aceptación se presenten en Internet, pues la localización de las partes y de los bienes de la transacción determinará que los tribunales nacionales tienen jurisdicción para resolver el caso y aplicar nuestras leyes. Si solo la parte consumidora es de domicilio costarricense, la ley aplicable será la costarricense; esto último con respaldo del artículo 1023 del Código Civil de Costa Rica.

En el caso de compras de bienes físicos, si el comprador no está satisfecho, deberá plantear su demanda en donde se localiza el servidor en el que se encuentra la tienda virtual, es decir, el demandante debe ir al foro del demandado para plantear el caso, con los costos que deben incluir si la tienda se encuentra en otro país. Sin embargo es parte de las complicaciones que nacen por las facilidades para el comercio internacional que se presentan en Internet.

Por ello, la creación de tribunales virtuales es una alternativa factible, que podrían utilizar las partes de un conflicto para procurar resolverlo lo más eficientemente posible.

Esto depende, eso sí, de que las partes elijan la utilización de las reglas de este tipo de tribunal virtual.

Por otro lado, la gran cantidad de transacciones internacionales, y el bajo monto económico de la mayoría de ellas, se ve necesaria la creación de nuevos mecanismos que representen la realidad actual. Por ello organismos con función de tribunales, en Internet, no son una mala opción para resolver el problema.

La mayoría de los consumidores normalmente persiguen la reposición del producto que han adquirido o la devolución del dinero pagado, es decir, en su mayoría se trata de asuntos cuyo valor usualmente no justifica incurrir en los costos de acceder al Poder Judicial. La alternativa administrativa es la mejor opción para los consumidores. Presentar una denuncia formal ante la Comisión Nacional del Consumidor es mucho menos costoso que acudir al Poder Judicial, no se requiere la intervención de un abogado y se trata de un proceso más expedito, o recurrir a medios de resolución alterna de conflictos.

Bruce (2002) sugiere otros medios de resolución alterna de conflictos, además de los tradicionales como la mediación, conciliación y arbitraje:

- La autotutela del consumidor: mediante el cual los mismos consumidores irán desechando a los proveedores que no brinden un servicio con la calidad que es esperada.
- El modelo de autorregulación empresarial: los mismos empresarios, antes de ser reglamentados por el Estado, buscan autorregularse por medio de códigos de ética o de conducta que dictan las agrupaciones gremiales, industriales o comerciales que regulan la actividad. Otra posibilidad es que los comerciantes que tengan una parte mayoritaria del mercado controlada regulen a los minoritarios.
- Los programas de sellos: en la Red algunas compañías reciben un tipo de sello de confianza, que debe ser renovado cada cierto tiempo, por parte de una

empresa fiscalizadora lo cual le dará a los consumidores un medio de fiabilidad para realizar sus transacciones en línea.

Menciona Pérez (2003) que el arbitraje en línea es un mecanismo ágil y eficaz para la solución extrajudicial de conflictos, implementado en Ginebra, Suiza, por medio del Centro de Arbitraje y Mediación de la OMPI. Este Centro, creado en 1994, ofrece servicios de arbitraje y mediación en relación con controversias internacionales comerciales entre partes privadas.

También indica Pérez (2003) que se encuentran aproximadamente 74 centros de arbitraje y conciliación en el mundo que han implementado el arbitraje en línea, para controversias relacionadas con el uso de las tecnologías en la contratación. Afirma que Perú y Colombia estaban en proceso de implementación de este procedimiento arbitral.

Para Pérez (2003), no existen reglas de competencia judicial internacional específicas para las actividades en Internet, más bien, tiende a promoverse una reforma procesal que facilite el desarrollo de mecanismos judiciales rápidos para garantizar una tutela efectiva en este contexto.

Después de todo este análisis, se presenta las recomendaciones que a continuación se exponen.

Es necesario incorporar expresamente en la Ley 7472 de Promoción de la competencia y defensa efectiva del Consumidor que, en esta materia, la legislación aplicable y la jurisdicción competente son las de donde resida el consumidor. Aunque esta protección se encuentra en el Código Civil (artículo 1023), no está de más que se indique expresamente en la Ley 7472, por ser una ley específica en materia de protección al consumidor.

El comprador tiene dos obligaciones principales que son recibir la cosa y pagar el precio convenido. En el caso de una compra y venta en Internet, los problemas de legislación aplicable y Juez competente, pueden ser resueltos incluyendo, en el contrato de

adhesión realizado por medio electrónico, una cláusula indicando que la ley que se aplicará y la jurisdicción competente para resolver eventuales problemas, será la del país donde resida el consumidor.

Muchas normas actuales no se ajustan al entorno electrónico, en el que el tiempo y el espacio de la conclusión de un contrato no son ya relevantes, por esto, se recomienda que para la protección del consumidor en una transacción electrónica, se considere que la legislación aplicable en caso de litigio sea la del país del consumidor para su protección y considerando que es la legislación que mayormente el consumidor conoce.

Es importante que el Estado implemente mecanismos efectivos de solución de controversias originados entre proveedores y consumidores de una relación comercial que traspasan las fronteras nacionales. Hasta el momento, ninguna de las legislaciones hace referencia a transacciones comerciales que involucran una parte en el extranjero. En el ambiente de comercio electrónico, estas son las más usuales, por lo que se hace todavía mucho más necesario implementar los mecanismos efectivos de tutela al consumidor para estos casos. Por lo que sería importante incorporar la posibilidad del arbitraje por medios electrónicos o telemáticos para agilizar el proceso de solución de conflictos. En este sentido, es importante revisar la experiencia española y de la Unión Europea.

Es importante una coordinación a nivel de Organismos Internacionales como los ya existentes como la Organización de las Naciones Unidas (ONU), la Organización para la Cooperación y de Desarrollo Económico (OCDE), o la Organización Mundial del Comercio (OMC) en donde se establezca una Comisión con diferentes representantes de países encargada de los asuntos de controversias en caso de reclamos que no puedan ser resueltos en el propio país del consumidor, que tenga un procedimiento ágil de instrucción y resolución de conflictos para que se respete los intereses económicos del consumidor y se le de una solución ágil y adecuada de su controversia.

En el anexo 6 detalla las normas en las diversas leyes relacionadas y proyectos de ley de Costa Rica con referencia a los vacíos jurídicos encontrados sobre la normativa para la protección del usuario en el ambiente de comercio electrónico.

Capítulo 7. Propuesta de modificaciones a la Ley 7472 de Promoción de la Competencia y Protección Efectiva del Consumidor.

Recogiendo todas las recomendaciones que se han presentado a lo largo de este análisis, se presenta las modificaciones que deben realizarse a la Ley 7472 de Costa Rica, con el fin de proteger al consumidor en las transacciones de compra y venta por medio de Internet, elemento nuevo no contemplado en la legislación existente.

El siguiente cuadro muestra en la columna izquierda el texto actual de la Ley y en la columna derecha la modificación a realizar.

Cuadro 8. Propuesta de modificación a la Ley 7472 de Costa Rica.

Texto actual	Modificación al texto
Artículo 29. Derechos del consumidor Sin perjuicio de lo establecido en tratados, convenciones internacionales de las que Costa Rica sea parte, legislación interna ordinaria, reglamentos, principios generales de derecho, usos y costumbres, son derechos fundamentales e irrenunciables del consumidor, los siguientes: a) La protección contra los riesgos que puedan afectar su salud, su seguridad, y el medio ambiente. b) La protección de sus legítimos intereses económicos y sociales. c) El acceso a una información, veraz y oportuna, sobre los diferentes bienes y servicios, con especificación correcta de cantidad, características, composición, calidad y precio. d) La educación y la divulgación sobre el consumo adecuado de bienes o servicios, que aseguren la libertad de escogencia y la igualdad en la contratación. e) La protección administrativa y judicial contra la publicidad engañosa, las prácticas y las cláusulas abusivas, así como los métodos comerciales desleales o que restrinjan la libre elección. f) Mecanismos efectivos de acceso para la tutela administrativa y judicial de sus derechos e intereses legítimos, que conduzcan a prevenir adecuadamente, sancionar y reparar con prontitud la lesión de estos, según corresponda. g) Recibir el apoyo del Estado para formar	Agregar: h) La Protección contra el uso indebido de sus datos personales: garantizar el derecho al acceso, oposición, rectificación, fijar el nivel de seguridad, uso conforme al fin de sus datos personales. i) La prohibición de interconexión de archivos para obtener un perfil de sus intereses. j) Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente. k) Derecho a la no discriminación en el acceso a productos y servicios, con atención a las necesidades de los consumidores vulnerables.

Texto actual	Modificación al texto
grupos y organizaciones de consumidores y la oportunidad de que sus opiniones sean escuchadas en los procesos de decisión que les afecten.	

Texto actual	Modificación al texto
Artículo 30. Funciones del Poder Ejecutivo En los términos establecidos en la presente ley, son funciones esenciales del Estado las siguientes: a) Velar porque los bienes y servicios que se vendan y se presten en el mercado, cumplan con las normas de salud, seguridad, medio ambiente y los estándares de calidad. b) Formular programas de educación e información para el consumidor, con el propósito de capacitarlo para que pueda discernir y tomar decisiones fundadas acerca del consumo de bienes y servicios, con conocimiento de sus derechos. c) Fomentar y promover las organizaciones de consumidores y garantizar su participación en los procesos de decisión y reclamo, en torno a cuestiones que afectan sus intereses. d) Garantizar el acceso a mecanismos efectivos y ágiles de tutela administrativa y judicial, para defender los derechos y los intereses legítimos de los consumidores. e) Estructurar una canasta básica que satisfaga, por lo menos, las necesidades de los costarricenses cuyo ingreso sea igual o inferior al salario mínimo establecido por ley y regular, cuando lo considere necesario, los bienes y servicios que la componen.	Incluir un inciso: f) Realizar campañas de educación con énfasis en capacitar al consumidor en materia de comercio electrónico, e instruirlo para que pueda tomar sus propias medidas de seguridad en una transacción electrónica. Por ejemplo: - Verificar la existencia real del proveedor a través de listas oficiales dado por el Estado de las empresas vigentes y activas. - Comprar sólo en sitios de reconocido prestigio. - Comprobar que el sitio utiliza medios seguros para realizar las transacciones electrónicas. - Utilizar dinero electrónico justo en la cantidad necesaria. - Revisar los términos del contrato electrónico y comprobar que las cláusulas no viole sus derechos y tenga establecido que la legislación aplicable y jurisdicción competente sea la de su propio país para su mejor protección. g) Velar porque el otorgamiento de una firma digital certificada se requiera al menos la condición de mayoría de edad y ésta sea exigida por la entidad certificadora. h) Velar por que las compras y ventas realizadas por medios electrónicos se exija poseer una firma digital, y que para compras que exija cierta capacidad contractual u otros requisitos personales, sea necesario para realizarla utilizar firmas digitales certificadas o avanzadas. i) Mantener una página Oficial del Estado con una lista de personas físicas o jurídicas que ofrecen ventas por Internet debidamente inscritas en Registro Mercantil y con firma digital certificada. j) Coordinar a nivel internacional para obtener una lista de las personas físicas y jurídicas debidamente identificadas, de otros países que venden por Internet con operaciones en Costa Rica, y ofrecer esta lista en una página oficial del Estado. O tener un sitio Oficial del Estado, y con un mecanismo fácil, en donde el consumidor pueda consultar por la existencia real de una empresa que vende por Internet.
Artículo 31. Obligaciones del	Agregar los incisos que explicite la obligación del proveedor de informar al consumidor lo

Texto actual	Modificación al texto
comerciante Son obligaciones del comerciante y el productor, con el consumidor, las siguientes: a) Respetar las condiciones de la contratación. b) Informar suficientemente al consumidor, en español, de manera clara y veraz, acerca de los elementos que incidan en forma directa sobre su decisión de consumo. Debe enterarlo de la naturaleza, la composición, el contenido, el peso, cuando corresponda, las características de los bienes y servicios, el precio de contado en el empaque, el recipiente, el envase o la etiqueta del producto, la góndola o el anaquel del establecimiento comercial y de cualquier otro dato determinante. De acuerdo con lo dispuesto en el reglamento de la presente ley, cuando el producto que se vende o el servicio que se presta se pague al crédito, deben indicarse, siempre en forma visible, el plazo, la tasa de interés anual sobre saldos, la base, las comisiones y la persona, física o jurídica, que brinda el financiamiento, si es un tercero. ***(Así modificado por Ley No.7623 de 11 de setiembre de 1996)*** c) Ofrecer, promocionar o publicitar los bienes y servicios de acuerdo con lo establecido en el artículo 34 de esta ley. d) Suministrar, a los consumidores, las instrucciones para utilizar adecuadamente los artículos e informar sobre los riesgos que entrañe el uso al que se destinan o el normalmente previsible para su salud, su seguridad y el medio ambiente. e) Informar al consumidor si las partes o los repuestos utilizados en reparaciones son usados. Si no existe advertencia sobre el particular, tales bienes se consideran nuevos. f) Informar cuando no existan en el país servicios técnicos de reparación o repuestos para un bien determinado. g) Garantizar todo bien o servicio que se ofrezca al consumidor, de conformidad con el artículo 40 de esta ley. h) Abstenerse de acaparar, especular, condicionar la venta y discriminar el consumo. i) Resolver el contrato bajo su responsabilidad, cuando tenga la obligación de reparar el bien y no la satisfaga en un tiempo razonable. j) Fijar plazos prudenciales para formular reclamos.	siguiente en caso de información y publicidad divulgada a través de la página Web o cualquier otro medio electrónico: p) identificación del proveedor, domicilio geográfico, y medios de contacto (teléfono, fax, e-mail, etc.), gastos de transporte, la forma de pago, las modalidades de entrega o de ejecución de servicios, el plazo de la validez de la oferta, garantías, procedimientos para reclamos, países a los que se dirige la publicidad, indicación de la posible recopilación de datos del consumidor y su justificación, advertencias sobre contenidos no apto y a qué tipo de población, así como: mecanismos de comunicación rápida, fácil y efectiva con la empresa; mecanismos efectivos de solución de disputas; servicios de atención a procedimientos legales; dirección del domicilio legal de la empresa y sus directivos, su referencia en el registro mercantil. Además agregar las siguientes obligaciones del proveedor: q) la difusión y promoción del uso de códigos de ética en las relaciones comerciales electrónicas. r) No utilizar información sobre consumidores con fines mercadotécnicos o publicitarios. s) No enviar publicidad, a través de medios electrónicos, a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla. Se incluye la publicidad enviada por correo electrónico. Los proveedores que sean objeto de publicidad son co-responsables del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros. t) No distribuir las direcciones electrónicas ni ninguna información personal del consumidor sin consentimiento del titular. u) Respetar la privacidad del consumidor en relación con el uso de cookies. v) Tener una política de privacidad y divulgarla en la página principal del sitio del proveedor o productor, que incluya lo siguiente: - la identificación de la empresa dueña del sitio y lo administra. - la naturaleza de la información recolectada; - la justificación del almacenamiento de la información - el uso que se le va a dar - quiénes comparten la información recolectada - los derechos de oposición que tiene el

Texto actual	Modificación al texto
k) Establecer, en las ventas a plazos, garantías de pago proporcionales a las condiciones de la transacción. l) Cumplir con los artículos 35, 36, 37, 38, 39, 40, 41 y 41 bis de esta ley. ***(Así modificado por el artículo 1, inc. a) de la ley No. 7854 del 14 de diciembre de 1998.)*** m) Cumplir con lo dispuesto en las normas de calidad y las reglamentaciones técnicas de acatamiento obligatorio. n) Mantener en buenas condiciones de funcionamiento y debidamente calibradas las pesas, las medidas, las registradoras, las básculas y los demás instrumentos de medición, que utilicen en sus negocios. ñ) Extender la factura o el comprobante de compra, donde conste, en forma clara, la identificación de los bienes o servicios, así como el precio efectivamente cobrado. En los casos de ventas masivas, se faculta al Ministerio de Economía, Industria y Comercio para autorizar el establecimiento de otros sistemas mediante los cuales se compruebe la compra. o) Apegarse a la equidad, los buenos usos mercantiles y a la ley, en su trato con los consumidores. Toda información, publicidad u oferta al público de bienes ofrecidos o servicios por prestar, transmitida por cualquier medio o forma de comunicación, vincula al productor que la transmite, la utiliza o la ordena y forma parte del contrato. El incumplimiento de alguna de las obligaciones enumeradas en este artículo, faculta al interesado para acudir a la Comisión nacional del consumidor creada en esta ley, o a los órganos jurisdiccionales competentes y para hacer valer sus derechos, en los términos que señala el artículo 43 de la presente ley.	usuario - el tiempo que la información es almacenada - los mecanismos de seguridad para evitar intromisiones en el almacenamiento de la información personal - cómo puede cambiar en el futuro la política de privacidad del sitio - la identificación de la persona responsable de la privacidad de la información - la identificación del organismo encargado de vigilar y fiscalizar en materia de tratamiento de datos personales. x) Solicitar la firma digital certificada para que un consumidor pueda acceder a páginas Web de contenidos no aptos para cierta población. y) Utilizar servidores y mecanismos seguros para realizar las transacciones de comercio electrónicas, y confirmar las órdenes de compra por e-mail o por teléfono cuando son por grandes cantidades de dinero. z) Establecer cláusulas de protección al consumidor en los contratos de adhesión, que garanticen que el proveedor se hará responsable de las pérdidas que sufra el consumidor por violación de la seguridad de los datos durante la transmisión en la Red. Za) Firmar digitalmente los contratos de adhesión realizados por medios electrónicos y entregar una copia fiel de este al consumidor.
Artículo 34. Oferta, promoción y publicidad La oferta, la promoción o la publicidad de los bienes y servicios debe realizarse de acuerdo con la naturaleza de ellos, sus características, condiciones, contenido, peso cuando corresponda, utilidad o finalidad, de modo que no induzca a error o engaño al consumidor. No pueden omitirse tales informaciones, si de ello puede derivarse daño o peligro para la	Agregar al final un párrafo que indique lo siguiente: Se considerará la publicidad falsa o engañosa como fraude y su sanción será de acuerdo a lo estipulado en el Código Penal según el daño que provoque. (se debe incluir este tipo de delito en el Código Penal)

Texto actual	Modificación al texto
salud o la seguridad del consumidor. Deben prevalecer las cláusulas estipuladas en los contratos, si son más beneficiosas que el contenido de la oferta, la promoción o la publicidad de los bienes y servicios. El empleo de términos comparativos en la oferta, la promoción o la publicidad de los bienes y servicios, sólo se admite respecto a datos esenciales, afines y objetivamente demostrables, siempre que se comparen con otros similares, conocidos o de participación significativa en el mercado. La comparación no es admisible cuando se limite a la proclamación, general e indiscriminada, de la superioridad de los productos propios; se tiene por engañosa la que omita cualquier elemento necesario para determinar el valor real de los productos. Al productor o al comerciante que, en la oferta, la promoción, la publicidad o la información, incumpla con las exigencias previstas en este artículo, se le debe obligar a rectificar la publicidad, costearla y divulgar la información veraz u omitida, por el mismo medio y forma antes empleados.	
Artículo 39. Cláusulas abusivas en contratos de adhesión En los contratos de adhesión, sus modificaciones, anexos o adenda, la eficacia de las condiciones generales está sujeta al conocimiento efectivo de ellas por parte del adherente o a la posibilidad cierta de haberlas conocido mediante una diligencia ordinaria. ***(Así modificado este párrafo por el artículo 1, inc. b) de la ley No. 7854 del 14 de diciembre de 1998.)*** Son abusivas y absolutamente nulas las condiciones generales de los contratos de adhesión, civiles y mercantiles, que: a) Restrinjan los derechos del adherente, sin que tal circunstancia se desprenda con claridad del texto. b) Limiten o extingan la obligación a cargo del predisponente. c) Favorezcan, en forma excesiva o desproporcionada, la posición contractual de la parte predisponente o importen renuncia o restricción de los derechos del adherente. d) Exoneren o limiten la responsabilidad del predisponente por daños corporales, cumplimiento defectuoso o mora. e) Faculten al predisponente para rescindir unilateralmente el contrato, modificar sus	Agregar incisos adicionales al artículo 39: k) En contratos electrónicos, se considera cláusula abusiva aquella que establezca la legislación aplicable en caso de litigio un país distinto al de residencia del consumidor. l) En contratos electrónicos, se considera cláusula abusiva aquella que establezca la jurisdicción competente en caso de litigio un país o lugar distinto al de residencia del consumidor. Incluir un artículo adicional: Artículo 39 bis. Cláusulas en contratos electrónicos: Todo contrato de adhesión celebrado a través de medios electrónicos debe contener las siguientes cláusulas. - La identificación de las partes; que incluye la identificación del Registro Mercantil del proveedor. - la dirección geográfica (domicilio social) del establecimiento del proveedor de bienes o servicios; - las obligaciones de las partes; - características y precio del producto o servicio pactado; - los gastos de entrega; - las modalidades de pago, - forma de entrega o ejecución, - Garantías, - la cláusula de confidencialidad de datos personales, en la cual hay un compromiso

Texto actual	Modificación al texto
condiciones, suspender su ejecución, revocar o limitar cualquier derecho del adherente, nacido del contrato, excepto cuando tal rescisión, modificación, suspensión, revocación o limitación esté condicionada al incumplimiento imputable al último. f) Obliguen al adherente a renunciar con anticipación a cualquier derecho fundado en el contrato. g) Impliquen renuncia, por parte del adherente, a los derechos procesales consagrados en el Código Procesal Civil o en leyes especiales conexas. h) Sean ilegibles. i) Estén redactadas en un idioma distinto del español. Son abusivas y relativamente nulas, las cláusulas generales de los contratos de adhesión que: a) Confieran, al predisponente, plazos desproporcionados o poco precisos para aceptar o rechazar una propuesta o ejecutar una prestación. b) Otorguen, al predisponente, un plazo de mora desproporcionado o insuficientemente determinado, para ejecutar la prestación a su cargo. c) obliguen a que la voluntad del adherente se manifieste mediante la presunción del conocimiento de otros cuerpos normativos, que no formen parte integral del contrato. d) Establezcan indemnizaciones, cláusulas penales o intereses desproporcionados, en relación con los daños para resarcir por el adherente. j) Los que no indiquen las condiciones de pago, la tasa de interés anual por cobrar, los cargos e intereses moratorios, las comisiones, los sobreprecios, los recargos y otras obligaciones que el usuario quede comprometido a pagar a la firma del contrato. ***(Así adicionado este inciso por el artículo 2, inc. a) de la ley No. 7854 del 14 de diciembre de 1998.)*** En caso de incompatibilidad, las condiciones particulares de los contratos de adhesión deben prevalecer sobre las generales. Las condiciones generales ambiguas deben interpretarse en favor del adherente.	de no utilizar los datos personales de los clientes para fines diferentes a los previsto inicialmente; - la indicación de que la legislación aplicable es la del lugar de residencia del consumidor (no hay que olvidar que se pueden realizar operaciones comerciales con personas físicas o morales de diversos países en los cuales la legislación a aplicar será distinta y el consumidor no conoce forzosamente), - la jurisdicción competente es la del lugar de residencia del consumidor, - procedimientos para reclamos o mecanismos efectivos de solución de disputas, - mecanismos de comunicación rápida, fácil y efectiva con la empresa, - servicios de atención a procedimientos legales; - dirección del domicilio legal de la empresa y sus directivos. Estas cláusulas deben ser legibles, claras y en idioma castellano. Además el contrato de adhesión debe ser fácilmente accesible y se debe entregar una copia fiel del contrato al consumidor. El contrato de adhesión no debe contener remisiones a textos que no se faciliten al consumidor. El contrato celebrado por medio electrónico debe estar firmado digitalmente por ambas partes: proveedor y consumidor. Artículo 39 ter. Perfección del contrato electrónico: - la recepción por parte del consumidor del acuse de recibo de su declaración contractual y del texto del propio contrato perfecciona el contrato. -el lugar de perfeccionamiento del contrato es, salvo acuerdo de las partes, el lugar donde se encuentra el consumidor, para su mejor protección. - la recepción, confirmación de recepción, o apertura del mensaje de datos no implica aceptación del contrato electrónico, salvo acuerdo de las partes. - el momento y lugar de envío o recepción del documento electrónico de acuerdo con lo establecido en el artículo 15 de la ley Modelo sobre Comercio Electrónico: "1-De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando entre

Texto actual	Modificación al texto
	en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos en nombre del iniciador. 2) De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue: *a)* Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar: i) En el momento en que entre el mensaje de datos en el sistema de información designado; o ii) De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos; *b)* Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar al entrar el mensaje de datos en un sistema de información del destinatario. 3) El párrafo 2) será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje conforme al párrafo 4). 4) 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 párrafo: *a)* Si el iniciador o el 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 tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.” (CNUDMI, 1998, p.18). Artículo 39 cuat. Las compras y ventas que requieran capacidad contractual se debe realizar con respaldo de firma digital o

Texto actual	Modificación al texto
	electrónica certificada de ambas partes. Artículo 30 qui. En contratos realizados por medio electrónicos, el consumidor tiene un plazo de 5 días para devolver un bien o servicio adquirido a través de Internet o de rescindir el contrato, contados a partir de la recepción del bien o servicio, y sin responsabilidad para él; 10 días si se adquirió fuera de la provincia de donde vive y 30 días si lo adquirió fuera del país.
Artículo 50. Potestades de la Comisión Nacional del Consumidor La Comisión nacional del consumidor tiene las siguientes potestades: a) Conocer y sancionar las infracciones administrativas, los incumplimientos de las obligaciones establecidas en el Capítulo V y, en particular, tutelar los derechos de los consumidores, de acuerdo con el artículo 29 de esta ley. b) Sancionar los actos de competencia desleal, mencionados en el artículo 17 de esta ley cuando, en forma refleja, dañen al consumidor. c) Ordenar, de acuerdo con la gravedad de los hechos, las siguientes medidas cautelares, según corresponda: el congelamiento o el decomiso de bienes, la suspensión de servicios o el cese temporal de los hechos denunciados que violen lo dispuesto en esta ley, mientras se dicta resolución en el asunto. d) Ordenar la suspensión del plan de ventas a plazo o de prestación futura de servicios, cuando se viole lo prescrito en el artículo 41 de esta ley. La parte dispositiva de la resolución debe publicarse para que sea del conocimiento general. e) Ordenar, cuando proceda, la devolución del dinero o del producto. Puede fijar, asimismo, un plazo para reparar o sustituir el bien, según corresponda. f) Trasladar, al conocimiento de la jurisdicción ordinaria, todas las prácticas que configuren los delitos perjudiciales para el consumidor, establecidos en el artículo 60 de esta ley. La Comisión nacional del consumidor no tiene competencia para conocer de la anulación de cláusulas abusivas en los contratos de adhesión, conforme al artículo 39 de esta ley,	Incluir atribuciones adicionales: g) Realizar tareas de control y fiscalización para comprobar el cumplimiento de las obligaciones del vendedor. h) realizar procedimientos para llegar a una conciliación o arbitraje (se debe detallar estos procedimientos). i) en casos de proveedores extranjeros, la Comisión se encargará de contactar a éstos proveedores y establecer la coordinación para llevar a cabo los procedimientos de conciliación o arbitraje (es importante estudiar la experiencia de los Organismos de Resolución Extrajudicial de Litigios que funcionan en la Unión Europea).

Texto actual	Modificación al texto
ni del resarcimiento de daños y perjuicios. Estos casos deben ser conocidos solo por los órganos jurisdiccionales competentes.	
Artículo 52. Conciliación Antes del inicio formal del procedimiento y cuando se trate de intereses puramente patrimoniales, la Unidad técnica de apoyo de la Comisión nacional del consumidor debe convocar a una audiencia de conciliación a las partes en conflicto. En casos extraordinarios y según se autorice en el Reglamento, las partes pueden realizar sus presentaciones por cualquier medio que lo permita. En la audiencia de conciliación, el funcionario de la Unidad técnica de apoyo de la Comisión nacional del consumidor debe procurar avenir a las partes proponiéndoles un arreglo y sugiriéndoles la conveniencia de él. En el acta correspondiente, que deben firmar las partes y el funcionario, se debe dejar constancia de todo acuerdo al que lleguen. En el mismo acto, el funcionario debe aprobar el arreglo, salvo cuando sea contrario a la ley. Este arreglo tendrá la misma eficacia de la resolución de la Comisión para promover la competencia en los términos del artículo 61 de esta ley, pero sin recurso ulterior. De no lograrse un acuerdo durante la audiencia de conciliación o si las partes no se presentan a ella, se debe iniciar el procedimiento indicado en el artículo 53 de esta ley.	Incluir un artículo aparte para casos de conciliación de conflictos surgidos entre un consumidor con un proveedor extranjero y en una compra y venta celebrada por medios electrónicos. Tomar la experiencia de los Organismos de Resolución extrajudicial de Litigios de la Unión Europea.
Artículo 53. Procedimiento La acción ante la Comisión nacional del consumidor solo puede iniciarse en virtud de una denuncia de cualquier consumidor o persona, sin que sea necesariamente el agraviado por el hecho que denuncia. Las denuncias no están sujetas a formalidades ni se requiere autenticación de la firma del denunciante. Pueden plantearse personalmente, ante la Comisión nacional del consumidor, por memorial, telegrama u otro medio de comunicación escrita. La Comisión nacional del consumidor siempre evacuará, con prioridad, las denuncias relacionadas con los bienes y los servicios consumidos por la población de menores	Incluir un artículo aparte que detalle el procedimiento para casos de conciliación de conflictos surgidos entre un consumidor con un proveedor extranjero y en una compra y venta celebrada por medios electrónicos. Tomar la experiencia de los Organismos de Resolución extrajudicial de Litigios de la Unión Europea.

Texto actual	Modificación al texto
ingresos, ya sea los incluidos en la canasta de bienes y servicios establecida por el Poder Ejecutivo o, en su defecto, los considerados para calcular el índice de precios al consumidor. En este caso, se atenderán con mayor celeridad las denuncias de bienes incluidos en los subgrupos alimentación y vivienda de ese índice. La acción para denunciar caduca en un plazo de dos meses desde el acaecimiento de la falta o desde que esta se conocía, salvo para los hechos continuados, en cuyo caso, comienza a correr a partir del último hecho. La Unidad técnica de apoyo debe realizar la instrucción del asunto. Una vez concluida, debe trasladar el expediente a la Comisión nacional del consumidor para que resuelva. La Comisión nacional del consumidor, dentro de los diez días posteriores al recibo del expediente, si por medio de la Unidad técnica de apoyo, no ordena prueba para mejor resolver, debe dictar la resolución final y notificarla a las partes. Si ordena nuevas pruebas, el término citado correrá a partir de la evacuación de ellas. Para establecer la sanción correspondiente, la Comisión nacional del consumidor debe respetar los principios del procedimiento administrativo, establecidos en la Ley General de la Administración Pública.	
Artículo 54. Sanciones La Comisión Nacional del Consumidor debe conocer y sancionar las infracciones administrativas cometidas en materia de consumo, estipuladas en esta ley, sin perjuicio de la responsabilidad penal o civil correspondiente. Según la gravedad del hecho, las infracciones cometidas en perjuicio de los consumidores deben sancionarse con multa del siguiente modo: **a)** De una a diez veces el menor salario mínimo mensual establecido en la Ley de Presupuesto Ordinario de la República, por las infracciones indicadas en los incisos d), e), f), j) y n) del artículo 31 y en el artículo 35 de esta ley. **b)** De diez a cuarenta veces el menor salario mínimo mensual fijado en la Ley de Presupuesto Ordinario de la República, por las infracciones mencionadas en los incisos b), h), i), k), l) y m) del artículo 31 de la	Agregar las sanciones para las infracciones indicadas en los incisos p) a la z) del artículo 31. Así como los artículos 39 bis, ter, cuat, qui sobre contratación electrónica.

Texto actual	Modificación al texto
presente ley. Debe aplicarse el máximo de la sanción administrativa indicada en el párrafo anterior cuando, de la infracción contra esta ley, se deriven daños para la salud, la seguridad o el medio ambiente, que ejerzan un efecto adverso sobre los consumidores. ***(Así modificado por el artículo 1, inc. c) de la ley No. 7854 del 14 de diciembre de 1998.)***	
Artículo 55. Arbitraje En cualquier momento y de común acuerdo, las partes pueden someter su diferendo, de forma definitiva, ante un árbitro o tribunal arbitral, para lo cual deben cubrir los gastos que se originen. Las partes pueden escoger al arbitro o al tribunal arbitral de una lista-registro que, al efecto, debe llevar la Comisión nacional del consumidor. Los árbitros pueden cobrar honorarios por sus servicios. Las personas incluidas en la citada lista deben ser de reconocido prestigio profesional y contar con amplios conocimientos en la materia.	Incluir un artículo que detalle el procedimiento para un arbitraje en los casos de conflictos originados de una compra y venta electrónica. Tomar la experiencia de los Organismos de Resolución extrajudicial de Litigios de la Unión Europea. También sería importante incorporar la posibilidad del arbitraje por medios electrónicos o telemáticos para agilizar el proceso de solución de conflictos.

Capítulo 8. Propuesta de Proyecto de Ley Marco de Protección del Consumidor

Esta propuesta de ley está pensada para que sea acogida por un grupo de países, ya sean: de una región, que conforman un grupo económico, que tienen relaciones comerciales, que conforman el grupo de la ONU, OCDE, OMC u otra organización internacional.

La solución en materia de comercio electrónico debe ser a nivel global o mundial, puesto que este tipo de comercio no tiene límites geográficos, no conoce distancias ni fronteras, por lo tanto debe encontrarse mecanismos que permitan un adecuado desarrollo de este comercio sin perjuicio de los consumidores.

Los países tienen su propia normativa de protección al consumidor, y se ha revisado la normativa existente con relación al comercio electrónico, protección a la privacidad y seguridad y contratación electrónica.

Se ha observado el hecho de que la normativa de los distintos países tienen diferencias entre sí, algunas han considerado el elemento electrónico en sus leyes, otras no, y lo relacionado con el consumidor tiene grandes vacíos en materia de comercio electrónico, privacidad y contratación electrónica.

De todo el estudio anterior, y acogiendo las recomendaciones indicadas en cada uno de los apartados, además de revisar detalladamente las normativas analizadas, se ofrece a continuación una propuesta de Ley Marco de Protección del Consumidor incluyendo el contexto del comercio electrónico para que sea acogida por países de un grupo regional o mundial.

La propuesta se basa en el estudio realizado y en una propuesta de Giraldo (1989), y se previene que hace falta realizar otros estudios para complementar el ámbito de aplicación de la propuesta de ley, pues solo incluye lo relacionado con el comercio electrónico a través de página Web por Internet, la relación de consumo Empresa-

Consumidor (B2C) y para personas físicas o jurídicas de derecho privado que actúan como proveedor o productor.

Además dentro de esta propuesta es todavía necesario reglamentar la integración, organización, potestades y funcionamiento de la Comisión Internacional de Controversia así como el Sistema de Intercambio Rápido de Información.

Como se mencionó anteriormente, la solución debe ser a nivel de grupos de países, es necesario lograr conformar un grupo de países interesados en resolver la problemática del consumidor en el contexto global incluyendo lo relacionado al comercio electrónico. Ya existe los grupos de trabajo de la CNUDMI, OCDE, OMC que han trabajado durante años sobre estos temas, este podría ser el espacio para estos análisis y planteamientos de soluciones.

Por lo tanto, y a sabiendas que todavía hace falta incluir otros aspectos ya mencionados, se presenta en el anexo 9 una propuesta de ley como base para una mayor discusión a nivel de grupos de países.

Capítulo 9. Conclusiones Generales, Recomendaciones y otras Áreas de Investigación

Después de todo un exhaustivo análisis de la situación jurídica del comercio electrónico, se llega a las siguientes conclusiones y recomendaciones.

El desarrollo de las tecnologías de comunicación e información da la oportunidad para todos los usuarios de realizar negocios a nivel global a través de Internet. Para aprovechar al máximo los beneficios de esta nueva modalidad de comercio, se requieren normas y la colaboración de todos los actores involucrados. Indica Maclay (2001) que la experiencia sugiere la importancia de la interacción entre los sectores público, privado, entes académicos y sin fines de lucro para fortalecer mecanismos de mercado y retroalimentación.

Es posible obtener el beneficio máximo de esta nueva modalidad de comercio si se establecen normas, en donde todos los actores involucrados deben colaborar para que se logre aprovechar las grandes posibilidades de este nuevo ambiente.

Por un lado, las empresas que venden por Internet deben publicar información clara y precisa a los usuarios, tener un código de conducta, y no esperar que el Estado legisle en todos los ámbitos.

Además, los proveedores de bienes y servicios, deben por su propia cuenta crear códigos de ética y ser los vigilantes de la aplicación de las reglas de respeto a los consumidores.

Por otro lado, el Estado tiene el deber de garantizar el desarrollo de la nación promoviendo un comercio electrónico acorde con la ley. En materia de regulación, le corresponde al Estado tomar la iniciativa para garantizar la protección de las partes, y ésta debe ser coordinada a nivel internacional para que no se creen reglas nacionales incompatibles que fragmenten los mercados regionales y globales.

Algunas áreas que deben ser de acción gubernamental son: la protección de los consumidores, incluyendo los aspectos de privacidad de la información personal, el cumplimiento de los contratos, la educación y concientización de los ciudadanos, acceso a la solución de controversias oportuna, reparación de daños y cooperación internacional.

Existe ya grupos de países que han creado una instancia internacional para la defensa del consumidor como la eConsumer.gov, un esfuerzo conjunto para reunir y compartir quejas sobre comercio electrónico transfronterizo. El proyecto tiene dos componentes: un sitio Web público en diversos idiomas y un sitio Web gubernamental de acceso restringido y protegido con clave. El sitio público provee información general en torno a la protección al consumidor en todos los países que pertenecen a la Red Internacional de Protección al Consumidor y Aplicación de la Ley, información para establecer contacto con las autoridades de protección al consumidor de dichos países y un formato de queja electrónico. Toda la información está disponible en inglés, francés, alemán y español. Los países que forman esta Red son: Alemania, Australia, Austria, Bélgica, Canadá, Czech Republic, Dinamarca, Estonian, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Japón, Latvia, Lituania, Luxemburgo, Malta, México, Países Bajos, Nueva Zelandia, Noruega, Polonia, Portugal, República Eslovaca, República de Corea, España, Suecia, Suiza, Reino Unido, Estados Unidos, Comisión Europea y la OCDE.

En relación a los derechos de los consumidores, ver anexo 1 Cuadro comparativo de las legislaciones sobre Derechos del Consumidor, los países analizados incluyen en sus leyes normas que abarcan todos los derechos, no obstante, en el entorno del comercio electrónico, debiera agregarse el derecho al acceso a Internet, más aún, el derecho a participar en el mundo interconectado.

Por otro lado, el consumidor debe tomar precauciones cuando compre por Internet para asegurar una compra satisfactoria. Una participación activa por su parte le permitirá informarse sobre su protección jurídica y conocer sus derechos y deberes en una relación comercial electrónica.

El consumidor debe informarse para conocer si la empresa es real y si es confiable, cuáles son los servicios que brinda, las garantías, posibilidades de devolución, costos reales que incluya el transporte, impuestos u otros, formas de pago. El consumidor debe informarse sobre las medidas de seguridad que ofrece la empresa con relación a sus datos personales, si tiene derechos sobre ellos y cuáles son. Un control activo por parte de los consumidores puede lograr erradicar los sitios en Internet que no ofrezcan calidad y seguridad deseada.

El consumidor debe verificar la distancia que existe entre el domicilio físico del sitio comercial y su domicilio, aún si para Internet la noción de distancia es virtual para correos la distancia es bien real, y es el consumidor quien paga los gastos inherentes al envío. El consumidor debe tomar ciertas medidas de seguridad como la verificación de que está utilizando un servidor seguro. Además puede verificar algunos de los datos del Comercio; si el comercio da su dirección y/o su número de teléfono, puede verificar la autenticidad de los mismos. Puede verificar también, la utilización del localizador de recursos, (URL, Uniforme Ressource Locator); si un documento tiene seguridad la dirección del documento es https://..... El consumidor debe conservar los términos y condiciones del contrato, así como todas las transacciones y correos electrónicos que haya enviado al comerciante y recibido de él.

El Estado no debe proteger o regular excesivamente, porque limita el comercio; es necesario buscar un equilibrio y promover lo relacionado a la autorregulación y códigos de conducta en las empresas, industrias y proveedores. El comercio electrónico es un potencial fundamental para el desarrollo de las economías locales, constituye un elemento clave de la competitividad de los países. El Estado, los proveedores de bienes y servicios, las empresas, los consumidores, es decir, todos los actores tienen que participar para identificar objetivos comunes, que puedan aportar un beneficio al desarrollo del comercio electrónico con respeto a los derechos del consumidor y la protección de su intimidad.

El consumidor necesita un mínimo de garantías sobre sus datos personales y los bienes que adquiere, así como una información objetiva y veraz, un marco jurídico claro y una

asistencia jurídica en casos de litigios. Al garantizar al consumidor lo básico de sus derechos, éste podrá aprovechar las oportunidades que le ofrece el mercado global y tendrá la seguridad de que sus intereses están protegidos, y por el otro lado, las empresas tienen un potencial de venta reflejado en la gran población consumidora del mundo, que apenas un número insignificante están incursionando en el mundo electrónico.

En todos los países se deben respetar un mínimo de seguridad de los productos que circulan para que pueda haber una libre circulación de mercancías. El libre mercado o mercado único, no debe violar ni debilitar las normas de protección a los consumidores.

Para que un ciudadano pueda comprar productos o contratar servicios a través de Internet con toda confianza como si lo hiciera en su propio país, es necesaria una normativa uniforme a nivel internacional, que tome como parámetro el nivel de protección del país con los estándares más altos de protección. Este propósito no es posible garantizarlo, si cada país tiene normas de seguridad y de protección al consumidor con grandes diferencias entre ellas. Y una normativa para grupos de países solo es posible con un trabajo conjunto y coordinado a nivel Organismos Internacionales.

Se requiere entonces de normas y condiciones necesarias mínimas y comunes en todos los países para que pueda haber una adecuada libre circulación de bienes y servicios. Para ello se debe impulsar la adopción de una normativa en materia de protección al consumidor, que sirva de guía, y que su aplicación sea garantizada en todos los países.

La normativa da un mínimo de garantías en la protección al consumidor en los países de todo el mundo y asegura un mercado más sano y transparente, amplía la oferta y da confianza al ciudadano para adquirir bienes y servicios provenientes de los demás países, asegurando un crecimiento del mercado a los niveles esperados.

Algunos asuntos que esta normativa debe regular adecuadamente son: la publicidad, la información que se da al consumidor, los contratos de adhesión, las garantías, la responsabilidad por producto defectuoso, los mecanismos de solución de conflictos, la seguridad y cumplimiento de los principios de protección de los datos personales, así como establecer normas sobre los casos especiales más relevantes para garantizar una adecuada circulación de bienes y servicios.

Una adecuada regulación sobre responsabilidad por producto defectuoso permite al consumidor iniciar un proceso administrativo o judicial y conseguir un resarcimiento justo por los perjuicios causados por un bien introducido al mercado, sin encontrar trabas jurídicas que impidan el efectivo ejercicio del derecho, esto último sólo es posible si se establecen mecanismos efectivos de solución de conflictos.

Igualmente la existencia de garantías en productos durables y las formas de hacerla efectiva, la protección de las cláusulas abusivas en los contratos de adhesión, o el derecho a rescindir un contrato hecho a distancia cuando el bien entregado no corresponde a las características ofrecidas o con las expectativas del consumidor, son aspectos que el consumidor tendrá en cuenta para adquirir bienes producidos en otros países, impulsando la integración económica y la circulación de bienes.

Por otro lado, lo concerniente a la protección de datos personales cobra importancia en esta nueva era, donde el desarrollo de las tecnologías de información y comunicación hacen vulnerable la intimidad de las personas. La normativa que se adopte debe velar por el cumplimiento de las garantías de protección de la persona frente al tratamiento de sus datos personales. Y ofrecer mecanismos ágiles y eficaces para perseguir a los infractores.

Alcanzar los estándares de protección de datos es una importante condición para participar en las negociaciones comerciales con importantes mercados como los de la Unión Europea, cuyas directivas y normativas exigen que los países con los cuales se tengan relaciones comerciales demuestren que tienen estándares similares de protección a los ofrecidos en los países miembros de la comunidad europea. En

momentos en que el país (en conjunto con las otras naciones centroamericanas) se encuentra negociando un tratado de libre comercio con los Estados Unidos y con el posible lanzamiento del ALCA a mediano plazo, así como un posible tratado de libre comercio con la Unión Europea, la necesidad de establecer un adecuado y moderno estatuto jurídico de la privacidad resulta a todas luces indispensable. De lo contrario, podría Costa Rica adquirir, al cabo de algunos años, la muy poco deseable etiqueta de paraíso del tráfico de datos personales, con insospechables consecuencias en nuestras pretensiones de ser parte del mercado global y una significativa pérdida de credibilidad en los foros internacionales que siempre han visto a esta Nación como un caso excepcional dentro del área (proyecto de Ley 15178, 2001).

Es necesario establecer explícitamente el procedimiento que debe realizar el consumidor para reclamar cuando una garantía tutelada por el Proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales sea violada. Este procedimiento debe incluir los casos en que el proveedor se encuentre en el extranjero. Debe estudiarse los mecanismos que ha utilizado la Unión Europea para que el grupo de países de Europa respeten y hagan cumplir las directivas sobre protección de datos establecidas a nivel de la Unión.

Es urgente que el país apruebe el Proyecto de Ley Protección de la persona frente al tratamiento de sus datos personales, incluyendo las modificaciones planteadas, para que haya una efectiva protección de los datos personales, sobre todo en estos tiempos donde el comercio electrónico se desarrolla a pasos agigantados y ya se ha legalizado los documentos electrónicos y firmas digitales en el país. Hasta el momento lo que se tiene es la jurisprudencia que ha aplicado la Sala Constitucional en esta materia.

La normativa a adoptar debe dar capacidad a las autoridades administrativas de cada uno de los países para que puedan efectivamente proteger al consumidor, y tener verdadero poder para velar por el cumplimiento de las normas. Es necesario que puedan imponer sanciones, ordenar el retiro del mercado de un bien de forma preventiva cuando existan indicios serios de que éste representa un peligro para la seguridad, salud o intimidad de las personas, ordenar medidas correctivas, promover

los mecanismos alternativos de solución de conflictos, y en la medida de las posibilidades, que puedan directamente solucionar el problema al consumidor, ordenando válidamente al proveedor a favor de éste el cumplimiento de la garantía. El procedimiento administrativo debe resolver efectivamente el problema planteado por un consumidor, y no convertirse en un obstáculo más que vuelva inalcanzable su derecho a reclamar y a ser resarcido.

No se debe invertir la carga de la prueba al consumidor en un procedimiento establecido para la solución de controversias, sino, obligar al proveedor demostrar que el problema se debió a factores ajenos a su responsabilidad.

El desarrollo del comercio electrónico transfronterizo ha incrementado las posibilidades de infracciones de derechos de los consumidores en el ámbito internacional. Por lo tanto, a nivel global, es necesario que se establezcan normas sobre Jurisdicción Internacional, que permitan al consumidor demandar el cumplimiento de sus derechos en el lugar de su domicilio.

La propuesta de Normativa "Proyecto de Ley Marco de Protección del Consumidor" trata de incluir todos y cada uno de los elementos anteriores, con el fin de que sea una propuesta para que sea discutida y adoptada por todos los países interesados en lograr un adecuado desarrollo del comercio electrónico con respeto a los derechos de los consumidores.

La propuesta incorpora normas para cada uno de los temas examinados, extrayendo de las leyes nacionales lo más importante, y llenando los vacíos encontrados. Es una propuesta de guía para trabajar en esta materia con el fin de lograr un marco común normativo para una adecuada protección al consumidor.

La idea de la CNUDMI de proporcionar leyes modelos es una buena idea. Es posible entonces que organismos internacionales propongan leyes modelos y entidades reguladores a los cuales los países se adhieran mediante tratados internacionales. Esto

permitiría uniformar los criterios internacionales que asegurarían los derechos de los consumidores en las contrataciones electrónicas internacionales.

En cuanto a controversias, la normativa debe contemplar la creación de mecanismos extrajudiciales de solución de conflictos en materia de protección al consumidor y protección de sus datos personales, que sean ágiles, expeditos y económicos tanto para los consumidores como para la industria y para los comerciantes, aún cuando los conflictos sea en otros países diferentes al del consumidor.

En este sentido, sería importante revisar el Sistema de Resolución Alternativa de Litigios (Resolución del Consejo, de 25 de mayo del 2000), implementado en la Unión Europea, así como la legislación española referente al Sistema Arbitral de Consumo, establecido en el Real Decreto 636/93, la Ley de Arbitraje de 2003 y demás normas aplicable.

Este sistema arbitral español tiene como finalidad atender y resolver con carácter vinculante y ejecutivo para ambas partes las quejas o reclamos de los consumidores y usuarios, en relación con los derechos legalmente reconocidos, todo ello sin perjuicio de la protección administrativa y la tutela judicial (Vega, 2005).

Actualmente las normas de derecho internacional privado son la guía para resolver conflictos, así como los Códigos Comerciales y Civiles, entre otros. Pero debido a que en muchos casos los problemas a que se ven sujetos los consumidores son de montos económicos muy bajos, además el comercio electrónico se caracteriza por la gran cantidad de transacciones internacionales, sería una pérdida de tiempo y de recursos económicos acudir a la jurisdicción civil para resolver esos problemas. Es necesaria la creación de nuevos mecanismos que representen la realidad actual, por ello la creación de organismos con función de tribunales en Internet puede ser una opción a analizar.

Bruce (2002) sugiere fortalecer los sistemas de mediación, conciliación y arbitraje y adaptarlos al mundo virtual, indica que los conflictos deben resolverse fuera de los tribunales de juicio e incluso de los mismos tribunales arbitrales.

Por último, las secciones correspondientes al Análisis de la Ley 8454 y del Proyecto de Ley 15178 de Protección de la Persona frente al tratamiento de sus Datos Personales, así como el capítulo de Propuesta de modificaciones a la Ley 7472, se plantearon observaciones que son importantes que se tomen en cuenta para que se gestione ante las instancias que corresponda, las modificaciones indicadas.

Otras áreas de investigación

Junto con el desarrollo de los derechos del consumidor y las obligaciones del proveedor, se hace necesario desarrollar las siguientes actividades por parte del Estado:

i- Fortalecer los órganos existentes o crear nuevos órganos con amplias facultades para conocer y perseguir los atentados a los derechos de los consumidores en el comercio electrónico;

ii- Crear efectivos mecanismos de solución de controversias originadas entre proveedores y consumidores;

iii- Estimular el desarrollo de códigos de conducta y la autorregulación de los proveedores;

iv- Promover programas de educación de los consumidores para que los mismos puedan, entre otras cosas, distinguir entre proveedores serios y establecidos, y aquellos que no lo son, así como utilizar mecanismos seguros de pago de sus compras por Internet.

También es necesario revisar lo relativo a la protección del consumidor en relación con las personas físicas y jurídicas de derecho público. Se ha analizado la normativa poniendo énfasis a la relación de consumo de las personas con negocios o empresas de derecho privado, y siempre pensando que la empresa tiene un fin último como lo es su propio beneficio y que este sea lo mayor y mejor posible. Mientras que una institución o empresa de derecho público, su fin último es el mismo que persigue el Estado de bienestar para beneficiar a la mayor población de ciudadanos. Por tanto, una investigación posterior debería revisar si las normas existentes permiten una adecuada

protección del consumidor en su relación con las empresas del Estado, o personas físicas y jurídicas de derecho público.

Otra área de investigación es con relación a los mecanismos de solución de controversias en casos de conflictos que no puedan ser resueltos en el país del consumidor. Es necesario analizar la posibilidad y la viabilidad de una Comisión Internacional de Controversias y diseñar procedimientos o mecanismos para una ágil resolución de conflictos que respete la legislación y jurisdicción aplicable. Es importante considerar la experiencia de los Organismos de Resolución Alternativa de Litigios que funciona en la Unión Europea y el Sistema Arbitral español.

También es importante analizar la experiencia de la Red Internacional de Protección al Consumidor y Aplicación de la Ley, o más bien, analizar la conveniencia de que Costa Rica se una al grupo de países que forman esta Red, para proteger al consumidor costarricense de los fraudes internacionales por Internet.

Otra área de investigación es sobre los "cookies" y el derecho a la privacidad. Cómo este tipo de mecanismo puede ser regulado para respetar el derecho a la privacidad de las personas.

El estudio analizó sólo lo relativo a las compras y ventas realizadas a través de una página Web por Internet, y en relación con personas físicas o jurídicas de derecho privado. Es necesario investigar sobre las otras formas de comercio como: subasta electrónica, ventas por correo electrónico, contratos perfeccionados mediante el empleo de Chat o videoconferencia. Y todo lo relacionado con comercio electrónico con la Administración Pública del Estado.

También es importante investigar las posibilidades de uniformar la normativa relacionada con las firmas y certificados digitales y documentos electrónicos, con el fin de estandarizar a nivel de grupos de países lo relativo al ámbito de aplicación, definiciones y conceptos, alcances, procedimientos, prohibiciones, sanciones, autoridades de certificación, etc. El comercio electrónico permite el intercambio

comercial a nivel internacional, y es necesario dar la misma protección jurídica a todos los que participan en ella, y esto solo es posible si existiera una sola normativa para todos o más bien, la misma normativa para todos, independiente del país de origen.

La naturaleza extraterritorial del fenómeno social que ha provocado el desarrollo de las tecnologías de información y comunicación, hace necesario pensar en soluciones coordinadas e integradas. Muchas experiencias normativas han generado resultados eficaces que tienen que ser tomadas en cuenta como posibles modelos a seguir, adecuándolos a las realidades propias, sin perder el contexto de una integración subregional y regional, pues en principio la Sociedad de la Información es un fenómeno transfronterizo. Esto hace importante el trabajo en torno a la legislación y jurisdicción aplicable en los casos que impliquen una diversidad de países en simultáneo (Iriarte, 2005, p.9).

Esta afirmación es aplicable, no sólo al tema de la regulación del comercio electrónico y firmas electrónicas, sino que también son necesarias soluciones coordinadas e integradas con relación a la normativa de protección al consumidor, por ser el consumidor un elemento importante en las relaciones de comercio electrónico; y en la materia de protección de los datos personales, pues en estas relaciones de comercio indudablemente se requiere del suministro de información personal.

Por lo tanto, un área de investigación lo será el diagnóstico y análisis de la situación de los países de una región o subregión de las posibilidades de armonización de sus normas (de protección al consumidor, protección de datos personales, comercio electrónico y firmas digitales) que permitan un desarrollo adecuado del comercio electrónico sin detrimento de los derechos de los involucrados.

Sugiere Iriarte (2005) que para que haya un verdadero desarrollo de la Sociedad de la Información, es necesario el diseño y desarrollo de políticas regionales, subregionales y nacionales que utilicen las tecnologías de información y comunicación para el desarrollo; y el desarrollo normativo tiene que estar basado en un desarrollo de políticas de largo plazo, que enmarquen el uso de las normas para el desarrollo.

Por último, otro campo de investigación es con relación a la brecha digital, es decir, cómo los Gobiernos pueden promocionar el desarrollo de las telecomunicaciones que permita a todos los sectores de la sociedad acceder a la información y al conocimiento, sin discriminación de ningún tipo.

En el caso de Costa Rica, ya hay una serie de trabajos adelantados con la mira de disminuir la brecha digital existente y avanzar en el desarrollo de las TIC's: el proyecto de Centros de Comunicación Inteligentes del Ministerio de Ciencia y Tecnología; el proyecto de alfabetización en informática que se viene dando desde hace varios años liderada por la Fundación Omar Dengo; el proyecto de ley de acceso a Internet, que establece como derecho el acceso a Internet y a las nuevas tecnologías de telecomunicación y que tuvo dictamen de mayoría por la Comisión Permanente de Asuntos Económicos, el 15 de mayo de 2001; la propuesta de Estrategia Siglo XXI, donde una de las metas es la universalización del acceso a la tecnología por toda la población costarricense; y el proyecto de Gobierno Digital que propone incrementar el acceso en las relaciones entre el Gobierno, las personas y los recursos disponibles, para promover la competitividad y productividad del país y mejorar la relación del Gobierno con los ciudadanos.

Es necesario hacer una revisión de lo actuado para determinar las fallas y lo que hace falta para que esa brecha digital se disminuya, sobre todo, revisar las políticas públicas de desarrollo de las TIC's, revisar la normativa existente a nivel nacional e internacional, y considerando que los procesos se están globalizando a raíz del desarrollo de las mismas TIC's, revisar los trabajos de armonización de leyes de los diferentes grupos de países y en los diferentes temas de regulación: protección al consumidor, comercio electrónico, firmas digitales y certificados digitales, protección de datos, etc.

Capítulo 10. Bibliografía

Abarca, S. *(2004). Diseños Cualitativos en la Investigación Gerencial.* Material didáctico del curso. III-2004. Doctorado en Ciencias de la Administración. UNED. 2004.

Abarca, S. (2004). *Los métodos cualitativos de investigación. Más allá de la investigación profesional.* Material didáctico del curso Diseños Cualitativos en la Investigación Gerencial. III-2004. Doctorado en Ciencias de la Administración. Costa Rica: UNED. Setiembre 2004.

Acuña, C. (2006). *En trámites en línea: Costa Rica transó 43 millones de dólares con tarjetas Visa.* La Prensa Libre. 2 de marzo de 2006, pag. 8. San José, Costa Rica.

Adame, J. (1994). *El Contrato de Compraventa Internacional*. México: Mc Graw Hill.

Agüero, Esteban; Echeverría, Leonor. (2002). *Comercio electrónico: el contrato de intercambio electrónico de datos (EDI) entre empresarios: estudio de Derecho comparado.* Tesis de Licenciatura en Derecho. Facultad de Derecho. Universidad de Costa Rica. Costa Rica.

Alonso Conde, Ana Belén. (2002). *Comercio Electrónico: antecedentes, fundamentos y estado actual.* Madrid: DYKINSON.

Álvarez, M; Ayala, J; Chaves, G.; Garat, C.; Landaverde, E.; López, N. y otros. (2005). *Firma digital y contratos electrónicos.* Documento conceptual para la legislación en la Era de la Información. Iniciativa GLIN AMERICAS. Banco Interamericano de Desarrollo. Consultado el 25 de diciembre de 2007 en http://209.85.207.104/search?q=cache:_Zk0vYYUztUJ:www.asamblea.go.cr/BIBLIO/glin/trabajo%2520cuarta%2520jornada/Firma%2520Digital%2520y%2520Contratos%2520Electr%C3%B3nicos.pdf+Firma+digital&hl=es&ct=clnk&cd=6&gl=cr

Amor, D. (2000). *The E-business (R)Evolution: Living and Working in an Interconnected World.* Prentice-Hall PTR.

Amor, Daniel. (2002). *E-business*. Argentina: Prentice Hall.

Arata Salinas, Angel Alfonso. 2004). *Las nuevas tecnologías de la información y la problemática jurídica del comercio electrónico***.** Consultado el 6 de julio de 2004 en http://sisbib.unmsm.edu.pe/bibvirtual/tesis/Human/Arata_S_A/concl.htm

Avellán, Juan. (octubre 1997). *Recopilación de legislación, infraestructura, estándares y artículos sobre firma digital.* Consultado el 8 de diciembre de 2004. http://www.qmw.ac.uk/~tl6345/index.htm.

Avellán, Juan. (Febrero 1997). *Lista de autoridades de certificación por países*. Consultado el 8 de diciembre de 2004 en http://www.qmw.ac.uk/~tl6345/ca.htm.

Aced, E. (2005). *Transferencias Internacionales de Datos. Protección de Datos de Carácter Personal en Ibeoramérica*. II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.105-127.

Argüello, F. (2005). *Protección de datos personales: la directiva comunitaria, su influencia y repercusiones en Latinoamérica.* II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.69-104.

Arias, B. (2002). *Vacíos legales en Costa Rica por el uso de la Red: El "e-practice".* Revista de Ciencias Jurídicas. No. 97. San José: Colegio de Abogados y Facultad de Derecho de la Universidad de Costa Rica.

Balarini, Pablo. (2003). *Derechos fundamentales de los individuos y comercio electrónico.* Comercio electrónico: Análisis jurídico multidisciplinario. Uruguay: B de F Ltda. p. 97-106.

Barbosa Huerta, Miguel (PRD) (2001). *Iniciativa con proyecto de Decreto que expide la Ley Federal de Protección de Datos Personales*. Publicación en Gaceta Parlamentaria: Septiembre 7, 2001. México. Consultado el 11 de noviembre de 2006 en http://www.cddhcu.gob.mx/servicios/datorele/cmprtvs/1po2/set/2.htm

Barrantes, Rodrigo. (2003). *Investigación, un camino al conocimiento, un enfoque cuantitativo y cualitativo*. San José, Costa Rica: EUNED.

Barriuso Ruiz, C. (2002). *La contratación electrónica*. 2 ed. Madrid: Ed. Dykinson.

Barth, J. F. (2005). *Marco Normativo y Jurisprudencial de la Protección de Datos en Costa Rica.* II Encuentro Iberoamericano de Protección de Datos. La Antigua-Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.261-270.

Bauzá, Marcelo. (2003). *Firma electrónica y entidades certificadoras.* Comercio electrónico: Análisis jurídico multidisciplinario. Uruguay: B de F Ltda. p. 73-96. 2003.

Beltrán, M. (1985). *Cinco vías de acceso a la realidad*. REIS, Núm. 29, Madrid, CIS.

Berrocal Lanzarot, Ana Isabel. (2004). *Responsabilidad de los prestadores de servicios de la sociedad de la información.* V Congreso de Derecho e Informática: "Sociedad y tecnologías. Los desafíos de la economía digital". España. Consultado el 7 de agosto de 2004 en http://sdi.bcn.cl/e-derecho/Ponencias/ver_po/ponen10.

Bruce, O. (2002). *Comercio electrónico y derechos del consumidor.* Revista de Ciencias Jurídicas. No. 99. Setiembre-Diciembre 2002. Costa Rica: Colegio de Abogados – Facultad de Derecho de la Universidad de Costa Rica. P. 153-169.

Burgos, Andrea. (2003). *Los Contratos con el Consumidor en Internet. El Contrato por medios electrónicos*. Universidad Externado de Colombia. p. 249-311.

Carvajal, T., Jiménez, S. (2002). *Cláusulas abusivas en contratos de adhesión en Internet.* Tesis para optar por el grado de Licenciatura en Derecho. Facultad de Derecho. Costa Rica: Universidad de Costa Rica.

Castañeda Rivero, Juan Manuel. (Nov. 2000-2001). *Legislación del comercio electrónico.* Revista electrónica Razón y Palabra. Núm. 20. Consultado el 8 de agosto de 2004 en http://www.razonypalabra.org.mx/anteriores/n20/20_jcastaneda.html.

Chirino, A., Carvajal, M. (2003). *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. Revista Costarricense de Derecho Constitucional. Tomo IV. Costa Rica: Investigaciones Jurídicas S.A. Julio del 2003. p.195-287.

Coase, Ronald (1960). El problema del costo social. Revista Estudios Públicos No.45, 1992. Centro de Estudios Públicos. Santiago de Chile. Consultado el 10 de febrero de 2008 en http://www.cepchile.cl/cgi-dms/procesa.pl?plantilla=/base.html&contenido=categoria&id_cat=656

Coase, Ronald (1937). The nature of the firm. Consultado el 10 de febrero de 2008 en http://www.cerna.ensmp.fr/Enseignement/CoursEcoIndus/SupportsdeCours/COASE.pdf.

Computer Segurity Institute. (2005). *Estudio de Seguridad y Delitos Informáticos 2000*. Consultado el 23 de agosto de 2005 en http://www.gocsi.com/

Cuestiones Mundiales. (Octubre 1997). *Estructura de comercio electrónico mundial*. Publicación Electrónica del USIS, Vol. 2, No. 4. Consultado el 6 de agosto de 2004 en http://usinfo.state.gov/journals/itgic/1097/ijgs/gj-12.htm.

Davara & Davara Asesores Jurídicos. (2004). *Fiscalidad electrónica*. Consultado el 6 de agosto de 2004 en http://www.davara.com/preguntas/fiscalidad.html.

Dávila, Andrés. (1999). *Las perspectivas metodológicas cualitativa y cuantitativa en las ciencias sociales: debate teórico e implicaciones praxeológicas*. En Métodos y técnicas cualitativas de investigación en ciencias sociales. Madrid, p. 69-83.

DCSSI (2004). *Guía para la elaboración de una política de seguridad para el sistema.* París. Dirección Central de la Seguridad de los Sistemas de Información. 3 de Marzo 2004. Consultado el 12 de julio de 2007 en www.ssi.gouv.fr/es/confianza/documents/methods/pssi-section4-referencesssi-2004-03-03_es.pdf

De Téramond Peralta, Carmen; Fernández Fonseca, Mónica. (2002). *Concepto, Valor jurídico y regulación de la Firma Digital en Costa Rica.* Tesis de Licenciatura. Facultad de Derecho. Universidad de Costa Rica. Costa Rica.

Del Peso Navarro, Emilio; Ramos González, Miguel Ángel. (1994) *Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas*. Madrid: Ediciones Díaz de Santos, S.A.

Diario del Navegante. (1998). *La OMC estudia regular fiscalmente el comercio en Internet*. 9-2-1998. Consultado el 7 de agosto de 2004 en http://www.el-mundo.es/navegante/98/febrero/19/ocm.html.

Diario del Navegante. *Bruselas apoyo el comercio electrónico sin impuestos específicos.* 8-7-1997. Consultado el 10 de agosto de 2004 en http://www.el-mundo.es/navegante/97/julio/08/nimpuestos.html.

Dirección Tecnología Educativa y Comunicación Visual. (Octubre 2001). *Delincuencia Informática*. Universidad Tecnológica Metropolitana. Chile. Consultado el 10 de agosto de 2004 en http://www.utem.cl/cyt/derecho/delitos.html.

Duer, W. (2007). *Los bytes al poder*. Revista Suma. No. 159. Agosto 2007. Suma Media Group.

Echegaray Rodríguez, Edgar. (2001). *Comercio electrónico y una necesaria regulación para la protección de los derechos del consumidor*. Tesis de grado para optar por el título de Licenciatura en Derecho. Facultad de Derecho. Universidad de Costa Rica. Costa Rica.

Escobar Espinar, Modesto. (2000). *El comercio electrónico. Perspectiva presente y futura en España.* Madrid. Fundación Retevisión.

eConsumer.gov (2005). *Tendencias de las quejas*. Consultado el 10 de febrero de 2007 en http://www.consumer.gov/econsumer/english/contentfiles/pdfs/PU15%20Jan-Dec%202005.pdf

Estrategia Siglo XXI. (2007). Costa Rica. Consultado el 3 de setiembre de 2007 en http://estrategia.or.cr/content/view/1/5/lang,es/

Fernández Gómez, Eva. (2002). *Comercio Electrónico*. España: Mc Graw Hill.

Ferreira, R. (2003). *Desarrollo de confianza en Internet, en manos de terceros*. Consultado el 24 de mayo de 2007 en http://www.iese.edu/es/files/5_8412.pdf

Fonseca, P. (2007). *Firma digital llegará por medio de los bancos*. La Nación. 26 de abril de 2007. Página 10A. San José, Costa Rica.

Fonseca, P. (2007). *Penetración de banda ancha creció 26% en primer semestre del 2007*. La Nación. 2 de noviembre de 2007. Página 20A. San José, Costa Rica.

Fundación Omar Dengo. (2007). Página de la Fundación. Costa Rica. Consultado el 3 de setiembre de 2007 en http://www.fod.ac.cr/

Garfinkel, S. y Spafford, G. (1997). *Web Security and Commerce. Risks, Technologies and Strategies.* Ed. O´Reilly.

Giraldo, Alejandro (1989). *Estado de situación de la Protección al consumidor en el ámbito nacional y comunitario: una propuesta de decisión 1989-2002*. VII Programa de Pasantías CAN – BID/INTAL. Biblioteca digital andina. Colombia. Consultado el 13 de setiembre de 2006 en http://www.comunidadandina.org/bda/docs/CAN-PAS-0003.pdf#search=%22Protecci%C3%B3n%20consumidor%20Colombia%22

González Pons, Esteban. *Entrevista*. 2001. Consultado el 6 de agosto de 2004 en http://iblnews.com/varios/lssi/ponsabc.htm.

González, Rafael; et. al. (2000). *Propuesta de estrategias para el desarrollo del Comercio electrónico en Costa Rica.* Proyecto de tesis. Departamento de Administración de Empresas. Instituto Tecnológico de Costa Rica. Costa Rica.

Gourion, P.A.; Ruano-Phillippeau, M. (2003). *La droit de Internet dans l'entreprise*, París: Ed. L.G.D.J.

Guisado, A. (2004). *Formación y perfección del contrato en Internet*. Madrid: Marcial Pons, Ediciones Jurídicas y Sociales, S.A.

Fonseca, P. (2007). *Firma digital llegará por medio de los bancos*. La Nación. 26 de abril de 2007. Página 10A. San José, Costa Rica.

Guerrero, O. (1986). *La teoría de la administración pública*. México: Harla. Integro.

Hernández, Roberto; et. al. (2003). *Metodología de la Investigación*. 3 ed. México: Mc Graw Hill.

Herrera Bravo, Rodolfo. (Setiembre 2003). *La ineficacia del derecho como regulador del comercio Electrónico*. Universidad Central de Chile. Lima, Chile. Consultado el día 7 de agosto de 2004 en http://www.alfa-redi.org/presentaciones/herrera1.pdf.

Hess Araya, Christian.(Febrero 2001). *Comentarios al proyecto de Ley de Firma Digital de Costa Rica*. Consultado el 16 de junio de 2004 en http://www.hess-cr.com/publicaciones/dereinfo/firmadigital.html.

Hess Araya, Christian. (2006). *Retomar la agenda digital*. Periódico La Nación. 2 de abril de 2006. Pag. 36 A. San José, Costa Rica.

H'obbes' Zakon, Robert. (Octubre 2000). *Cronología de Internet de Hobbes v5.0.* Consultado el 23 de febrero de 2005 en http://articulos.astalaweb.com/Internet%20-%20Historia/1_Internet%20-%20Historia.asp.

Hess, C. (2000). *Los contratos Web*. Ponencia presentada al I Congreso Internacional de Derecho e Informática en Internet. Febrero 2000. Consultado el 3 de marzo de 2007 en http://www.hess-cr.com/secciones/dere-info/contrweb.shtml

Irabien, J.F. (2003). *El reconocimiento de certificados digitales extranjeros*. Revista de Derecho Informático Alfa-Redi. No. 60. Julio 2003. Consultado el 2 de setiembre de 2007 en http://www.alfa-redi.org/rdi-articulo.shtml?x=1313

Iriarte, E. (2005). *Estado situacional y perspectiva del derecho informático en América Latina y el Caribe*. CEPAL. Naciones Unidas. Consultado el 28 de agosto de 2007 en http://www.cepal.org/publicaciones/DesarrolloProductivo/5/LCW25/LCW25.pdf

Iturraspe, Urtza; Zaballa, Ibon. (2003). *Introducción a las firmas digitales*. Revista Robotiker, No. 8. Consultado el 6 de diciembre de 2004 en http://revista.robotiker.com/articulos/articulo45/pagina1.jsp

Jované, Lissy. (2004). *Problemas jurídicos del comercio electrónico.* Consultado el 11 de noviembre de 2004 en
http://www.legalinfo-panama.com/articulos/articulos_13a.htm

Kalakota, R. y Whinston, A. (1997). *Electronic Commerce. A Manager´s Guide*. USA: Addison-Wesley.

Landaverde, Melvin; Soto, Joaquín; Torres, Jorge (2000). *Delitos informáticos*. Universidad de El Salvador. Consultado el 5 de julio de 2005 en
http://www.monografias.com/trabajos6/delin/delin.shtml

Lara, F. (2007). *Gobierno financiará computadoras a maestros*. La Nación, 16 de junio de 2007, página 25 A. Costa Rica.

Lewis, E. (2005). *Delitos Informáticos de Costa Rica 2004-2005*. Expedientes en Archivos del Organismos de Investigación Judicial. Sección de Delitos Informáticos. Costa Rica.

Lijphart, A. (Setiembre, 1971). *Comparative politics and the comparative method*. The American Political Sciense Review, V.65, No.3, 682-693. Consultado el 10 de Julio de 2007 en
http://links.jstor.org/sici?sici=0003-0554%28197109%2965%3A3%3C682%3ACPATCM%3F2.0.CO%3B2-I

Loyo, Cristina. (1997). *El impacto económico de la tecnología*. Revista Lania. Año 6, vol 19, 20. Primavera- Verano 1997. Consultado el 20 de enero de 2005 en
http://www.lania.mx/biblioteca/newsletters/1997-primavera-verano/art1.html

Maclay, Colin y otros. (2001). *Preparación Andina para el Mundo Interconectado: Introducción y evaluación regional*. Cambridge: Hardvard University. Consultado el 28 de agosto de 2007 en

http://www.cid.harvard.edu/archive/andes/documents/workingpapers/it/preparaction_andina_mundo_interconectado_maclay.pdf

Magliona, C. (2001). *Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico*. Revista de Derecho Informático. No.34 mayo 2001. Alfa-Redi. Consultado el 11 de noviembre de 2006 en http://www.alfa-redi.org/rdi-articulo.shtml?x=681

Manson, Marcelo. *Legislación sobre delitos informáticos***.** Consultado el 30 de julio de 2004 en http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml.

Mata, Ricardo. (2001). *Delincuencia informática y derecho penal*. Madrid: Edisofer. S.L.

Menéndez, J.C. (2005). *El contrato vía Internet.* Barcelona: J.M. Bosch Editor. 2005.

MICIT (2007). *Centros Comunitarios Inteligentes*. Ministerio de Ciencia y Tecnología. Costa Rica. Consultado el 3 de setiembre de 2007 en http://www.micit.go.cr/cecis/index.html

Molina Mateos, José María. (1994). *Seguridad, información y poder*. Madrid: Incipit Editores.

Monge, B.; Murillo, T. G. (2000). *La seguridad jurídica de la compraventa mercantil por medio de Internet.* Tesis para optar por el grado de Licenciatura en Derecho. Facultad de Derecho. Universidad de Costa Rica.

Morales Avendaño, Karla; Figueroa Loaiza, Manuel. (2003). *Formas Alternativas de Comercio Internacional: La Contratación Electrónica y la Seguridad Jurídica Transaccional.* Tesis de Licenciatura. Facultad de Derecho. Universidad de Costa Rica. Costa Rica.

Moreno, M. (2002). *DERECHO-e Derecho del Comercio Electrónico*. Madrid: Marcial Pons Ediciones Jurídicas y Sociales S.A.

Moya, Ronald. (2006). *Prófugos pagaban $800 por alterar registro de información*. La Nación. Página 12 A. 25 de febrero de 2006. San José, Costa Rica.

Noticiasdot.com. (2004). *Gobierno español prepara proyecto decreto ley para comercio electrónico.* Barcelona. Consultado el 10 de agosto de 2004 en http://www.noticiasdot.com/publicaciones/2003/0903/0109/noticias010903/noticias010903-18.htm.

Mundo-R. (2005). *Historia de Internet.* Consultado el 23 de febrero de 2005 en http://internet.fiestras.com/servlet/ContentServer?pagename=OpenMarket/Xcelerate/Render&c=Articulo&cid=982160102453&pubid=982158432634&MosaicoWebLogicSession=Qh0CYscfi4rsXFKNK93n09sIboXtnRZ4ZaJ1jZhfKK9Hgm1bchmx|-4328663300077665062/167807397/6/6081/6081/6083/6083/6081/-1

Noticiasdot.com. (2004). *Noticias relacionadas del 16 de junio de 2004*. Consultado el 10 de agosto de 2004 en http://www.noticiasdot.com/publicaciones/2004/0604/1706/noticias170604/noticias170604-4.htm.

Ogliastri, E. (2007). *Ocho tendencias en la gestión del entorno*. Revista Summa. No.159. Agosto 2007. Summa Media Group.

Palazzi, P. (2002). *La transmisión internacional de datos personales y la protección de la privacidad.* Argentina: AD-HOC S.R.L.

Peña, Helen; Palazuelos, Silvia; Alarcón, Rosalía. (1997). *Tipos de delitos informáticos reconocidos por Naciones Unidas.* División de Estudios de Posgrado. Facultad de Derecho. México: UNAM. Consultado el 17 de julio de 2004 en http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm.

Pérez, Melba Rocío (2003). *Aspectos generales de la contratación por medios electrónicos. El contrato por medios electrónicos*. Universidad Externado de Colombia. P. 149-178.

Pérez Merayo, Guillermo. (2001). *Comentarios acerca de las deficiencias que presenta el Proyecto de Ley sobre la Firma Digital.* Ponencia presentada a la Jornada para el Desarrollo Archivístico 2001 titulada: "Los Sistemas de Información y la automatización de Archivos". Consultado el 9 de junio de 2004 en http://www.centrodeconocimiento.com/firmadigital/index.htm.

Pilioura, Thomi. *Electronic Payment Systems on Open Computer Networks: A Survey.* Consultado el 5 de diciembre de 2004 en http://cuiwww.unige.ch/OSG/publications/OO-articles/%20TechnicalReports/98/electPayment.pdf

Pinochet, R. (2001). *Contratos electrónicos y defensa del consumidor*. Madrid: Marcial Pons Ediciones Jurídicas y Sociales S.A.

Puente, A. (2005). *Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal*. II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.37-67.

RACSA (2004). *Reglamento autónomo de servicio para la regulación del correo electrónico masivo no deseado.* La Gaceta No.151. 4 de agosto de 2004. Costa Rica. Consultado el 4 de febrero de 2007 en http://www.racsa.co.cr/consejos_navegacion/spam/reglamento_spam_gaceta.pdf

RACSA. (2005). *Disminuye brecha digital*. Radiográfica Costarricense S.A. Consultado el 28 de enero de 2005 en http://www.racsa.co.cr/racsa_noticias/disminuye_brecha_digital.htm

Ramos Suárez, Fernando. (1998). *Problemas jurídicos del comercio electrónico*. Revista Electrónica de Derecho Informático. 2-Set-1998. Consultado el 15 de julio de 2004 en http://publicaciones.derecho.org/redi/N@mero_10_-_Mayo_de_1999/ramos2.

Ramos Suárez, F. (2001). *La seguridad en el comercio electrónico*. Revista de la Contratación Electrónica. Núm. 19. pp.122 ss.

Ramírez Ramírez, Ángel. (2002). *Desafíos jurídicos del comercio electrónico*. Tesis de Maestría en Derecho Económico. Costa Rica: Universidad Estatal a Distancia.

Ramos, Fernando. (Setiembre 1998). *Problemas jurídicos del comercio electrónico*. Revista Electrónica de Derecho Informático R.E.D.I. Número 2. Consultado el 2 de diciembre de 2004 en http://www.derecho.org/redi/numero2/ramos2.shtml

Ramos, Fernando. (2004). *El comercio electrónico: la seguridad técnica y jurídica.* Madrid. Consultado el 2 de diciembre de 2004 en http://www.masterdisseny.com/master-net/legalia/0006.php3

Reche Martínez, D.; García Linares, A.J.; Richarte Reina, J.M. (2003). *Certificados Digitales y su utilización en Entornos Clínicos.* INFORSALUD'2003. Consultado el 8 de diciembre de 2004 en http://www.seis.es/inforsalud03/INFORSALUD2003_reched2.pdf

Reidenberg, J. (1999). *Privacidad y Comercio Electrónico en los Estados Unidos*. Seminario "The Legal and Policy Framework for Global Electronic Comerse: A Progress Report", 4 al 6 de marzo de 1999. Universidad de California- Berkeley. Consultado el 24 de mayo de 2007 en http://reidenberg.home.sprynet.com/Privacidad-USA.htm

Remolina, N. (2005). *La protección de datos personales y el hábeas data en Colombia: Avances, retos y elementos para su regulación*. II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.153-196.

Ribas, Alejandro. (1998). *Aspectos jurídicos del comercio electrónico en Internet.* Pamplona, Aranzadi.

Rivas, Xavier. (1998). *Comercio electrónico en Internet. Aspectos jurídicos* (Extracto de la obra del mismo autor: Manual práctico sobre comercio electrónico en Internet.) Revista Electrónica de Derecho Informático R.E.D.I. Número 2. Septiembre de 1998. Consultado el 2 de diciembre de 2004 en http://www.derecho.org/redi/numero2/ribas2.shtml.

Rivas, Xavier. (1998). *Esquema de la propuesta de directiva sobre firmas electrónicas (COM(98) 297*. Novática. Número 135, Septiembre-Octubre 1998. Consultado el 1 de diciembre de 2004 en http://www.ati.es/PUBLICACIONES/novatica/1998/135/nv135sum.html.

Rivas, Xavier (2004). *Aspectos jurídicos de Internet.* CONTRACT-SOFT. Consultado el 1 de diciembre de 2004 en http://www.onnet.es/cs.htm

Rivera, G. (2003). *Constitución Política de la República de Costa Rica*. Costa Rica: Editec Editores S.A.

Rivero Sánchez, Juan Marcos (1997). *QUO VADIS: DERECHO DEL CONSUMIDOR?* Medellín: Biblioteca Jurídica Dike, c1997. 181 p.

Rubio, J. (2004). *Compendio de normas de Protección al Consumidor. Superintendencia de Industria y Comercio*. Colombia: Imprenta Nacional. Consultado el 22 de diciembre de 2006 en http://www.sic.gov.co/Normatividad/Jurisprudencia/Proteccion_Normas.pdf

Ruiz, María José. (2004). *Comprar en Internet ¿Ventaja o desafío?* Consultado el 8 agosto de 2004 en http://www.informatica-juridica.com/trabajos/Comprar_en_Internet.asp

Salas Araya, Yorleny; Fernández Araya, Mauricio. (2003). *El comercio electrónico en la sociedad costarricense*. Revista Intersedes. Vol. IV. No.7. Costa Rica: Universidad de Costa Rica.

Salas Arroyo, Jessica; Sánchez Delgado, José Daniel. (1999). *Algunas figuras delictivas en Internet.* Tesis para optar por el grado de Licenciatura en Derecho. Facultad de Derecho. Costa Rica: Universidad de Costa Rica.

Salas, E., Barrantes, J. (2002). *Código Civil de Costa Rica y Jurisprudencia, Síntesis de Jurisprudencia de la Sala Constitucional; Salas Primera, Segunda y Tercera, Tribunal Primero y Segundo, ambos Civil y de San José.* Costa Rica: Biblioteca Jurídica DIKÉ y La Casa de los Riscos.

Salas, E., Barrantes, J. (2001). *Código de Comercio de Costa Rica y Jurisprudencia, Síntesis de Jurisprudencia de la Sala Constitucional, Sala Primera y Sala Segunda, Tribunal Primero Civil, Tribunal Segundo Civil, Tribunal de Heredia, Juzgados de Instancia y Contraloría General de la República*. Costa Rica: Biblioteca Jurídica DIKÉ y La Casa de los Riscos.

Salas, E., Barrantes, J. (1997). *La Cláusula de intereses en un contrato de tarjeta de crédito*. Costa Rica: Imprenta y Litografía Mundo Gráfico S.A.

Samilovich, Sergio. (2001). *Cibernegocios*. Buenos Aires, Argentina: Netic Infoservicios, 2001.

Sarra, A.V. (2000). *Comercio electrónico y derecho: aspectos jurídicos de los negocios en Internet.* 1. ed. Buenos Aires, Argentina : Astrea.

Sartori, G.; Morlino, L. (1994). La comparación en las ciencias sociales. Madrid: Alianza Editorial.

SICE. Legislación Nacional – Argentina. Decreto 427/98. Consultado el 11 de junio de 2004 en http://www.sice.oas.org/e-comm/legislation/argB.asp

Sierra Bravo, R. (1992). *Técnicas de investigación social*. Madrid: Editorial Paraninfo S.A.

Simón, B. (2007). *Seguridad en Internet y firma digital*. Hermes Soluciones de Internet. Consultado el 20 de julio de 2007 en http://www.hermes.co.cr/boletin/firma%20digital.html

Sistema de cifrado. Guía de “Gnu Privacy Guard''. Consultado el 8 de diciembre de 2004 en http://sunsite.icm.edu.pl/gnupg/gph/es/manual/x220.html

Solano, Monserrat. *Atención a ciberdelitos*. La Nación. 1 de junio de 2001. San José, Costa Rica. Consultado el 28 de febrero de 2006 en http://www.nacion.com/ln_ee/2001/junio/01/pais15.html

Superintendencia de Industria y Comercio. Ministerio de Comercio, Industria y Turismo. Colombia. Consultado el 21 de setiembre de 2006 en http://www.sic.gov.co/Normatividad/Decretos/Decreto%201747-00.php

Tanus, Gustavo. (2004). *Anteproyecto de ley formato digital de los actos jurídicos*. Comercio electronico. Consultado el 9 de junio de 2004 en http://www.geocities.com/SiliconValley/Circuit/4888/anteproy.htm.

Téllez, J. (2004).*Derecho Informático*. 3 ed. México: McGraw Hill/Interamericana Editores S.A.

Telmo, D. (2007). *Algunas consideraciones acerca del concepto de hermenéutica*. Consultado el 11 de julio de 2007 en www.fhumyar.unr.edu.ar/escuelas/3/materiales%20de%20catedras/trabajo%20de%20campo/hermeneutica.htm

Tiquicia.com. (2001). *La Regulación del comercio electrónico*. Editorial Tiquicia.com. 16 enero 2001. Consultado el 8 de junio de 2004 en http://www.tiquisia.com/editorial/index03.asphttp://www.tiquisia.com/editorial/index03.asp

Vásquez, R. (2002). *La contratación en Internet. Innovación tecnológica y contratación. La forma de los contratos. Contratación informática. Comercio electrónico.* La Seguridad Jurídica en las Transacciones Electrónicas. Seminario organizado por el Consejo General del Notariado en la UIMP. España: Civitas Ediciones S.A.

Velasco, C. (2003). *Privacidad y protección de datos personales en Internet. Es necesario contar con una regulación específica en México*. Boletín de Política Informática No.1. México. Consultado el 3 de mayo de 2007 en http://www.inegi.gob.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf

Vega, J. (2005). *Contratos electrónicos y protección de los consumidores*. Madrid: Reus S.A.

Villate, J. (1998). *P3P un estándar para la privacidad. ¿Es lo que necesitamos?* Revista de Derecho Informático. No.1 Agosto 1998. Alfa Redi. Consultado el 25 de mayo de 2007 en http://www.alfa-redi.org/rdi-articulo.shtml?x=138

Materiales normativos y de organizaciones internacionales

CNUDMI. (1999). *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación en el Derecho Interno 1996 con el nuevo artículo 5 bis aprobado en 1998.* Nueva York: Organización de las Naciones Unidas. Consultado el 23 de enero de 2007 en http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce.html

CNUDMI. (2002). *Ley Modelo de la CNUDMI sobre Firma Electrónica con la Guía para su incorporación al derecho interno 2001*. Nueva York: Organización de las Naciones Unidas. Consultado el 23 de enero de 2007 en http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce.html

CNUDMI (2004). *Aspectos jurídicos del comercio electrónico Contratación electrónica: disposiciones para un proyecto de convención.* A/CN.9/WG.IV/WP.108. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. Grupo de Trabajo IV (Comercio Electrónico). 43º período de sesiones. Nueva York, 15 a 19 de marzo de 2004. Consultado el 6 de octubre de 2006 en http://daccessdds.un.org/doc/UNDOC/LTD/V03/907/69/PDF/V0390769.pdf?OpenElement.

CNUDMI. (2005). *Convención de la Naciones Unidas sobre la utilización de las comunicaciones electrónicas en contratos internacionales.* Organización de las Naciones Unidas. Consultado el 19 de noviembre de 2006 en http://www.uncitral.org/pdf/spanish/texts/electcom/2005Convention_s.pdf

CNUDMI (2005)*. Proyecto II Convención de la Naciones Unidas sobre las Utilizaciones de las Comunicaciones Electrónicas en los Contratos Internacionales.* Organización de las Naciones Unidas. Consultado el 3 de setiembre de 2006 en http://www.uncitral.org/pdf/spanish/texts/electcom/2005Convention_s.pdf

Comisión de las Comunidades Europeas. (2006). *Comunicación de la Comisión Al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo sobre la aplicación de la Directiva 1997/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia.* Bruselas, 21.9.2006. COM(2006) 514 final. Consultado el 8 de diciembre de 2006 en http://eur-lex.europa.eu/LexUriServ/site/es/com/2006/com2006_0514es01.pdf

Constitución Política de Chile. (2005). Chile. Consultado el 18 de octubre de 2006 en http://www.bcn.cl/pags/legislacion/leyes/constitucion_politica.htm

Constitución Política de la República de Colombia de 1991 con reformas hasta el 2005. (2005). Consultado el 18 de octubre de 2006 en http://pdba.georgetown.edu/Constitutions/Colombia/col91.html

Constitución Política de Costa Rica (2002). Consultado el 18 de octubre de 2006 en http://www.constitution.org/cons/costa_rica/costa_rica.htm

Constitución Política de Ecuador. (1998). Consultado el 18 de octubre de 2006 en http://www.presidencia.gov.ec/modulos.asp?id=109

Constitución Política de los Estados Unidos Mexicanos. (2002). Consultado el 18 de octubre de 2006 en http://constitucion.presidencia.gob.mx/index.php?idseccion=216

Constitución Política del Perú.(2000). Consultado el 18 de octubre de 2006 en http://www.tc.gob.pe/legconperu/constitucion.html

Convenio sobre la Ley Aplicable a las Obligaciones Contractuales abierto a la firma en Roma el 19 de junio de 1980 (80/934/CEE) (Convención de Roma 1980). Journal officiel n° L 266 du 09/10/1980 p. 0001 – 0019. Consultado el 29 de enero de 2007 en http://www.rome-convention.org/instruments/i_conv_orig_es.htm

Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Adoptado el 28 de enero de 1981 en Estraburgo. Consultado el 30 de junio de 2007 en www.apdcat.net/media/246.pdf

*Decreto 1441 por el cual se regula la organización, el reconocimiento y el régimen de control y vigilancia de las ligas y asociaciones de consumidores y se dictan otras disposiciones. 24 de mayo de1982***.** Superintendencia de Industria y Comercio, Ministerio de Comercio, Industria y Turismo. República de Colombia. Consultado el 22 de diciembre de 2006 en

http://www.sic.gov.co/Normatividad/Decretos/Decreto%201441-82.php

Decreto Legislativo 295 Código Civil. Publicado 25.07.84. Perú. Consultado el 8 de setiembre de 2006 en http://www.cajpe.org.pe/rij/bases/legisla/peru/codciv.htm

Decreto 3466 por el cual se dictan normas relativas a la idoneidad, la calidad, las garantías, las marcas, las leyendas, las propagandas y la fijación pública de precios de bienes y servicios, la responsabilidad de sus productores, expendedores y proveedores, y se dictan otras disposiciones. 2 de diciembre de1982. Superintendencia de Industria y Comercio, Ministerio de Comercio, Industria y Turismo. República de Colombia. Consultado el 22 de diciembre de 2006 en
http://www.sic.gov.co/Normatividad/Decretos/Decreto%203466-82.php

Decreto 3467 por el cual se dictan unas normas relativas a las ligas y Asociaciones de Consumidores. 2 de diciembre de 1982. Superintendencia de Industria y Comercio, Ministerio de Comercio, Industria y Turismo. República de Colombia. Consultado el 22 de diciembre de 2006 en
http://www.sic.gov.co/Normatividad/Decretos/Decreto%203467-82.php

Decreto 3468 por el cual se crea y organiza el Consejo Nacional de Protección al Consumido. 2 de diciembre de 1982.Superintendencia de Industria y Comercio, Ministerio de Comercio, Industria y Turismo. República de Colombia. Consultado el 22 de diciembre de 2006 en
http://www.sic.gov.co/Normatividad/Decretos/Decreto%203468-82.php

*Decreto 2153 de 30 de diciembre de 1992***.** Ministerio de Desarrollo Económico. Sistema de Información de Comercio Exterior. Colombia. Consultado el 22 diciembre de 2006 en http://www.sice.oas.org/compol/natleg/Colombia/D2153.asp

Decreto 1747 por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. 11

de Septiembre de 2000. Superintendencia de Industria y Comercio. Ministerio de Comercio, Industria y Turismo. Colombia. Consultado el 21 de setiembre de 2006 en http://www.sic.gov.co/Normatividad/Decretos/Decreto%201747-00.php

Decreto 181. Reglamento a la Ley 19799. 17 de agosto del 2002. Chile. Consultado el 1 de octubre de 2006 en http://www.bcn.cl/pags/home_page/ver_articulo_en_profundidad.php?id_subarticulo=498&id_destaca=407

Decreto 3496 Reglamento a la Ley de Comercio Electrónico. RO/735 del 31 de diciembre del 2002. Ecuador. Consultado el 15 de setiembre de 2006 en http://cpsr-peru.ifpeople.net/bdatos/ecuador/spam/3496-Ecuador.pdf#search=%22Decreto%203496%202002%20Ecuador%22

Decreto Legislativo 691 Dictan Normas de Publicidad en Defensa del Consumidor. Publicado el 6 de noviembre de 1991. Congreso de la República. Biblioteca Virtual INDECOPI. Perú. Consultado el 2 de enero de 2007 en http://www.congreso.gob.pe/ntley/Imagenes/DecretosLegislativos/00691.pdf

*Decreto de Ley 25868 Ley de Organización y Funciones del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)***.** Perú. 1992. Consultado el 31 de enero de 2007 en http://www.sice.oas.org/compol/natleg/Peru/25868.asp

Decreto Legislativo 807 Ley sobre Facultades, Normas y Organización del INDECOPI. Perú. 1996. Consultado el 31 de enero de 2007 en http://www.sice.oas.org/compol/natleg/Peru/807a.asp

Decreto legislativo 716 Ley de protección al consumidor. 11 de diciembre de 2000. Instituto Nacional de Defensa de la Competencia y de la Protección de la propiedad intelectual INDECOPI. Perú. Consultado el 13 de setiembre de 2006 en http://www.indecopi.gob.pe/upload/cpc/tuo716.pdf#search=%22Decreto%20Legislativo%20716%20Ley%20de%20Protecci%C3%B3n%20al%20consumidor%22

Decreto Supremo No. 19-2002-JUS. Reglamento de la Ley 27269 de Firmas y certificados digitales. 2002. Perú. Consultado el 18 de setiembre de 2006 en http://www.indecopi.gob.pe/upload/crt/firmasDigitales/reglamentods019-2002-jus.PDF#search=%22Reglamento%20Ley%2027269%20Per%C3%BA%22

*Decreto de reformas del 29 de mayo de 2000, se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en materia común y para toda la República en materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor***.** México. Consultado el 15 de enero de 2007 en http://www.stjsonora.gob.mx/acceso_informacion/marco_normativo/Codigo_Federal_Procedimientos_Civiles.pdf

*Decreto sobre firma electrónica. Se reforman los artículos 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113 y 114. Se adicionan los artículos 89 bis, 90 bis, 91 bis, 93 bis. Se adicionan los Capítulos Primero, Segundo, Tercero y Cuarto al Título Segundo, denominado "Del Comercio Electrónico", correspondiente al Libro Segundo, todos del Código de Comercio***.** Publicada 29 agosto 2003. Diario Oficial. México. Consultado el 11 de setiembre de 2006 en http://www.mexicofiscal.com.mx/novedades/dec290803.htm

Decisión 2000/520/CE de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Consultado el 3 de mayo de 2007 en https://www.agpd.es/upload%2FCanal_Documentacion%2Flegislacion%2FUnion%20Europea%2FDecisiones%2FB.12%29%20Decisi%F3n%20%20sobre%20la%20adecuaci%F3n%20conferida%20por%20los%20principios%20de%20puerto%20seguro.pdf

Decisión 2002/16/CE de la Comisión Europea Publicada el 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE. Consultado el 28 de marzo de 2007 en http://www.cpsr-peru.org/bdatos/decisiones/europa/Decision2002_16_CE_clausulastipotercerospaises.pdf/view

Directive 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 1539) Consultado el 9 de mayo de 2007 en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:EN:NOT

Directiva 93/13/CEE, de 5 abril 1993 del Consejo, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DOL núm. 95, de 21 abril [LCEur 1993, 1071]). Consultado el 5 de setiembre de 2006 en http://www.aeat.es/normlegi/ecomercio/dir93_13ce.htm

Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DO L 281 de 23 de noviembre de 1995. Consultado el 5 de setiembre de 2006 en http://europa.eu.int/spain/novedades/documentos/31995L46.htm

Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Consultado el 17 de octubre de 2006 en http://www.a-nei.org/documentos/Dir_9766CE.pdf

Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia - Declaración del Consejo y del Parlamento Europeo sobre el apartado 1 del artículo 6 - Declaración de la Comisión sobre el primer guión del apartado 1 del artículo 3 Diario Oficial n° L 144 de 04/06/1997 p. 0019 – 0027. Bruselas. Consultado el 8 de diciembre de 2006 en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:ES:HTML

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. Diario Oficial n° L 013 de 19/01/2000 P. 0012-0020. Consultado el 24 de noviembre de 2006 en http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:ES:HTML

Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Consultado el 15 de noviembre de 2006 en http://eur-lex.europa.eu/LexUriServ/site/es/oj/2000/l_178/l_17820000717es00010016.pdf

Directiva 2002/16/ce relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la directiva 95/46/ce. Decisión de la comisión del 27 de diciembre del 2001. Consultado el 17 de octubre de 2006 en

http://www.cpsr-peru.org/bdatos/decisiones/europa/Decision2002_16_CE_clausulastipotercerospaises.pdf

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). DO L 201 de 31.7.2002. Consultado el 5 de setiembre de 2006 en http://europa.eu/scadplus/leg/es/lvb/l24120.htm

Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) no 2006/2004 del Parlamento Europeo y del Consejo. Diario Oficial de la Unión Europea No. L 149 de 11-6-2005 p.22-39. Consultado el 5 setiembre de 2006 en http://www.consumo-inc.es/novedad/documentos/directiva.pdf

El Parlamento Europeo, El Consejo y la Comisión. *Carta de los Derechos Fundamentales de la Unión Europea* (2000/C 364/01). D. O. 18-12-2000. 364/01. Consultado el 27 de marzo de 2007 en
http://www.europarl.europa.eu/charter/pdf/text_es.pdf

El Parlamento Europeo, El Consejo. *Plan de acción para una utilización más segura de Internet (Safer Internet).* 2005. Consultado el 3 de mayo de 2007 en
http://europa.eu/scadplus/leg/es/lvb/l24190.htm

Electronics Signatures in Global and National Commerce Act. Law 106-229 106 th Congress. 30 junio 2000. USA. Consultado el 19 de setiembre de 2006 en http://www.cio.noaa.gov/itmanagement/pl106229.pdf#search=%22Electronic%20Signatures%20in%20Global%20and%20National%20Commerce%20Act%202000%22

Ley 19496 sobre protección de los derechos del consumidor. 7 de marzo 1997. Ministerio de Economía, Fomento y Reconstrucción. Biblioteca del Congreso Nacional. Chile. Consultado el 20 de diciembre de 2006 en http://www.sbif.cl/sbifweb/servlet/LeyNorma?indice=3.4&idContenido=2487

Ley 19.955 modifica la Ley Nº 19.496 sobre Protección de los Derechos de los Consumidores. Actualidad Jurídica. Base de Datos del Diario Oficial. Ministerio de Economía, Fomento y Reconstrucción Subsecretaria de Economía, Fomento y Reconstrucción. 14 de julio de 2004. Chile. Consultado el 20 de diciembre de 2006 en http://www.anfitrion.cl/actualidad/20ulle/04071419955.html

Ley19.628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal. Publicada en el Diario Oficial de 28 de agosto de 1999. Chile. Consultado el 21 de octubre de 2006 en http://www.informatica-juridica.com/anexos/anexo137.asp

Ley 19.812 que modifica la ley 19.628, sobre protección de la vida privada. 11 de junio de 2002. Chile. Consultado el 21 de octubre de 2006 en http://www.informatica-juridica.com/anexos/anexo867.asp

Ley 472 por la cual se desarrolla el artículo 88 de la Constitución Política de Colombia en relación con el ejercicio de las acciones populares y de grupo y se dictan otras disposiciones. 5 de agosto 1980. Colombia. Consultado el 20 de enero de 2007 en www.derechoshumanos.gov.co/descargas/LEY472DE1998.doc

LEY 73 DE 1981 por la cual el estado interviene en la Distribución de Bienes y Servicios para la Defensa del Consumidor, y se conceden unas Facultades Extraordinarias. Superintendencia de Industria y Comercio, Ministerio de Comercio, Industria y Turismo. República de Colombia. Consultado el 22 de diciembre de 2006 en http://www.sic.gov.co/Normatividad/Leyes/Ley%2073-81.php

LEY 446 por la cual se adoptan como legislación permanente algunas normas del Decreto 2651 de 1991, se modifican algunas del Código de Procedimiento Civil, se derogan otras de la Ley 23 de 1991 y del Decreto 2279 de 1989, se modifican y expiden normas del Código Contencioso Administrativo y se dictan otras disposiciones sobre descongestión, eficiencia y acceso a la justicia. 7 de julio de 1998. Colombia. Consultado el 22 diciembre de 2006 en http://www.sic.gov.co/Normatividad/Leyes/Ley%20446-98.php

Ley 527 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial No. 43.673, de 21 de agosto de 1999. Colombia. Consultado el 8 de setiembre de 2006 en http://www.secretariasenado.gov.co/leyes/L0527_99.HTM

LEY 588 Por medio de la cual se reglamenta el ejercicio de la actividad notarial. Diario Oficial No. 44.071, de 6 de julio de 2000. Colombia. Consultado el 21 de setiembre de 2006 en http://www.secretariasenado.gov.co/leyes/L0588000.HTM

Asamblea Legislativa (1969). *Decreto 4534. Convención Americana sobre Derechos Humanos*. Pacto de San José de Costa Rica del 22 de noviembre de 1969, en la Conferencia Especializada Interamericana sobre Derechos Humanos. Consultado el 17 de junio de 2007 en www.poder-judicial.go.cr/salasegunda/normativa/Convención%20Americana%20sobre%20Derechos%20Humanos.doc

Asamblea de Costa Rica. (1886). *Ley 63 Código Civil de Costa Rica.* Costa Rica. Consultado el 3 de marzo de 2007 en http://www.asamblea.go.cr/ley/leyes_nombre.htm

Asamblea Legislativa. (1964). *Ley 3284 Código de Comercio de Costa Rica*. 27 de mayo de 1964. Consultado el 3 de marzo de 2007 en http://www.asamblea.go.cr/ley/leyes_nombre.htm

Asamblea Legislativa**.** *Ley 4573. Código Penal*, *con reformas de la Ley 7899 del 3 de agosto de 1999*. Costa Rica. 1970. Consultado el 20 enero de 2007 en http://www.secmca.org/archivos/Codigo%20Penal.pdf.

Asamblea Legislativa. (1971). *Ley 4755 Código de Normas y Procedimientos Tributarios.* Costa Rica. Consultado el 1 de febrero de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/6000/4755.doc

Asamblea Legislativa (1995). *Ley 7472 Promoción de la Competencia y Defensa Efectiva del Consumidor***.** Costa Rica. Consultado 23 de diciembre de 2006 en http://www.asamblea.go.cr/ley/leyes_nombre.htm

Asamblea Legislativa (1989). *Ley 7130. Código Procesal Civil*. Costa Rica: Sistema Costarricense de Información Jurídica. Consultado el 31 de enero de 2007 en http://www.pgr.go.cr/scij/index_pgr.asp?url=busqueda/normativa/normas/nrm_articulo.asp?nBaseDato=1&nNorma=12443&nVersion=6&nArticulo=71404.

Asamblea Legislativa (1994). *Ley No. 7425. Ley de Registro, Secuestro y Examen de documentos privados e intervención de las comunicaciones.* Costa Rica. Consultado el 15 de enero de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/7000/7425.doc.

Asamblea Legislativa. (1990). *Ley No.7202. Ley Sistema Nacional de Archivos.* Costa Rica. Consultado el 21 de enero de 2007 en http://www.tse.go.cr/Ley_arch.htm.

Asamblea Legislativa. (1995). *Ley 7535 reformase del código de normas y procedimientos tributarios, ley no. 4755, del 3 de mayo de 1971 y sus reformas*. Costa Rica. Consultado el 20 de enero de 2007 en http://www.asamblea.go.cr/ley/leyes_numero.htm

Asamblea Legislativa (1993). *Ley 7333 Orgánica del Poder Judicial*. Costa Rica. Consultado el 20 de enero de 2007 en http://www.asamblea.go.cr/ley/leyes_numero.htm

Asamblea Legislativa (1995). *Ley No.7494. Ley de Contratación Administrativa*. Costa Rica. Consultado el 21 de enero de 2007 en http://www.asamblea.go.cr/ley/leyes_numero.htm

Asamblea Legislativa. (1995). *Ley No.7557. Ley General de Aduanas*. Costa Rica. Consultado el 3 de abril de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/7000/7557.doc

Asamblea Legislativa. *Ley 8131 de Administración Financiera de la República y Presupuestos Públicos*. 2001. Consultado el 13 de abril de 2007 en http://www.asamblea.go.cr/ley/leyes_nombre.htm

Asamblea Legislativa. (2001). *Ley 8148 adición de los artículos 196 bis, 217 bis y 229 bis al código penal ley nº 4573, para reprimir y sancionar los delitos informáticos*. Costa Rica. Consultado el 22 de enero de 2007 en http://www.racsa.co.cr/asamblea/ley/leyes/8000/8148.doc

Asamblea Legislativa (2005). *Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos.* Sistema Costarricense de Información Jurídica. .Costa Rica. Consultado el 15 de setiembre de 2006 en http://www.pgr.go.cr/

Asamblea Legislativa. (Febrero 2004). *Expediente 14.276 Ley Firma Digital y Certificado Digitales.* Comisión Permanente de Asuntos Jurídicos. Costa Rica. Consultado el 3 de enero de 2005 en http://archivo.ucr.ac.cr/normat/Firma%20Digital.pdf

Asamblea Legislativa. (2005). *Boletín Semanal del 22 al 26 de agosto de 2005*. Costa Rica. Consultado el 6 de setiembre de 2005 en http://www.asamblea.go.cr/actual/bol_prns.htm

Ley Orgánica de Defensa del Consumidor. Registro Oficial No.116 del 10 de julio de 2000. Ecuador. Consultado el 23 de diciembre de 2006 en http://www.estade.org/IIILegislaci%F3n/indexlink_leyes.html

Ley Orgánica de la Defensoría del Pueblo. R-22-058 (R.O. 280, 8-III-2001). Ecuador. Consultado el 31 de enero de 2007 en http://www.defensordelpueblo.gov.ec/paginas/pdf/legislacion/LEY_ORG_DEF.pdf

Ley de Comercio Electrónico, Firmas Y Mensajes De Datos. Ley No. 67. R.O. Suplemento 557 De 17 De Abril Del 2002. Ecuador. Consultado el 8 de setiembre de 2006 en peru.cpsr.org/bdatos/ecuador/privacidad/Ley2002-67ecuador.pdf

*Ley Federal de Protección al Consumidor***.** Publicada en el Diario Oficial de la Federación el 24-12-1992. México. Consultado el 20 de octubre de 2006 en http://www.economia.gob.mx/pics/p/p1376/L34.pdf

Ley Federal de transparencia y acceso a la información pública gubernamental. Diario Oficial de la Federación 11 de junio de 2002. Última reforma publicada DOF 06-06-2006. México. Consultado el 20 de octubre de 2006 en http://www.ordenjuridico.gob.mx/Federal/PE/PR/Leyes/11062002(1).pdf

Ley 26301 de Habeas Data. Promulgada 2 de mayo de 1994. Diario Oficial El Peruano del 23 de mayo de 1994. Perú. Consultado el 4 de noviembre de 2006 en http://www2.congreso.gob.pe/ccd/leyes/cronos/1994/ley26301.htm

*Ley 27269 Ley de Firmas y Certificados Digitales***.** Publicada el 2 de mayo de 2000. Perú. Consultado el 15 de setiembre de 2006 en http://www.sice.oas.org/e-comm/legislation/peru.asp

Ley 27.291 Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de la voluntad y la utilización de la firma electrónica. 24 de junio de 2000. Perú. Consultado el 11 de setiembre de 2006 en http://lac.derechos.apc.org/clegislacion.shtml?x=9559

Ley 19799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma. (2002). Ministerio de Economía, Fomento y Reconstrucción. Subsecretaría de Economía, Fomento y Reconstrucción. Chile. Consultado el 15 de setiembre de 2006 en http://www.modernizacion.cl/1350/articles-40703_ley_19799_firma_electronica.pdf#search=%22Chile%20Ley%2019799%20documentos%20electr%C3%B3nicos%2C%20firma%20electr%C3%B3nica%20y%20servicios%20de%20certificaci%C3%B3n%22

Ley 28493 Ley que regula el uso del correo electrónico comercial no solicitado (SPAM). 2005. Perú. Consultado el 11 de setiembre de 2006 en http://www.elcomercioperu.com.pe/EdicionOnline/Html/2005-04-12/onlPolitica0288301.html

Ley Orgánica 15/99 de protección de datos de carácter personal (LOPD). 13 diciembre 1999. B.O.E. 14-12.99. España. Consultado el 26 de marzo de 2007 en http://protecciondedatos.urjc.es/PD/legislacion/index.php

Ley 19.628 sobre protección de la vida privada. Chile. Agosto 1.999. Consultado el 20 de octubre de 2006 en http://www.informatica-juridica.com/anexos/anexo137.asp

Ley 26301 de Hábeas Data. Diario Oficial El Peruano del 23 de mayo 1994. Perú. Consultado el 8 de abril de 2007 en http://www.cajpe.org.pe/RIJ/bases/LEGISLA/PERU/pe_8.PDF

LEY 43 De Firma Digital De Panamá. 31.07.2001. Consultado el 15 de junio de 2004 en http://www.hfernandezdelpech.com.ar/Leyes/Ley%20de%20firma%20digital%20de%20Panama.htm.

Ley 26 General para la Defensa de los Consumidores y Usuarios, de 19 de julio de 1984. España. Consultado el 11 de setiembre de 2007 en http://noticias.juridicas.com/base_datos/Admin/l26-1984.html#c3

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. España. Consultado el 11 de setiembre de 2007 en http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html

Ley 34/2002 sobre telecomunicaciones y servicios de la sociedad de la información y del comercio electrónico, de 11 de julio. España. Consultado el 11 de setiembre de 2007 en http://209.85.165.104/search?q=cache:f9TFWX0B2-YJ:travesia.mcu.es/documentos/ley_34_comercio_elec.pdf+Ley+34/2002&hl=es&ct=clnk&cd=4&gl=cr

Naciones Unidas (1990). *Directrices para la regulación de los archivos de datos personales informatizados.* Resolución 45/95 de la Asamblea General de 14 de diciembre de 1990. Consultado el 1 de julio de 2007 en http://www.un.org/spanish/documents/ga/res/45/list45.htm

OCDE (1980). *Directrices relativas a la protección a la intimidad y de la circulación transfronteriza de datos personales.* Adoptada 23 de setiembre de 1980. Consultado el 3 de mayo de 2007 en https://www.agpd.es/upload%2FCanal_Documentacion%2Flegislacion%2FOrganismos%20Internacionales%2FOCDE%2FOCDE-Directrices%20sobre%20protecci%F3n%20de%20privacidad-Trad..pdf

OCDE. (1999). *Recomendación del consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico.* Traducción realizada por la Secretaría de Comercio y Fomento Industrial, Subsecretaría de Comercio Interior y Procuraduría Federal del Consumidor. México. Consultado el 9 de marzo de 2006 en http://www.oecd.org/dataoecd/18/27/34023784.pdf

OCDE. (2002).*Directrices de la OCDE sobre Protección a la privacidad y flujos transfronterizos de datos personales.* Consultado el 17 de octubre de 2006 en http://www.oecd.org/dataoecd/16/51/15590267.pdf

OCDE (2002). *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* Organisation for Economic Co-operation and Development (OECD), París. Consultado el 2 de octubre de 2006 en http://www.csi.map.es/csi/pdf/ocde_directrices_esp.pdf#search=%22OCDE%201997%20Criptograf%C3%ADa%22

Proyecto de documento de trabajo sobre el funcionamiento del acuerdo de puerto seguro. Grupo de trabajo sobre protección de datos art. 29. 11194/02/ES WP 62. 2 de julio 2002. Consultado el 26 de octubre de 2006 en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp62_es.pdf

Proyecto de ley estatutaria 143-2003 por la cual se dictan disposiciones para la protección de datos de carácter personal y se regula la actividad de recolección, tratamiento y circulación de los mismos. Colombia. Consultado el 10 de noviembre de 2006 en http://www.cpsr-peru.org/privacidad/privfinanciera/habeasdata_defpueblo.pdf

Proyecto de ley estatutaria 071 de 2005 Cámara por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones. 10 de agosto de 2005. Ministerio de Hacienda. Colombia. Consultado el 11 de noviembre de 2006 en http://www.cpsr-peru.org/privacidad/privfinanciera/proy071-2005camara.pdf

Proyecto de ley 14029 Derecho de acceso a Internet. Asamblea Legislativa. Costa Rica. 2001. Consultado el 4 de febrero de 2007 en http://www.asamblea.go.cr/proyecto/14000/14029.doc

Proyecto de ley 15178 de Protección de la persona frente al tratamiento de datos personales. Asamblea Legislativa. Costa Rica. 2003. Consultado el 4 de febrero de 2007 en http://www.asamblea.go.cr/proyecto/15100/15178.doc.

Proyecto Ley de Comercio Electrónico No.16081. 6 de diciembre de 2005. Asamblea Legislativa. Costa Rica. Consultado el 22 de febrero de 2007 en http://www.asamblea.go.cr/proyecto/exp_16000.htm

Asamblea Legislativa (2004). Proyecto original de Ley de firmas y documentos electrónicos, versión del 25 de junio de 2004. Costa Rica. Consultado el 31 de marzo de 2007 en http://www.hess-cr.com/secciones/dere-info/lacralo.shtml

*Proyecto de Decreto que expide la Ley Federal de Protección de Datos Personales***.** Dip. Miguel Barbosa Huerta (PRD). Publicación en Gaceta Parlamentaria, 7 de Septiembre de 2001. Secretaría de Servicios Parlamentarios. México. Consultado el 5 de febrero de 2007 en http://www.cddhcu.gob.mx/servicios/datorele/cmprtvs/1po2/set/2.htm

Proyecto de Ley de Protección de Datos. R.M. No.94-2002-JUS. Diario Oficial El Peruano 23 de julio de 2004. Perú. Consultado el 11 de noviembre de 2006 en https://www.agpd.es/upload/Canal_Documentacion/legislacion/ProyectoProteccionDatosPers-peruano.pdf

Proyecto de Ley 5233 sobre la Privacidad de los Datos Informáticos y la Creación del Comisionado para la Protección de la Privacidad. Perú. 23 setiembre 1999. Consultado el 11 de noviembre de 2006 en http://www2.congreso.gob.pe/ccd/proyectos/pr9909/00523395.htm

Reglamento a la Ley de Certificados, firmas digitales y documentos electrónicos. Decreto 33018 del 20 de marzo del 2006. Gaceta diario Oficial No.77 del 21 de abril del 2006. San José, Costa Rica. Consultado el 15 de setiembre de 2006 en http://www.pgr.go.cr

Reglamento (CE) n° 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Reglamento de Bruselas I). Diario Oficial n° L 012 de 16/01/2001 p. 0001 – 0023. Consultado el 30 de enero de 2007 en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:ES:HTML

Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. *DO L 8 de 12.1.2001, p. 1/22.* Consultado el 28 de marzo de 2007 en http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=es&type_doc=Regulation&an_doc=2001&nu_doc=45

Resolución aprobada por la Asamblea General de Naciones Unidas sobre Protección al Consumidor 1985. Superintendencia de Industria y Comercio, Ministerio de Comercio, Industria y Turismo. República de Colombia. Consultado el 22 de diciembre de 2006 en http://www.sic.gov.co/Normatividad/Supranacionales/Resolucion%20ONU.php

Resolución del Consejo del 19 de enero de 1999 sobre la dimensión relativa a los consumidores en la sociedad de la información. (1999/C 23/01). Diario Oficial de las Comunidades Europeas 29 enero 1999. Consultado el 7 de diciembre de 2006 en http://eur-lex.europa.eu/LexUriServ/site/es/oj/1999/c_023/c_02319990128es00010003.pdf

Resolución del Consejo, de 25 de mayo del 2000, relativa a una red a comunitaria de órganos nacionales encargados de la solución extrajudicial de litigios de consumo. Diario Oficial C 155 de 6.6.2000. Consultado el 30 de enero de 2007 en http://europa.eu/scadplus/leg/es/lvb/l32043.htm

Resumen Decisión nº 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999, por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Consultado el 3 mayo de 2007 en http://europa.eu/scadplus/leg/es/lvb/l24190.htm

UNCTAD. (2003). *Informe sobre comercio electrónico y desarrollo 2003.* Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Naciones Unidas. Nueva York y Ginebra. Consultado el 11 de noviembre de 2004 en http://www.unctad.org/sp/docs//ecdr2003_sp.pdf

USA Congress (2000). Electronics Signatures in Global and Nacional Commerce Act. Law 106-229 106 th Congress. 30 junio 2000. Consultado el 19 de setiembre de 2006 en http://www.cio.noaa.gov/itmanagement/pl106229.pdf#search=%22Electronic%20Signatures%20in%20Global%20and%20National%20Commerce%20Act%202000%22

Utah Digital Signature Act. Utah Code §§ 46-3-101 to 46-3-504
Enacted by L. 1995, ch. 61. Università degli Studi di Trento. Facoltà Di Giurisprudenza. Dipartimento Di Scienze Giuridiche. Italie. Consultado el 2 octubre de 2006 en http://www.jus.unitn.it/users/pascuzzi/privcomp97-98/documento/firma/utah/udsa.html

Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. WP74. 11639/02/EN. Adopted on 3 June 2003. Article 29 - Data Protection Working Party. WP74. Consultado el 3 de mayo de 2007 en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting from "Binding Corporate Rules". Adopted on April 14th , 2005. WP107. O5/EN. Article 29 Data Protection Working Party. Consultado el 9 de mayo de 2007 en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp107_en.pdf

Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules. Adopted on April 14th, 2005. WP108. 05/EN**.** Article 29 Data Protection Working Party. Consultado el 9 de mayo de 2007 en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

ANEXOS

Anexo 1. Cuadro comparativo de las legislaciones sobre derechos del consumidor.

De acuerdo con el Marco Teórico planteado, las legislaciones latinoamericanas cumplen con las siguientes medidas de protección al consumidor:

a) El logro de la transparencia y el derecho a recibir, antes de la transacción y en su caso después de ella, información suficiente y fiable que contenga, en particular la identidad comprobada del proveedor y la información necesaria para probar la autenticidad de cada uno de los elementos de una transacción.
b) La no discriminación en el acceso a productos y servicios, con atención a las necesidades de los consumidores vulnerables.
c) La protección de los consumidores frente a las prácticas de comercialización no solicitadas, engañosas y desleales, incluida la publicidad, y el apoyo a que se pongan a disposición del consumidor medios fiables para filtrar el contenido de los sistemas de comunicación.
d) La protección de los intereses económicos de los consumidores, con una distribución equitativa de riesgos y responsabilidades que refleje en especial la responsabilidad del proveedor al optar por medios electrónicos de comercio y con inclusión, en particular, de las condiciones necesarias para que el consumidor pueda tomar decisiones ponderadas.
e) La protección de la salud, seguridad e intimidad de los consumidores, incluida la protección contra la utilización abusiva de datos personales.
f) La información y educación del consumidor, a fin de posibilitar la adquisición de las competencias adecuadas.
g) La consulta de los consumidores a la hora de desarrollar nuevas políticas o mecanismos reglamentarios.
h) La representación de los intereses de los consumidores en los órganos de control y vigilancia pertinentes."

Medida de protección	**Costa Rica**	**Chile**	**Ecuador**	**Perú**	**México**	**Colombia**
El logro de la transparencia y el derecho a recibir, antes de la transacción y en su caso después de ella, información suficiente y fiable que contenga, en particular la identidad comprobada del proveedor y la información necesaria para probar la autenticidad de cada uno de los elementos de una transacción.	Art.46 Constitución Política. Art.29 inc.c Ley 7472 establece el derecho a información veraz y oportuna. Art.31 inc.b establece como obligación del comerciante informar suficientemente al consumidor.	Art.3 inc.b Ley 19496 establece el derecho a información veraz y oportuna y el deber del consumidor de informarse. Art.32 establece que la información básica comercial, incluyendo la identidad del proveedor, debe ser en castellano. También indica la información que debe dar en los casos de contratos ofrecidos por medios electrónicos. Art.33 Ley 19496 la información del producto debe ser	Art. 4 inc.4 Ley Orgánica de Defensa del Consumidor establece el derecho a la información veraz y oportuna. Art.9 a la 16 Ley Orgánica de Defensa del Consumidor, norma lo relacionado a la información comercial básica. Art.17 Ley Orgánica de Defensa del Consumidor indica que es un deber del proveedor dar información veraz, suficiente, clara, completa y oportuna.	Art.5 inc.b Decreto 716 establece el derecho a la información. Art.15 indica que el proveedor debe dar información veraz, suficiente y de fácil acceso. Art.15 a la 23 Decreto 716 establece lo relacionado a la información en la oferta de bienes y servicios.	Art.1 inc.III,VI Ley Federal de Protección al Consumidor establece el principio básico de información adecuada y clara, y el otorgamiento de información para la defensa de sus derechos. Art.7 obliga al proveedor a informar. Art. 12 obliga al proveedor entregar comprobante de la transacción. Art.17 la publicidad debe contener identificación del proveedor.	Art.14 Dec 3466 la información debe ser veraz y suficiente y prohibe la propaganda que induzca a error.

Medida de protección	Costa Rica	Chile	Ecuador	Perú	México	Colombia
		suceptible a comprobación.			Art.32 Ley Federal de Protección al Consumidor la información debe ser veraz y no engañosa ni abusiva. Art.32 a la 45 se refiere a la información y publicidad.	
La no discriminación en el acceso a productosy servicios, con atención a las necesidades de los consumidores vulnerables.	Art.46 Constitución Política. Art.33 inc.d Ley 7472 establece la prohibición de negar un producto o servicio. El proyecto de ley 14029 Derecho de acceso a Internet establece como derecho el acceso a Internet y a las nuevas tecnologías de telecomunicación (aprobado por Comisión Permanente de Asuntos Económicos, a los quince días de mayo de 2001)	Art.3 inc. C. Establece el derecho a no ser discriminado.	Art.55 inc.1,2,4 Ley Orgánica de Defensa del Consumidor establece como prohibición: condicionar la venta, rehusar atender a un consumidor o aprovecharse de la edad, salud o nivel de educación del consumidor.	Art.5 inc.c Decreto 716, establece el derecho a acceder a una variedad de productos y a elegir libremente. Art. 5 inc.d aclara que los consumidores no pueden ser discriminados por ninguna razón. Art.7 B Decreto 716 establece que los proveedores no pueden discriminar a los solicitantes.	Art.7 Ley Federal de Protección al Consumidor obliga al proveedor a no negar producto o servicio a persona alguna. Art.58 Prohibe la discriminación en el acceso a bienes o servicios.	No se menciona nada sobre prohibición del trato discriminatorio en las normas mencionadas.
La protección de los consumidores frente a las prácticas de comercialización no solicitadas, engañosas y desleales, incluida la publicidad, y el apoyo a que se pongan a disposición del consumidor medios fiables para filtrar el contenido de los sistemas de comunicación.	Art.46 Constitución Política. Art.17 Ley 7472 Prohibe los actos de competencia desleal que perjudiquen al consumidor. Art. 29 inc.e establece estos aspectos como derechos del consumidor. Art.34 Ley 7472 la información de la publicidad debe ser veraz. Art.54 Ley 7472 establece sanciones a	Art.24 Ley 19496 establece infracciones a la publicidad falsa o engañosa. No regula la publicidad abusiva. Art.28 Ley 19496 establece cuándo se comete infracción a esta Ley. Art.28 A establece infracción por información confusa en la identidad del proveedor. Art.28 B se refiere a información enviada por correo electrónico.	Art. 4 inc.6 Ley Orgánica de Defensa del Consumidor, se refiere al derecho a la protección contra publicidad engañosa y métodos comerciales desleales. Art.6,7,8 Ley Orgánica de Defensa del Consumidor, regula la publicidad y su contenido. Art.55 establece las prácticas comerciales prohibidas.	Art.31 inc.VI Decreto 716, el consumidor tiene el derecho a la reparación, reposición o devolución de su dinero cuando el producto no cumple con la publicidad ofrecida. Art.8 Decreto 716 indica que el proveedor es responsable de la calidad de los productos, veracidad de la propaganda y de la información divulgada. Art.13 Decreto 716	Art.1 inc.VII Ley Federal de Protección al Consumidor establece el principio básico de protección contra publicidad engañosa o abusiva y métodos comerciales coercitivos y desleales. Art.10 prohibe métodos comerciales desleales y coercitivas, así como cláusulas abusivas. Art.17 se refiere a la publicidad enviada por correo electrónico.	Art.14,15,16 Dec 3466 la información debe ser veraz y suficiente y prohibe la propaganda que induzca a error. Art.31 Dec 3466 establece responsabilidades al productor por las marcas, leyendas y propagandas.

Medida de protección	Costa Rica	Chile	Ecuador	Perú	México	Colombia
	las infracciones a la Ley.			establece el derecho a la protección contra métodos comerciales coercitivos. Decreto legislativo 691 norma todo lo relacionado a la publicidad en defensa del consumidor. Ley 28493 regula lo relacionado a publicidad enviada por correo electrónico.	Art.25 bis corresponde a la Procuraduría imponer medidas precautorias cuando haya prácticas comerciales abusivas. Art.32 Ley Federal de Protección al Consumidor la información debe ser veraz y no engañosa ni abusiva. Art.32 a la 45 se refiere a la información y publicidad.	
La protección de los intereses económicos de los consumidores, con una distribución equitativa de riesgos y responsabilidades que refleje en especial la responsabilidad del proveedor al optar por medios electrónicos de comercio y con inclusión, en particular, de las condiciones necesarias para que el consumidor pueda tomar decisiones ponderadas.	Art.46 Constitución Política. Art.29 inc.b Ley 7472 lo establece como derecho. Art.32 Ley 7472 establece el régimen de responsabilidad del proveedor. Art.39 Ley 7472 establece la nulidad de los contratos por adhesión con cláusulas abusivas. Art. 40, 41,41 bis 42,43 (Garantía, ventas a plazo, tarjetas de crédito, verificación del mercado, acceso a la vía judicial) son normas que protegen los intereses económicos del consumidor.	Art.3 inc. e Ley 19496 establece el derecho a la reparación e indemnización de daños y el deber del consumidor de accionar cuando ha sido lesionado. Art. 3 bis establece los casos que el consumidor puede poner fin a un contrato, el inc. b indica que los contratos celebrados por medio electrónico son de estos casos. Art.12 A indica que en los casos de contratos electrónicos se requiere del consentimiento informado del consumidor. Art.16, 16 A y 16 B, 17 Ley 19496 norma lo relativo a las cláusulas abusivas en los contratos de adhesión. Art.18 al art.27 establece lo relacionado a la	Art.4 inc.2,3 el derecho de recibir bienes y servicios de calidad. Art. 4 inc.5 Ley Orgánica de Defensa del Consumidor, se refiere al trato equitativo por parte de los proveedores en cuanto a las condiciones de los bienes y servicios. Art.4 inc.8 establece el derecho a la reparación e indemnización de daños, inc 10,11 el derecho a mecanismos de tutela de derechos, acciones administrativas. Art.17 a la 31 Ley Orgánica de Defensa del Consumidor establece las responsabilidades y obligaciones del proveedor. Art.41 a la 50 establece normas para la protección contractual. Art.41, 42, 43, 44 establece lo	Art.5 inc.d lo Decreto 716 establece el derecho a la protección de los intereses económicos. Art.5 inc.e establece el derecho a la reparación de daños. Art.6 a la 14 Decreto 716 establece sobre las obligaciones de los proveedores. Art.29 a la 38 Decreto 716 establece las responsabilidades de los proveedores frente a los consumidores. Art.39 a la 44 establece infracciones y sanciones. No hay referencia a los contratos de adhesión.	Art.1 inc.IV,V Ley Federal de Protección al Consumidor establece el principio básico de prevención y reparación de daños patrimoniales y morales y el principio de acceso a los órganos administrativos. Art.1 inc.VIII establece como principio básico la protección del consumidor en transacciones electrónicas. Art.1 inc.IX establece el principio de respeto a derechos y obligaciones contraídas en la srelaciones de consumo. Art.42 obliga al proveedor entregar el bien o servicio ofrecido de acuerdo con la oferta dada en la publicidad. Art.46 a la 50 se refiere a las promociones y ofertas.	Art.11 Dec 3466 garantiza la calidad de los bienes y servicios ofrecidos. Art.18 al 22 norma lo relacionado a la fijación de precios. Art.25, 26 establece sanciones por incumplimientos de calidad e idoneidad. Art.36 a la 40 Dec 3466 los consumidores puede ejercer acciones de indemnización de perjuicios sufridos en la relación contractual.

Medida de protección	Costa Rica	Chile	Ecuador	Perú	México	Colombia
		responsabilidad por incumplimientos por parte del proveedor, son normas para la protección de los intereses económicos del consumidor.	relacionado a contratos de adhesión y cláusulas prohibidas. Art.45 establece el derecho a la devolución incluyendo bienes o servicios adquiridos por Internet.		Art.51 a 56 se refiere a las ventas a domicilios mediatas o inmediatas. Aquí podría incluirse las que se realizan por medio de Internet. Art.85 a 90 bis Ley Federal de Protección al Consumidor se refiere a los contratos de adhesión. Art.85 prohibe las cláusulas abusivas en estos contratos.	
La protección de la salud, seguridad e intimidad de los consumidores, incluida la protección contra la utilización abusiva de datos personales.	Art.24 y Art.46 Constitución Política. Art.29 inc.a Ley 7472 establece como un derecho la protección a la salud, seguridad y medio ambiente. Art.30 inc.a art.42 es una función del Estado velar por que los bienes y servicios cumplan con normas de seguridad, medio ambiente y los estándares de calidad Art.31 inc.d es una obligación del comerciante informar al consumidor para proteger su salud, seguridad y medio ambiente Art.54 y 56 establece sanciones. No se dice nada sobre la intimidad.	Art.3 inc. d Ley 19496 establece como un derecho la protección a la salud, seguridad y medio ambiente y el deber del consumidor de evitar los riesgos. No se dice nada sobre la intimidad. Art.45 Ley 19496 indica que para productos peligrosos debe informarse sobre su uso seguro.	Art.4 inc.1 Ley Orgánica de Defensa del Consumidor establece el derecho a la vida, salud y seguridad. No se dice nada sobre la intimidad. Art. 56 a la 60 se refiere a la protección a la salud y seguridad.	Art.5 inc.a Decreto 716 lo establece como un derecho la protección a la salud y seguridad física. Art.9 los productos y servicios no deben arriesgar la salud y seguridad del consumidor. Art.10 el proveedor es responsable de informar sobre los peligros y riesgos del producto o servicio. Art.24 A prohibe métodos de cobranza que atenten contra la privacidad.	Art.1 inc.I Ley Federal de Protección al Consumidor establece como principio básico la protección a la vida, salud y seguridad. Art.17 permite a los consumidores que su información no sea trasmitida a terceros. Art.18 bis exige a los proveedores respetar la voluntad del consumidor en cuanto a recibir publicidad o enviar su información a terceros. Art.25 bis corresponde a la Procuraduría imponer medidas precautorias cuando haya riesgos a la salud y seguridad de los consumidores. Art.78 bis inc.I obliga al proveedor a utilizar la información del consumidor en forma confidencial y prohibe su difusión o transmisión a otros proveedores.	Art.17 Dec 3466 en leyendas y propagandas se debe indicar la nocividad del bien o servicio y su correcto uso.

Medida de protección	Costa Rica	Chile	Ecuador	Perú	México	Colombia
					Art.128 ter inc. II es una infracción grave cuando se pone en peligro la vida, salud o seguridad de los consumidores.	
La información y educación del consumidor, a fin de posibilitar la adquisición de las competencias adecuadas.	Art.29 inc.d Ley 7472 lo establece como un derecho. Art.30, 66 Ley 7472, transitorio IV es una función del Estado.	Art. 3 inc. f Ley 19496 lo establece como un derecho. Art.58 inc. a Ley 19496 lo establece como un deber del Servicio Nacional del Consumidor.	Art.4 inc.7 lo establece como un derecho. Art.63 inc.4 lo establece como una función de las asociaciones de consumidores. Art. 89 Ley Orgánica de Defensa del Consumidor establece que el Ministerio de Educación debe incluir la educación del consumidor en sus programas.	Art.15 a la 23 Decreto 716 establece lo relacionado a la información en la oferta de bienes y servicios. No establece nada acerca de la educación del consumidor.	Art. 1 inc.II Ley Federal de Protección al Consumidor establece el principio básico de la educación y divulgación sobre el consumo adecuado. Art.8 bis la Procuraduría elaborará material para educar, orientar e informar al consumidor. Art.24 inc.V la Procuraduría formula y realiza programas de educación para el consumo.	Art.1 Dec.1441 educar al consumidor es un objetivo de las ligas de consumidores. Art.10 inc.o Dec.1441 establece la función de educar a las ligas y asociaciones de consumidores.
La consulta de los consumidores a la hora de desarrollar nuevas políticas o mecanismos reglamentarios.	Art.46 Constitución Política. Art.29 inc.g Ley 7472 establece el derecho a formar organizaciones de consumidores para plantear sus opiniones en las decisiones que les afecten. Art.30 inc. C es una función del Estado promover las organizaciones de consumidores.	Art. 5 al art. 11 bis Ley 19496 se refiere a las organizaciones para la defensa de los derechos de los consumidores, sus funciones y cómo se constituyen.	Art.61 Ley Orgánica de Defensa del Consumidor es un objetivo de las asociaciones de consumidores: defender derechos e intereses de los consumidores.	Art.4 Decreto 716 indica que las Asociaciones de consumidores tiene como finalidad la protección de los consumidores. Art. 39 la Comisión de Protección al Consumidor se encarga de las infracciones y sanciones a la Ley.	Art.31 la Procuraduría consultará a las organizaciones de consumidores en la elaboración de planes y programas.	Art.10 Dec 1441 establece las funciones de las ligas y asociaciones de consumidores. Art.12 Dec 1441 indica que las ligas y asociaciones representan a los consumidores en la defensa de sus derechos.
La representación de los intereses de los consumidores en los órganos de control y vigilancia pertinentes.”	Art.46 Constitución Política. Art.29 inc.g Ley 7472 establece el derecho a formar organizaciones de consumidores. Art.30 inc. C es una función del Estado promover las organizaciones de consumidores.	Art.8 Ley 19496 lo establece como un deber de las asociaciones de consumidores.	Art.4 inc.9 establece el derecho de recibir auspicio del Estado para constitui asociaciones. Art. 61 a la 63 Ley Orgánica de Defensa del Consumidor, define, establece los requisitos y objetivos de las asociaciones de	Art.4 Decreto 716 indica que las Asociaciones de consumidores tiene como finalidad la protección de los consumidores. Art.39 la Comisión de Protección al Consumidor se encarga de las infracciones y sanciones a la Ley.	Art.19,20 Ley Federal de Protección al Consumidor y Indica que la Secretaría y la Procuraduría Federal del Consumidor son organismos del Estado creadas para proteger los derechos e intereses de los	Decreto 3468 del 2 de diciembre de 1982 crea el Consejo Nacional de Protección al Consumidor. Decreto 3467 del 2 de diciembre de 1982 se dictan normas relativas a las ligas y asociaciones de consumidores.

Medida de protección	Costa Rica	Chile	Ecuador	Perú	México	Colombia
	Art.18,19, 44, 45 Ley 7472 crea la Comisión para Promover la Competencia y la Comisión Nacional del Consumidor. Art.51 legitima las organizaciones de consumidores.		consumidores.		consumidores. Art.24, inc.XVIII es una atribuciónde la Procuraduría promover y apoyar la constitución de organizaciones de consumidores.	Art. 43 Dec 3466 y la Ley 446 de 1998 establecen funciones y atribuciones a la Superintendencia de Industria y Comercio para la protección de consumidor.

Anexo 2. Matrices comparativas de las normas con relación a la contratación electrónica

Principios de seguridad jurídica de los mensajes de datos o documento electrónico

Principio	CNUDMI	Costa Rica	Chile	Colombia	Ecuador	México	Perú
Reconocimiento jurídico	Art.5 Ley Modelo Comercio Electrónico Art.6 Ley Modelo Firmas Electrónicas	Art.4, 9 Ley 8454	Art.3, 5 Ley 19799	Art.5, 10, 28 Ley 527	Art.2, 14 Ley 67	Art.89 bis, 97 Dec. Firma Elect. del 29 agosto 2003	Art.1 Ley 27269 y Art. 5, 6, 7 Regl. A la Ley 27269
Fuerza probatoria	Art.9 Ley Modelo Comercio Electrónico Art.6 Ley Modelo Firmas Electrónicas	Art.4 Ley 8454	Art.3, 5 Ley 19799	Art. 10, 11, 28 Ley 527	Art.52, 54, 55 Ley 67	Art.89, 89 bis Dec. Firma Elect. Del 29 agosto 2003	Art.7, 8 Regl. A la Ley 27269
Equivalencia funcional	Art.6, 7, 8 Ley Modelo Comercio Electrónico	Art. 3, 9 Ley 8454	Art.3 Ley 19799	Art.6, 7, 8 Ley 527	Art. 6, 7 Ley 67	Art. 89, 93, 93 bis, 97 Dec. Firma Elect. 29 agosto 2003	Art. 5, 6 Regl. A la Ley 27269
Neutralidad tecnológica	Art.3 Ley Modelo Firmas Electrónicas	Art.2 Ley 8454	Art.1 Ley 19799	No	Art.10 Decreto 3496	Art.89, 96 Decreto Firma Elect. 29 agosto 2003	Art. 9 Regl. A la Ley 27269
Autonomía de la voluntad	Art.4 Ley Modelo Comercio Electrónico Art.5 Ley Modelo Firmas Electrónicas	Art.2 Ley 8454	No	Art. 4 Ley 527	Art.48, 49 Ley 67	Artículo 89, 90 bis, 91, 91 bis 94 Decreto Firma Elect. 29 agosto 2003	Art. 2 Regl. A la Ley 27269
Compatibilidad internacional	Art.5 Ley Modelo Comercio Electrónico Art. 12 Ley Modelo Firmas Electrónicas	Art.13 Ley 8454	Art. 1 15 Ley 19799	Art. 3 Ley 527	Art.28 Ley 67	Art.89, 114 Decreto Firma Elect. 29 agosto 2003	Art.48 Regl. A la Ley 27269

Aspectos que deben ser regulados en una contratación electrónica

Elemento regulado	CNUDMI	Chile	Colombia	Costa Rica	Ecuador	México	Perú
Reconocimiento de firma electrónica	Art.6 Ley Modelo CNUDMI sobre Firmas electrónicas	Art.3 Ley 19799	Art.28 Ley 527	Art.9 Ley 8454	Art.14 Ley 67	Art.97 Dec. sobre firma electrónica del 29 de agosto del 2003	Art. 5, 6 Regl. Ley 27269
Formación y validez de los contratos	Art. 5,11,12 Ley Modelo CNUDMI sobre Comercio Electrónico	Art.3,5 Ley 19799	Art. 14 Ley 527	Art.4 Ley 8454	Art.2, 45 Ley 67	Art.89 bis, 93, 93 bis Dec. sobre firma electrónica del 29 de agosto del 2003	Art.7 Regl. Ley 27269
Identificación de las partes	Art.13 Ley Modelo CNUDMI sobre Comercio Electrónico	Art.3 Ley 19799	Art.16, 17 Ley 527	Art.10 Ley 8454	Art.10 Ley 67	Art.90, 90 bis Dec. sobre firma electrónica del 29 de agosto del 2003	Art. 8 Regl. Ley 27269
Perfección	Art. 14, 15 Ley Modelo CNUDMI sobre Comercio Electrónico		Art.20, 21, 22, 23, 24, 25 Ley 527		Art.46 Ley 67	Art.91, 91 bis, 94 Dec. sobre firma electrónica del 29 de agosto del 2003	
Jurisdicción, arbitraje, controversias					Art.47 Ley 67		

Elemento regulado	CNUDMI	Chile	Colombia	Costa Rica	Ecuador	México	Perú
Atribución, presunción de origen	Art. 13,14 Ley Modelo CNUDMI sobre Comercio Electrónico	Art.2 inc.g Ley 19799	art. 16, 17 Ley 527	art. 10 Ley 8454	art. 10 Ley 67	art. 90, 90 bis Dec. sobre firma electrónica del 29 de agosto del 2003	art. 8 Regl. A la Ley 27269
Acuse de recibo, presunción de recepción	Art.14 Ley Modelo CNUDMI sobre Comercio Electrónico		art. 20,21,22 Ley 527			Art.92 Dec. Sobre firma electrónica del 29 de agosto de 2003	
Tiempo y lugar de envío y recepción	Art.15 Ley Modelo CNUDMI sobre Comercio Electrónico		art. 23, 24, 25 Ley 527		art. 11 Ley 67.	art. 91, 91 bis, 94 Dec. sobre firma electrónica del 29 de agosto del 2003.	
Concordancia del mensaje enviado con el recibido	Art.14 Ley Modelo sobre Comercio Electrónico		art. 18 Ley 527				
Mensajes de datos duplicados	Art.13 Ley Modelo sobre Comercio Electrónico		art. 19 Ley 527		art. 12 Ley 67	Art. 95 Decreto sobre firma electrónica del 29 de agosto del 2003	
Efectos jurídicos del acuse de recibo	Art.14 Ley Modelo sobre Comercio Electrónico		art. 22 Ley 527				

Disposiciones de Organismos Internacionales sobre contratación electrónica y protección al consumidor.

Tema a regular	Unión Europea	OCDE	Naciones Unidas	Otros
Información y Publicidad	Art. 4, 10 Directiva 1997/97/CE. Art. 5, 7, 10, 16 Directiva 2000/31/CE. Art. 13 Directiva 2002/58/CE.	Recomendación de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico.		
Validez de los contratos vía Internet	Directiva 2000/31/CE		Art. 1, 5, 6, 11, 12 Ley Modelo CNUDMI de Comercio Electrónico. Art. 6 Ley Modelo CNUDMI sobre firma electrónica. Art. 9 Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 23 de noviembre de 2005.	Ley de Utah de Estados Unidos
Cláusulas del contrato	Art. 3 Directiva 1993/13/CE. Art. 5 Directiva 97/7/CE			
Identificación de las partes	Art. 5 Directiva 2000/31/CE Art. 4 Directiva 1997/7CE		Art. 13, 14 Ley Modelo CNUDMI de Comercio Electrónico. Art. 7 Convención de las Naciones Unidas	
Tiempo y lugar de perfección del contrato	Art. 2 Directiva 97/7/CE Art. 11 Directiva 2000/31/CE		Art. 15 Ley Modelo CNUDMI de Comercio Electrónico.	
Aspectos relacionados con el pago	Art. 8 Directiva 97/7/CE Art. 4, 5 Directiva 2002/58/CE			
Resolución del contrato	Art. 6 Directiva 97/7/CE			
Reclamos, Legislación aplicable, jurisdicción competente	Resolución del Consejo de 25 de mayo de 2000 relativa a una red comunitaria de órganos nacionales encargados de la solución extrajudicial de litigios de cnsumo. Art. 13, 14, 15, 16 del Reglamento de Bruselas I (44/2001). Art. 17, 18 Directiva 2000/31/CE			Art. 3, 4, 5 Convención de Roma de 1980.

Otros asuntos de la normativa de firma digital y certificados digitales

Asunto	Ley Modelo	Costa Rica	Chile	Colombia	Ecuador	México	Perú
1.Entidades de certificación		x	x	x	x	x	x
2.Entidad de registro o validación							x
3.Certificados digitales		x	x	x	x	x	x
4.Derechos de los consumidores			x	x	x		
5.Delitos informáticos					x		
6.Transporte	x			x			
7.Utilización por el Estado		x	x				

2. Entidades de certificación

- México, Perú, Colombia, Ecuador, Chile, Costa Rica: Los seis países establecen disposiciones relacionadas con las entidades de certificación.

- Cuatro de ellos coinciden en exigir que quienes presten servicios de certificación sean Personas Jurídicas. (Empresa Unipersonal o jurídica: ECU; Notarios y corredores públicos, personas privadas morales, instituciones públicas: MEX; Notarios y cónsules: COL, cualquier persona Nacional o extranjera Públicas o Privadas: CHL, CR, persona natural o jurídica: Perú).

- Exigen capacidad económica y financiera, así como técnica suficiente para desempeñar sus funciones.

- Deben ser Autorizadas por un órgano de control.

2. Entidad de registro o validación

- Perú es el único país que establece disposiciones sobre entidades de registro separadas a las entidades de certificación. Estas entidades deben cumplir la función de levantamiento de datos y comprobación de la información del solicitante de un certificado digital. Deberán registrarse ante la autoridad de control. Se trata de personas jurídicas que cuenten con el respaldo económico suficiente para realizar sus funciones.
- Los restantes países (México, Chile, Perú, Costa Rica, Colombia), las funciones de registro son parte de las funciones de las entidades de certificación.

3. Certificados digitales

- Todos los países coinciden en regular los certificados digitales con algunas variaciones en los respectivos reglamentos.

- Revocatoria: (COL, CHL,MEX,PER,ECU,CR)
- Reconocimiento internacional (MEX, CR, PER, ECU,CHL)

    - Requisitos (ECU,COL,MEX,PER,CHL,CR)
    - Duración (MEX,ECU,PER,COL,CHL,CR)
    - Extinción (ECU,MEX,CHL)
    - Suspensión (ECU,CR)
    - Cancelación (PER,CHL)
    - Aceptación (COL,CR)
    - Registro (COL,MEX,PER,CHL,CR)

4. Derechos de los usuarios o consumidores

- Ecuador, en la ley 67 se contemplan capítulos específicos sobre los siguientes aspectos relacionados con los derechos de los consumidores:
    - Derecho a dar el consentimiento expreso.
    - A ser informado.
    - A acceder a la información.
    - A elegir si recibe información por escrito o electrónica
    - Derecho de retracto

- Colombia: en su ley solo se indica que ésta se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

- Chile: en su ley se establece que es obligación del prestador de servicios de certificación de firma electrónica cumplir con las demás obligaciones legales,especialmente las establecidas en esta ley, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada.

- México, Perú y Costa Rica: Sus leyes de comercio electrónico no mencionan nada al respecto de los consumidores.

5. **Infracciones informáticas/ delitos informáticos**

- Ecuador incluye en su Ley 67 un capítulo con disposiciones que reforman su Código Penal:
    - Adecuación de algunos tipos penales
    - Falsificación electrónica
    - Violación de información protegida.
    - Sabotaje informático
    - Apropiación ilícita.

6. Transporte

- Colombia es el único que siguiendo las recomendaciones de la ley Modelo de comercio electrónico de UNCITRAL, incluye un capítulo sobre transporte de mercancías y sobre la aplicación del principio de equivalente funcional y de la validez jurídica a los actos que componen el contrato de transporte de mercancías.

7. **Utilización por el Estado**

México, Colombia, Perú, Ecuador: No.

Costa Rica y Chile: Establecen es sus leyes la posibilidad de que el Estado utilice la firma y documentos electrónicos en su relación con otras instituciones públicas, así como con los particulares.

Anexo 3. Cuadro comparativo de la normativa de Protección de la Privacidad o Datos Personales

Derechos a la protección de datos personales

Garantía	Chile	Colombia	Costa Rica	Ecuador	México	Perú
Derecho de acceso	Art.3, 4, 12, 14 Ley 19628	Art. 15 Constitución Art.6, inc.8; 14, 16 Proy.Ley Est.143-003. Art.4, inc. 9 Proy.Ley Est.071-2005	Art.3, 9, 11 Proyecto 15178	Art. 94 Constitución	Art. 20, 24 Ley Federal de Transparencia y Acceso a la Información Art.15,16 Proy. Dec Ley Federal de Protección de Datos Personales	Art. 2 inc.5 Constitución Art. 15 Proy. De ley de Protección de Datos Personales
Derecho de rectificación y cancelación	Art. 6,12, 13 Ley 19628	Art. 15 Constitución Art.6 inc.5; art. 14 inc.5; art.17 Proy.Ley Est.143-003. Art.18 Proy.Ley Est.071-2005	Art.3, 9 Proyecto 15178	Art. 94 Constitución	Art. 20, 25 Ley Federal de Transparencia y Acceso a la Información Art.19 Proy. Dec Ley Federal de Protección de Datos Personales	Art. 2 inc. 7 Constitución, Art.200 Constitución Ley 26301 de Habeas Data. Art. 16,17 Proy. De ley de Protección de Datos Personales
Derecho de oposición	Art.3, 12, 13 Ley 19628	Art.19 Proy.Ley Est.143-003. Art.4, inc.23; 18 Proy.Ley Est.071-2005	Art.3, 11 Proyecto 15178	Art.9 Ley 67	Art.19 Proy. Dec Ley Federal de Protección de Datos Personales	Art. 2 inc.24 Constitución Art.17 Proy. De ley de Protección de Datos Personales
Derecho al consentimiento	Art.3, 4 Ley 19628	Art.6, inc 3,4,32 Proy.Ley Est.143-003. Art.4, inc.2; 11 Proy.Ley Est.071-2005	Art.4 Proyecto 15178	Art. 9 Ley 67	Art. 21 Ley Federal de Transparencia y Acceso a la Información Art.6 Proy. Dec Ley Federal de Protección de Datos Personales	Art. 2 inc.24 Constitución Art.14, 16 Código Civil Art.8 Proy. De ley de Protección de Datos Personales

Garantía	Chile	Colombia	Costa Rica	Ecuador	México	Perú
Derecho de fijar el nivel de protección	Art.11 Ley 19628	Art.6, 8 inc.13 Proy.Ley Est.143-003. Art. 95 ley 270 Art.32 inc.C Ley 527 Art.4, inc.14, 9 inc.h Proy.Ley Est.071-2005	Art.7 Proyecto ley 15178		Art. 20 Ley Federal de Transparencia y Acceso a la Información Art. 12,13 Proy. Dec Ley Federal de Protección de Datos Personales	Art. 6 y 10 Constitución Art.12 Proy. De ley de Protección de Datos Personales
Derecho de uso conforme al fin	Art. 5, 9 Ley 19628	Art.32, inc.C Ley 527 Art.6 inc.7 Proy.Ley Est.143-003. Art.4, inc.3 Proy.Ley Est.071-2005	Art. 5 Proyecto ley 15178		Art. 20 Ley Federal de Transparencia y Acceso a la Información Art.8 Proy. Dec Ley Federal de Protección de Datos Personales	Art.5 Proy. De ley de Protección de Datos Personales
Derecho para la prohibición de interconexión de archivos		Art.4, inc.6 Proy.Ley Est.071-2005				
Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente		Art.21 Proy.Ley Est.143-003.			Art.18 Proy. Dec Ley Federal de Protección de Datos Personales	
Derecho de conocimiento	Art.3, 4, 12 Ley 19628	Art.4 inc.5; 12 Proy.Ley Est.071-2005 Art.14 Proy.Ley Est.143-003	Art. 3, proy. Ley 15 178		Art. 9 Proy. Dec Ley Federal de Protección de Datos Personales	Art. 6 Proy. De ley de Protección de Datos Personales
Derecho a la calidad de los datos	Art. 9 Ley 19628	Art. 4, inc.4; 9 inc. I; 13 Proy.Ley Est.071-2005 Art. 6, 8 Proy. Ley Est.143-003	Art. 5 Proy. Ley 15178		Art. 8 Proy. Dec Ley Federal de Protección de Datos Personales	Art.7 Proy. De ley de Protección de Datos Personales
Derecho de indemnización Derecho de tutela	Art. 23 Ley 19628 Art.16 Ley 19628	Art. 94 Proy. Ley Est.143-003 Art.10, 68 Proy. Ley Est.143-003. Art.31 Proy.Ley Est.071-2005	Art. 10 Proy. Ley 15178 Art.15 y 16 Proy. Ley 15178		Art. 21 Proy. Dec Ley Federal de Protección de Datos Personales Art. 22 Proy. Dec Ley Federal de Protección de Datos Personales	Art.20 Proy. De ley de Protección de Datos Personales Art.19, 35 Proy. De ley de Protección de Datos Personales
Derecho a la no discriminación	Art. 10 Ley 19628	Art. 63 Proy. Ley Est.143-003	Art. 6 proy. Ley 15178		Art. 7 Proy. Dec Ley Federal de Protección de Datos Personales	Art.11 Proy. De ley de Protección de Datos Personales

Normas constitucionales, generales y en proyecto

País	Constitución Política	Norma general	Normas en proyecto
Chile	No existe norma expresa, pero la construcción jurídica de la protección de datos personales se basa en el artículo 19 incisos 4 y 5, de la Constitución Política de la República, que reza: "CAPITULO III. De los Derechos y Deberes Constitucionales Artículo 19.- La Constitución asegura a todas las personas: (…) 4º.- El respeto y protección a la vida privada y a la honra de la persona y de su familia. 5º.- La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley."	Ley 19.628 "SOBRE PROTECCION DE LA VIDA PRIVADA", publicada el 28 de agosto de 1999, modificada por la Ley N° 19.812, de 13 de junio de 2002. Esta ley excluye de su aplicación los tratamientos de datos que se realicen en virtud del ejercicio de la libertad de información. El Reglamento de la Ley 19.628 es el Decreto 779 de 2000 del Ministerio de Justicia que regula el registro de Bancos de Datos Personales a cargo de los organismos públicos.	Proyecto de Ley que delimita el ámbito de la vida privada frente a la libertad de expresión del 13 de marzo de 2001 (en trámite). Proyecto de Ley que amplia beneficios de la ley de protección de la vida privada en lo relativo a los informes comerciales, a las personas jurídicas comprendidas en el articulo 545 del Código Civil del 15 de marzo de 2000. (en trámite) . Oficio 3029 de 17-08-00 al Senado, comunica aprobación de proyecto Proyecto de Ley que resguarda el derecho a la vida privada en materia telefónica del 28 de octubre del 2003 (en trámite). Proyecto de Ley que Modifica la ley n° 19.628, de Proteccion de Datos de carácter Personal, estableciendo norma sobre el uso de bases de datos en los correos electrónicos. Del 8 de enero de 2003 (en trámite).
Colombia	El artículo 15 de la Constitución, modificado por el acto legislativo N° 02 del 18 de diciembre de 2003 dice lo siguiente: "Todas las personas	No existe	Actualmente se encuentra en estudio el proyecto de ley estatutaria N° 143 de 2003 Senado, por la cual se dictan disposiciones

País	Constitución Política	Norma general	Normas en proyecto
	tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley"		para la protección de datos personales y se regula la actividad de recolección, tratamiento y circulación de los mismos". Aún falta tres debates para que se convierta en ley de la República. Proyecto de ley estatutaria 071 de 2005, presentado por el Ministerio de Hacienda y algunos congresistas, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la Información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones.
Costa Rica	Art. 24 de la Constitución Política establece: la garantía del derecho a la intimidad, a la libertad y al secreto de las comunicaciones, e indica que son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley fijará en qué casos podrán los Tribunales de Justicia ordenar el	No existe norma general	Existen en trámite legislativo el Proyecto de Ley No.15.178 Protección de la persona frente al tratamiento de sus datos personales. Texto 27 marzo 2003 pasó a Comisión Permanente de Asuntos Jurídicos. Este proyecto es el más completo en términos de aplicación de los

País	Constitución Política	Norma general	Normas en proyecto
	secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento. Igualmente la Ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que aplique ilegalmente esta excepción.		principios de tutela y de la creación de una organización técnica específica dirigida a realizar un modelo institucional de tutela. *Proyecto de Ley 15890 que adiciona un artículo 24 bis a la Constitución Política que dice:* "*Toda persona tiene derecho a tener o no tener personalidad virtual, donde su presencia, contenido y proyección se encuentre regulada por cada una de ellas. No podrá ser utilizada con fines discriminatorios en perjuicio de su titular. El Estado garantizará que la información contenida en la personalidad virtual goce de la adecuada seguridad informática y jurídica, con exclusión de terceros no autorizados que pretendan obtenerla. El Estado podrá hacer uso del contenido de la personalidad virtual de las personas, previa autorización de estas, siempre que se realice en beneficio y provecho de las mismas."* Proyecto de Ley Exp. No. 14.785, Adición de un nuevo capítulo IV, denominado "del Recurso de Hábeas Data", al título III de la Ley de Jurisdicción Constitucional, Ley Nº 7135, de 19 de octubre de 1989, texto 18 de junio 2002, pasó a Comisión Permanente de Asuntos Jurídicos.

País	Constitución Política	Norma general	Normas en proyecto
Ecuador	El numeral 8 del artículo 23 de la Constitución garantiza la intimidad personal y familiar. Su numeral 21 del artículo 23 prohíbe la utilización de la información personal de terceros referentes a sus creencias religiosas, filiación política ni sus datos sobre salud y vida sexual. El artículo 94 de la Constitución de 1998 dispone lo siguiente: "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito" "Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. "Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización "La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional"	No existe norma general	No existe normas en proyecto
México	El artículo 16 de la Constitución de los Estados Unidos Mexicanos señala que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones. Del mismo modo regula casos relativos a la práctica de cateos, visitas domiciliarias, la exhibición de documentos y papeles personales, así como la violación de correspondencia.		Proyecto de decreto de Ley Federal de Protección de Datos personales 2001

País	Constitución Política	Norma general	Normas en proyecto
	Las disposiciones señaladas no se refieren específicamente a la regulación de los datos personales, sino al derecho a la privacidad.		
Perú	La Constitución Política de 1993, en el artículo 2°, inciso 6) establece el derecho: "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". A su vez el artículo 200º inciso 3) de la Constitución Política de 1993, establece la Garantía Constitucional del Hábeas Data (Ley Nº 26301 modificada por la Ley Nº 26545, y la Ley Nº 23506), que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5 y 6 de la Constitución. El artículo 2° inciso 5) que norma por primera vez el derecho a solicitar de cualquier entidad pública, sin expresar la causa, la información que requiera y a recibirla, salvo que esa información afecte la intimidad personal, o aquellas que expresamente se excluyan por ley o por razones de seguridad nacional. Es así que el derecho a la información ante una entidad pública encuentra como uno de sus límites a la intimidad personal. A su vez la misma norma constitucional protege el secreto bancario y la reserva tributaria, los cuales sólo pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del	No existe norma general	Anteproyecto de la ley de Protección de Datos Personales elaborado por la comisión especial constituida por el Poder Ejecutivo mediante la Resolu-ción Ministerial N° 094-2002-JUS. El 23 de julio de 2004 se publica en el Diario Oficial El Peruano para recibir comentarios. Proyecto de ley sobre la privacidad de los Datos Informáticos y la creación del Comisionado para la Protección de la Privacidad. Fecha de presentación 23-09-1999. Proponentes: cuatro congresistas

País	Constitución Política	Norma general	Normas en proyecto
	congreso con arreglo a ley y siempre que se refieran al caso investigado; el inciso 7) del mismo artículo, que reconoce los derechos a la intimidad, al honor y a la propia imagen; y por último el inciso 10) del referido artículo 2°, consagra también la reserva e inviolabilidad de las comunicaciones y documentos privados, los cuales no pueden ser abiertos, interceptados, intervenidos ni incautados sino por mandamiento motivado del Juez, con las garantías previstas en la Ley (Ley N° 27697, que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional) y guardando secreto de los asuntos ajenos al hecho que motiva su examen.		

Resumen de situación de protección de datos personales

País	Norma Constitucional	Hábeas Data	Ley o Proyecto de Ley Protección de Datos Personales
Chile	Art. 19 inc. 4 y 5.	Art. 16 Ley 19628	Ley chilena 19628 sobre la protección de la vida privada
Colombia	Art. 15	Proyecto de Ley Estatutaria 071-2005 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones. 10 de agosto de 2005. Art. 15 Constitución Política	Proyecto de ley estatutaria N° 143 de 2003 por la cual se dictan disposiciones para la protección de datos de carácter personal y se regula la actividad de recolección, tratamiento y circulación de los mismos.
Costa Rica	Art. 24	Proyecto de Ley No.14785 de adicionar un nuevo capítulo denominado Del Recurso de Habeas Data al Título III de la Ley 7135 de Jurisdicción Constitucional. El 18 junio 2002 pasó a estudio de la Comisión Permanente de Asuntos Jurídicos.	Proyecto de Ley No.15.178 Protección de la persona frente al tratamiento de sus datos personales, el 27 de marzo de 2003 pasó a estudio de la Comisión Permanente de Asuntos Jurídicos. Proyecto de Ley No.14029 de Acceso a Internet, con dictamen de mayoría de la Comisión Permanente de Asuntos Económicos, el 15 de mayo de 2001. Establece la prohibición de los proveedores de ceder los datos personales a terceros y la inviolabilidad de las comunicaciones y documentos privados por Internet.
Ecuador	Art. 23 inc. 8, 21	Art. 94 Constitución Política	Art. 9 Ley 67 de Comercio electrónico, firmas y mensajes de datos
México	Art. 16	Capítulo VI del Proyecto de Ley Federal de Protección de Datos Personales	Proyecto de decreto de Ley Federal de Protección de Datos personales del 2001
Perú	Art. 2 inc. 5, 6, 7, 10 Constitución Política	Art.200 inc. 3 Constitución Política, Ley 26301	Anteproyecto de ley de Protección de Datos Personales Resolución Ministerial N° 094-2002-JUS del 2004.

Anexo 4. Resumen de la normativa en materia de Comercio Electrónico. (Chile, Colombia, Costa Rica, Ecuador, México y Perú)

País	Ley modelo de comercio electrónico – CNUDMI- Firma digital
CHILE	Ley 19799 sobre documentos electrónicos, firma electrónica y servicios de certificación. Promulgada el 25 de marzo de 2002 y publicada el 12 de abril del 2002. La ley establece normas técnicas para la identificación de las distintas partes que participan en un intercambio comercial en línea y regula la forma de realizar trámites en la red. Así estará la firma electrónica avanzada que es la que asegurará la identidad, no repudiabilidad e integridad del mensaje. En tanto, dará seguridad jurídica al reconocer como plenamente válidos los actos y contratos celebrados por medios telemáticos y posibilitando que los medios electrónicos se presenten como medio de prueba en juicios.
COLOMBIA	La Ley 527 expedida el 18- ago- 1999 por el Congreso de la República, basada en la Ley Modelo propuesta por la CNUDMI con algunas adiciones, define y reglamenta el acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales, a la vez que se establecen las entidades de certificación. Decreto número 1747 de 2000 (septiembre 11) por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Ley 588 de 2000 (julio 5) por medio de la cual se reglamenta el ejercicio de la actividad notarial dándole la posibilidad de que sean entidades de certificación.
COSTA RICA	Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos del 30 de agosto de 2005, vigente desde el 13 de octubre del 2005. **Proyecto Ley de Comercio Electrónico No.16081 en estudio en la Comisión Permanente de Asuntos Jurídicos, el 6 de diciembre 2005, Este Proyecto de Ley regula el régimen jurídico aplicable a la prestación de servicios por Internet, que a sus efectos se denominarán contratos y obligaciones electrónicas, así como la responsabilidad derivada, las infracciones y sanciones.** **Decreto 33018 Reglamento a la Ley de Certificados, Firmas digitales y documentos electrónicos, 20 de marzo 2006.**
ECUADOR	Aprobada Ley 67 el 17 de abril de 2002. **Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.** Decreto 3496, RO/735 del 31 de diciembre de 2002, Reglamenta la Ley de Comercio Electrónico, Regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica, la prestación de servicios electrónicos (incluido el comercio electrónico) y la protección a los usuarios. Basada en la Ley Modelo propuesta por la CNUDMI con algunas adiciones
MEXICO	Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor. Del 23 de mayo de 2000 (D.O. 29 de mayo de 2000). Decreto de Reformas al Código de Comercio en Materia de Firma Electrónica vigente a partir 29 de agosto de 2003 El mismo adopta básicamente la ley modelo sobre firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) introduce en la legislación mexicana el concepto de firma electrónica fiable o avanzada y complementa la parte relativa a Mensaje de Datos detallando conceptos como Intermediario, Acuse de Recibo, Copia, Error, etc.
PERU	**Ley 27269 Ley de firmas y certificados digitales del 26 de mayo del 2000 y vigente del 15 de julio del 2000. Reglamento de la Ley de Firmas y Certificados Digitales, regula la utilización de la firma electrónica (decreto 19-2002-JUS).** Las disposiciones varían sustancialmente de las recomendaciones de la UNCITRAL.

Anexo 5. Aspectos regulados en las legislaciones de comercio electrónico

Objeto y ámbito de aplicación

Colombia: Ley 527

> "Art. No.1 Ámbito de Aplicación. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:
> a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;
> b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo." (Ley 527 de Colombia, 1999, p.1)

Ecuador: Ley 67

> "Art. 1.- Objeto de la ley.- Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas." (Ley 67 de Ecuador, 2002, p.1)

Perú: Ley 27269

No posee actualmente una legislación o proyecto de ley sobre mensajes de datos. Sin embargo, el Reglamento de la Ley 27.269 regula la utilización de firmas electrónicas en mensajes de datos y documentos electrónicos.

Chile: Ley 19799

> "Artículo 1º.- La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso." (Ley 19799 de Chile, 2002, p.1)

México: Decreto sobre firma electrónica del 29 de agosto del 2003, donde se agrega los Capítulos I, II, III y IV al Título Segundo al Libro Segundo del Código de Comercio

> "Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte." (Decreto sobre firma electrónica, 2003, p.1)

Costa Rica: Ley 8454

> "Artículo 1º—Ámbito de aplicación. Esta Ley se aplicará a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles." (Ley 8454 de Costa Rica, 2005, p.1)

Reconocimiento jurídico

Colombia: artículos 5, 10 y 28 de la Ley 527 de 1999.

> "Art. 5.- Reconocimiento Jurídico de los Mensajes de Datos.

No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos." (Ley 527 de Colombia, 1999, p.2)

"ARTICULO 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE 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 sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original." (Ley 527 de Colombia, 1999, p.3)

"ARTICULO 28. ATRIBUTOS JURIDICOS DE UNA FIRMA DIGITAL. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.
PARAGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:
1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional." ." (Ley 527 de Colombia, 1999, p.9)

Ecuador: artículo 2 y 14 de la Ley 67 del 2002.

"Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento." (Ley 67 de Ecuador, 2002, p.1).

"Art. 14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba enjuicio." (Ley 67 de Ecuador, 2002, p.3).

Perú: artículo 1 de la Ley 27269 del 2000, artículos 5, 6, 7 del Reglamento de la Ley 27269.

"Art. 1 La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad." (Ley 27269 de Perú, 2000, p.1).

"Artículo 5º .- Firmas en la Infraestructura Oficial de Firma Electrónica
Toda firma electrónica añadida o asociada lógicamente a un mensaje de datos o a un documento electrónico y generada bajo la Infraestructura Oficial de Firma Electrónica, cumple con lo dispuesto en la Ley y el Reglamento." (Reglamento de la ley 27269 de Perú, 2002, p. 4).

"Artículo 6º .- Validez de otras firmas electrónicas
Para efectos de la manifestación de voluntad, las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos o un documento electrónico y generadas fuera de la Infraestructura Oficial de Firma Electrónica tendrán la misma validez y eficacia jurídica que

las firmas manuscritas, siempre que sean acreditadas o reconocidas por la autoridad administrativa competente." (Reglamento de la ley 27269 de Perú, 2002, p. 4).

"Artículo 7º .- Documentos Firmados Electrónicamente como medio de prueba
Las firmas electrónicas así como los mensajes de datos y documentos firmados electrónicamente podrán ser admitidas como prueba en toda clase de procesos o procedimientos. El Juez podrá solicitar a la autoridad administrativa competente el nombramiento de un perito especializado en firmas electrónicas." (Reglamento de la ley 27269 de Perú, 2002, p. 4).

Chile: artículos 3, 5 de la Ley 19799 del 2002.

"Artículo 3º.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito." (Ley 19799 de Chile, 2002, p. 2).

"Artículo 5º.- Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes:..." (Ley 19799 de Chile, 2002, p. 2).

México: artículo 89 bis, 97 del Decreto sobre firma electrónica del 29 de agosto del 2003, donde se agrega los Capítulos I, II, III y IV al Título Segundo al Libro Segundo del Código de Comercio.

"Artículo 89 bis. No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos." (Decreto sobre firma electrónica de México, 2003, p. 2).

"Artículo 97. Cuando la Ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos." (Decreto sobre firma electrónica de México, 2003, p. 5).

Costa Rica: artículos 4, 9 de Ley 8454 del 2005.

"Artículo 4º—**Calificación jurídica y fuerza probatoria.** Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos. (Ley 8454 de Costa Rica, 2005, p. 4).

"Artículo 9º—**Valor equivalente.** Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.
Los documentos públicos electrónicos deberán llevar la firma digital certificada." (Ley 8454 de Costa Rica, 2005, p. 10).

Definición de Mensajes de Datos

Colombia:

"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." (Ley 527 de Colombia, 1999, p. 1).

Ecuador:

"Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos." (Ley 67 de Ecuador, 2002, p. 13)

Perú:

"Es la información generada, transmitida, recibida, archivada, comunicada por medios electrónicos, ópticos o cualquier otro análogo; tales como, el intercambio electrónico de datos (EDI, por sus siglas en inglés), el correo electrónico, el telegrama, el télex, el telefax, entre otros." (Reglamento de la Ley 27269 de Perú, 2002, p.4)

Chile:

Define Documento electrónico como "toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior." (Ley 19799 de Chile, 2002, p.1).

México:

"La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología." (Decreto de firma electrónica de México, 2003, p. 2).

Costa Rica:

"DOCUMENTO ELECTRÓNICO: Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático." (Ley 8454 de Costa Rica, 2005, p.3)

Definición de Firma Electrónica o Digital.

Colombia:

"Firma digital. 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." (Ley 527 de Colombia, 1999, p. 1).

Ecuador:

"Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos." (Ley 67 de Ecuador, 2002, p. 3).

Perú:

"Firma digital.- Aquella firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la Integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido. Firma electrónica.- Cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincular, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita." (Ley 27269 de Perú, 2000, p.2)

Chile:

"Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor; g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría." (Ley 19799, 2002, p.2)

México:

"Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio. Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica." (Decreto de Firma Electrónica de México, 2003, p.1)

Costa Rica:

"Entiéndase por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.

Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado." (Ley 8454 de Costa Rica, 2005, p. 9)

Fuerza probatoria

Colombia: arts. 10, 11 y 28 de la Ley 527 de 1999

"ARTICULO 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE 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 sólo hecho

que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original." (Ley 527 de Colombia, 1999, p. 3).

"ARTICULO 11. CRITERIO PARA VALORAR PROBATORIAMENTE UN MENSAJE DE DATOS. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente." (Ley 527 de Colombia, 1999, p. 3).

"ARTICULO 28. ATRIBUTOS JURIDICOS DE UNA FIRMA DIGITAL. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.
PARAGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:
1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional." (Ley 527 de Colombia, 1999, p. 9).

Ecuador: arts. 52, 54, 55 de la Ley 67 de 2002

"Art. 52.- Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil." (Ley 67 de Ecuador, 2002, p. 10)

"Art. 54.- Práctica de la prueba.- La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:
a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;
b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados; y,
c) El facsímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.
En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.
Cualquier duda sobre la validez podrá ser objeto de comprobación técnica." (Ley 67 de Ecuador, 2002, p. 10)

"Art. 55.- Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de

que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas." (Ley 67 de Ecuador, 2002, p. 11)

Perú: art. 7, 8 del Reglamento de la Ley 27269 de 2000

"Artículo 7º .- Documentos Firmados Electrónicamente como medio de prueba.

Las firmas electrónicas así como los mensajes de datos y documentos firmados electrónicamente podrán ser admitidas como prueba en toda clase de procesos o procedimientos. El Juez podrá solicitar a la autoridad administrativa competente el nombramiento de un perito especializado en firmas electrónicas." (Reglamento de la Ley 27269 de Perú, 2000, p. 4)

"Artículo 8º .- Presunciones acerca de las firmas electrónicas bajo la Infraestructura Oficial de Firma Electrónica

Tratándose de mensaje de datos o documentos firmados electrónicamente con firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, se presume que el documento o mensaje de datos fue enviado y firmado por su titular, de manera tal que identifica y vincula al firmante, y garantiza la autenticación e integridad del mismo.

Las disposiciones y presunciones del Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública." (Reglamento de la Ley 27269 de Perú, 2000, p. 5)

Chile: art. 3 y 5 de la Ley 19799 de 2002.

"Artículo 3º.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.

Lo dispuesto en el inciso anterior no será aplicable a los actos o contratos otorgados o celebrados en los casos siguientes:

a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico;

b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes, y

c) Aquellos relativos al derecho de familia.

La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en los artículos siguientes." (Ley 19799 de Chile, 2002, p. 2)

"Artículo 5º.- Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes:

1.- Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales, y

2.- Los que posean la calidad de instrumento privado tendrán el mismo valor probatorio señalado en el número anterior, en cuanto hayan sido suscritos mediante firma electrónica avanzada. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales." (Ley 19799 de Chile, 2002, p. 2)

México: art. 89, 89 bis del Decreto sobre firma electrónica del 29 de agosto del 2003, donde se agrega los Capítulos I, II, III y IV al Título Segundo al Libro Segundo del

Código de Comercio.

"Art. 89….**Firma Electrónica:** Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio." (Decreto de Firma Electrónica de México, 2003, p.1)

"Artículo 89 bis. No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos." (Decreto de Firma Electrónica de México, 2003, p.2)

Costa Rica: Art. 4 de la Ley 8454 del 2005.

"Artículo 4º—Calificación jurídica y fuerza probatoria. Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos." (Ley 8454 de Costa Rica, 2005, p.4)

Equivalencia Funcional

Colombia: artículos 6, 7, 8 Ley 527 de 1999.

"ARTICULO 6o. 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 de que la información no conste por escrito.

ARTICULO 7o. FIRMA. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;

b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

ARTICULO 8o. ORIGINAL. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original." (Ley 527 de Colombia, 1999, p.2).

Ecuador: artículos 6, 7 Ley 67 de 2002.

"Art. 6.- Información escrita.- Cuando la ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la

información que este contenga sea accesible para su posterior consulta." (Ley 67 de Ecuador, 2002, p. 1).

"Art. 7.- Información original.- Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos." (Ley 67 de Ecuador, 2002, p. 2).

Perú: no lo establece explícitamente, pero el artículos 5 y 6 del Reglamento a la Ley 27269 establece

"Artículo 5º.- Firmas en la Infraestructura Oficial de Firma Electrónica
Toda firma electrónica añadida o asociada lógicamente a un mensaje de datos o a un documento electrónico y generada bajo la Infraestructura Oficial de Firma Electrónica, cumple con lo dispuesto en la Ley y el Reglamento.
Artículo 6º .- Validez de otras firmas electrónicas
Para efectos de la manifestación de voluntad, las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos o un documento electrónico y generadas fuera de la Infraestructura Oficial de Firma Electrónica tendrán la misma validez y eficacia jurídica que las firmas manuscritas, siempre que sean acreditadas o reconocidas por la autoridad administrativa competente." (Reglamento de la Ley 27269, 2002, p. 4)

Chile: No lo establece explícitamente, sin embargo, el artículo 3 Ley 19799 da seguridad jurídica a las transacciones electrónicas.

"Artículo 3º.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito." (Ley 19799 de Chile, 2002, p.2)

"La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en los artículos siguientes." (Ley 19799 de Chile, 2002, p.2)

México: Artículo 89, 93, 93 bis, 97 del Decreto sobre firma electrónica del 29 de agosto del 2003, donde se agrega los Capítulos I, II, III y IV al Título Segundo al Libro Segundo del Código de Comercio.

"**Artículo 89.-** Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.
Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa." (Decreto sobre Firma Electrónica de México, 2003, p. 1)

"Artículo 93. Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.
Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.
Artículo 93 bis. Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la Ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos:
I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y
II. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar." (Decreto sobre Firma Electrónica de México, 2003, p. 4)

"Artículo 97. Cuando la Ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.
La Firma Electrónica se considerara Avanzada o Fiable si cumple por lo menos los siguientes requisitos:
I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;
II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;
III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y
IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.
Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable." (Decreto sobre Firma Electrónica de México, 2003, p. 4)

Costa Rica: artículo 3 y 9 de la Ley 8454 del 2005.

"Artículo 3º—**Reconocimiento de la equivalencia funcional.** Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.
En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular." (Ley 8454 de Costa Rica, 2005, p.3).
"Artículo 9º—**Valor equivalente.** Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.
Los documentos públicos electrónicos deberán llevar la firma digital certificada." (Ley 8454 de Costa Rica, 2005, p.10).

Neutralidad tecnológica

Colombia: no lo tiene expresamente en la Ley.

Ecuador: art. 10 Decreto 3496 de 2002.

> "Art. 10.- Elementos de la infraestructura de firma electrónica.- La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento." (Decreto 3496 de Ecuador, 2002, p. 3).

Perú: art. 9 del Reglamento de la Ley 27269 de 2002.

> "Artículo 9º .- Tecnologías de firmas electrónicas al interior de la Infraestructura Oficial de Firma Electrónica
> La Infraestructura Oficial de Firma Electrónica se puede basar en las siguientes tecnologías de firmas electrónicas:
> a) Tecnologías de firmas digitales, sobre la cual se basa la Infraestructura Oficial de Firma Digital.
> b) Otras tecnologías de firmas electrónicas que sean aprobadas por la autoridad administrativa competente de acuerdo con el principio de neutralidad tecnológica." (Reglamento de la Ley 27269 de Perú, 2002, p. 5).

Chile: art. 1 de la Ley 19799 del 2002.

> "Artículo 1º.- La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.
> Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel.
> Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados." (Ley 19799 de Chile, 2002, p.1).

México: Artículo 89 y 96 del Decreto sobre firma electrónica del 29 de agosto del 2003, donde se agrega los Capítulos I, II, III y IV al Título Segundo al Libro Segundo del Código de Comercio.

> "Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.
> Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa." (Decreto sobre Firma Electrónica de México, 2003, p.1).

> "Artículo 96. Las disposiciones del presente Código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una Firma Electrónica." (Decreto sobre Firma Electrónica de México, 2003, p.5).

Costa Rica: Art. 2 de la Ley 8454 del 2005.

"Artículo 2º—**Principios.** En materia de certificados, firmas digitales y documentos electrónicos, la implementación, interpretación y aplicación de esta Ley deberán observar los siguientes principios:

a) Regulación legal mínima y desregulación de trámites.
b) Autonomía de la voluntad de los particulares para reglar sus relaciones.
c) Utilización, con las limitaciones legales, de reglamentos autónomos por la Administración Pública para desarrollar la organización y el servicio, interno o externo.
d) Igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas." (Ley 8454 de Costa Rica, 2005, p.2).

Autonomía de la Voluntad

Colombia: art. 4 de la Ley 527 de 1999.

"ARTICULO 4o. MODIFICACION MEDIANTE ACUERDO. Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I, podrán ser modificadas mediante acuerdo." (Ley 527 de Colombia, 1999, p.2)

Ecuador: Artículo 48 y 49 del Título III, Capítulo III de la Ley 67 de 2002.

"Art. 48.- Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

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

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

Art. 49.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,
b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;

2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;

3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,

4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir." (Ley 67 de Ecuador, 2002, p.9).

Perú: art. 2 reglamento de la Ley 27269 de 2002.

"Artículo 2º.- Principio de la autonomía de la voluntad

Las disposiciones contenidas en el Reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la Infraestructura Oficial de Firma Electrónica, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en el artículo 1º de la Ley." (Reglamento de la Ley 27269 de Perú, 2002, p. 2).

Chile: No tiene expresado este principio dentro del texto de la Ley 19799.

México: Artículo 89, 90 bis, 91, 91 bis 94 del Decreto sobre firma electrónica del 29 de agosto del 2003, donde se agrega los Capítulos I, II, III y IV al Título Segundo al Libro Segundo del Código de Comercio.

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

Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa." (Decreto sobre Firma Electrónica de México, 2003, p.1).

"Artículo 90 bis.-..... Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del Emisor, se presumirá que se actuó con la debida diligencia si el método que usó el Destinatario o la Parte que Confía cumple los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas." (Decreto sobre Firma Electrónica de México, 2003, p.2).

"Artículo 91. Salvo pacto en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará como sigue: ..." (Decreto sobre Firma Electrónica de México, 2003, p.3).

"Artículo 91 bis. Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido cuando ingrese en un Sistema de Información que no esté bajo el control del emisor o del intermediario." (Decreto sobre Firma Electrónica de México, 2003, p.3).

"Artículo 94. Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido en el lugar donde el Emisor tenga su establecimiento y por recibido en el lugar donde el Destinatario tenga el suyo. Para los fines del presente artículo:..." (Decreto sobre Firma Electrónica de México, 2003, p.4).

Costa Rica: Art. 2 de la Ley 8454 del 2005.

"Artículo 2º—**Principios.** En materia de certificados, firmas digitales y documentos electrónicos, la implementación, interpretación y aplicación de esta Ley deberán observar los siguientes principios:

a) Regulación legal mínima y desregulación de trámites.

b) Autonomía de la voluntad de los particulares para reglar sus relaciones.

c) Utilización, con las limitaciones legales, de reglamentos autónomos por la Administración Pública para desarrollar la organización y el servicio, interno o externo.
d) Igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas." (Ley 8454 de Costa Rica, 2005, p.2).

Compatibilidad Internacional

Chile: art. 1, 15 de la Ley 19799 del 2002.

"Artículo 1º.- La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.
Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel." (Ley 19799 de Chile, 2002, p.1).

"Art. 15…Los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente." (Ley 19799 de Chile, 2002, p.6).

Colombia: art. 3 de la Ley 527 de 1999.

"ARTICULO 3o. INTERPRETACION. En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.
Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira." (Ley 527 de Colombia, 19991, p.2).

Costa Rica: art. 13 de la Ley 8454 del 2005.

"Artículo 13—**Homologación de certificados extranjeros.** Se conferirá pleno valor y eficacia jurídica a un certificado digital emitido en el extranjero, en cualesquiera de los siguientes casos:
a) Cuando esté respaldado por un certificador registrado en el país, en virtud de existir una relación de corresponsalía en los términos del artículo 20 de esta Ley.
b) Cuando cumpla todos los requisitos enunciados en el artículo 19 de esta Ley y exista un acuerdo recíproco en este sentido entre Costa Rica y el país de origen del certificador extranjero." (Ley 8454 de Costa Rica, 2005, p.14)

Ecuador: art. 28 de la Ley 67 del 2002.

"Art. 28.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta ley y su reglamento." (Ley 67 de Ecuador, 2002, p.5).

México: Artículo 89 y 114 del Decreto sobre firma electrónica del 29 de agosto del 2003, donde se agrega los Capítulos I, II, III y IV al Título Segundo al Libro Segundo del Código de Comercio.

"Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.
Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa." (Decreto sobre Firma Electrónica de México, 2003, p.1).

"Artículo 114. Para determinar si un Certificado o una Firma Electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:
I. El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado la Firma Electrónica, y
II. El lugar en que se encuentre el establecimiento del prestador de servicios de certificación o del Firmante.
Todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que un Certificado expedido en la República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por este Título.
Toda Firma Electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que una Firma Electrónica creada o utilizada en la República Mexicana si presenta un grado de fiabilidad equivalente.
A efectos de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente para los fines de los dos párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.
Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable." (Decreto sobre Firma Electrónica de México, 2003, p.9).

Perú: art. 48 del Reglamento a la Ley 27269 del 2002.

"Artículo 48º .- Reconocimiento de certificados emitidos por entidades extranjeras
La autoridad administrativa competente podrá reconocer certificados digitales emitidos por entidades extranjeras, de acuerdo con las prácticas y políticas que para tal efecto apruebe, las mismas que deben velar por el cumplimiento de las obligaciones y responsabilidades establecidas en el Reglamento u otra norma posterior. Asimismo, podrá autorizar la operación de aquellas entidades de certificación nacionales que utilicen los servicios de entidades de certificación extranjera, de verificarse tal supuesto, las entidades nacionales asumirán las responsabilidades del caso.

Para los efectos de lo dispuesto en el párrafo precedente, la entidad extranjera deberá comunicar a la autoridad administrativa competente el nombre de aquellas entidades de certificación que autorizarán las solicitudes de emisión de certificados digitales así como la gestión de los mismos.
La autoridad administrativa competente emitirá las normas que aseguren el cumplimiento de lo establecido en el presente artículo; así como los mecanismos adecuados de información a los agentes del mercado.” (Reglamento de la Ley 27269 de Perú, 2002, p. 14).

Anexo 6. Vacíos en la regulación costarricense

Debilidades de la Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos

Debilidad	**Comentario**
Referencia a firma digital	Es una tecnología particular de firma electrónica. Modificación a la Ley es difícil si la tecnología cambia. Ecuador, Chile y México se refieren a la firma electrónica. Colombia y Costa Rica se refieren a la firma digital. Perú se refiere a ambos términos.
Perfeccionamiento de contratos	No hay referencia al tiempo y lugar de perfección de contrato electrónico, ni los códigos civil y comercio. Colombia, Ecuador y México lo establecen como la Ley Modelo.
Legislación y jurisdicción aplicable	Importante incluir que en los casos que involucran a un consumidor, la legislación y jurisdicción aplicable será la de residencia habitual del consumidor, como lo hace Ecuador en su Ley 67 de Comercio Electrónico. Es importante también incorporar la posibilidad de arbitraje por medios electrónicos.
Protección al consumidor	Es importante que se haga referencia de la prevalencia de las normas de protección al consumidor, como lo hace Colombia en su Ley 527 de Comercio electrónico.
Infracciones informáticas	Es importante hacer un estudio exhaustivo de las infracciones informáticas e incluirlas en el Código Penal costarricense, Ecuador incluyó reformas al código penal en su ley 67.
Otras debilidades	Permiso para que las instituciones públicas otorguen certificados a sus funcionarios (más de una autoridad raíz). Puede haber problemas de interoperabilidad que hace difícil la compatibilidad de certificados extendidos por diferentes autoridades certificadoras raíces. El cese de actividades de un Certificador no debería afectar la vigencia de los certificados que éste ya había extendido. Se requiere que se establezca explícitamente cómo se abordará estos casos sin afectar a las personas que recibieron certificados extendidos por el Certificador antes de su cese de actividades. La garantía de fidelidad puede ser por hipoteca, fianza o póliza de fidelidad de un ente asegurador, o un depósito en efectivo. Más bien, se debería establecer que la garantía de fidelidad sólo podrá ser por depósito en efectivo. Conveniencia de designar al Ministerio de Ciencia y Tecnología como Autoridad Certificadora Raíz, por su capacidad para montar la infraestructura de Clave Pública requerida. La jefatura de la Dirección de Certificadores de Firma Digital será nombrada por el ministro de Ciencia y Tecnología y será un funcionario de confianza. Es necesario explicitar jurídicamente la regulación de las entidades de certificación, que incluya además los siguientes elementos: tipo de productos que pueden brindar, los servicios concatenados a tales productos, controles administrativos a partir de la inscripción de un registro de estas entidades, entre otros.

Vacíos en la regulación del comercio electrónico, proyectos de ley, normativa existente.

Vacío	**Ley 8454**	**Proyecto Ley 14029 de Acceso a Internet**	**Proyecto de Ley 16081 de comercio electrónico**	**Código Civil**	**Código Comercio**
Identificación del proveedor en la publicidad					
Obligación de ambas partes de firmar digitalmente el contrato	Art.9 Los documentos públicos electrónicos deberán llevar la firma digital certificada. Art. 12. Mecanismos. Con las limitaciones de este capítulo, el Estado, las instituciones públicas y las empresas públicas y privadas, las personas jurídicas y los particulares, en general, en sus diversas relaciones, estarán facultados para establecer los mecanismos de certificación o validación que convengan a sus				

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
	intereses. Para tales efectos podrán: inc. c) De consumo, instituir mecanismos de certificación para la emisión, la recepción y el intercambio de documentos electrónicos y firmas asociadas, para relaciones jurídicas concretas.				
Protección de los datos personales		Art.6 Derechos de los usuarios del servicio de Internet. g) La confidencialidad de los datos y la información personal que faciliten al proveedor, quien no podrá publicarlos ni proporcionárselos a terceros, sin la autorización expresa del usuario.			
Cookies, SPAM					
Cláusulas abusivas en contratos electrónicos					
Lugar y momento de perfección del contrato electrónico			Art. 5. Formalización. Se entenderá por contrato formalizado por vía	**ARTÍCULO 1012.-** Si las partes no estuvieren reunidas, la aceptación debe	**ARTÍCULO 443.-** En la compra-venta que se negoció por correspondencia

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
			electrónica el celebrado sin la presencia simultánea de las partes, prestando su consentimiento en origen y en destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, conectados por medio de cable, radio o medios ópticos o electromagnéticos. El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes civiles y comerciales y se tendrá como lugar de perfeccionamiento el que acordaren las partes, en su defecto el domicilio de quien recibió el servicio. Art.6 Consentimiento. La validez del consentimiento del	hacerse dentro del plazo fijado por el proponente para este objeto. Si no se ha fijado plazo, se tendrá por no aceptada la propuesta, si la otra parte no respondiere dentro de tres días cuando se halle en la misma provincia; dentro de diez, cuando no se hallare en la misma provincia, pero sí en la República; y dentro de sesenta días, cuando se hallare fuera de la República. **ARTÍCULO 1013.-** El proponente está obligado a mantener su propuesta, mientras no reciba respuesta de la otra parte en los términos fijados en el artículo anterior. **ARTÍCULO 1049.-** La venta es perfecta entre las partes desde que convienen en cosa y	privarán las siguientes reglas: a) Si el proponente fija un término de espera, estará obligado a mantener su oferta hasta ese día; y b) Si no fija fecha de espera, estará obligado a mantener su oferta cinco días, si se trata de la misma plaza; si se trata de otra plaza dentro del territorio nacional, diez días; y si es en el exterior, un mes. Estos términos se contarán desde el día en que el proponente deposite la oferta en las oficinas de correos. **ARTÍCULO 444.-** El contrato quedará perfecto desde el momento en que, dentro de los

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
			contrato electrónico estará sujeta a la existencia de mecanismos tecnológicos que indubitablemente tengan tal finalidad. La recepción, confirmación de recepción o apertura de mensajes de datos o telecomunicaciones en general, salvo acuerdo previo en contrario, se considerarán como propuestas o tratativas y no implican aceptación del contrato electrónico.	precio. **ARTÍCULO 1053.-** Si la promesa de vender una cosa mediante un precio determinado o determinable ha sido aceptada, da derecho a las partes para exigir que la venta se lleve a efecto.	términos indicados en el artículo anterior, el proponente reciba comunicación de la otra parte aceptando pura y simplemente. Si la contestación contuvi ere algunas modificaciones o condiciones, el contrato no se perfeccionará hasta tanto el proponente original no acepte los cambios y así lo haga saber. Esa contestación, por su parte, producirá el perfeccionamiento del contrato, cuando llegue a poder del posible comprador.
Capacidad contractual			Art.4. Capacidad, legitimación y titularidad. La capacidad para contraer obligaciones y celebrar contratos electrónicos se		

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
			presume; sin menoscabo del derecho de retracto cuando este proceda, serán válidas las contrataciones y obligaciones contraídas cuando sean realizadas por un tercero que ha tenido acceso consentido a la identificación del titular, en caso contrario serán absolutamente nulas.		
Información por parte del Estado de las empresas autorizadas a vender por Internet					
Utilización de mecanismos tecnológicos seguros en las transacciones electrónicas					
Responsabilidad del proveedor por pérdidas por violación a la seguridad en la transmisión en la Red		Art.6 Derechos de los usuarios del servicio de Internet. b) La inviolabilidad y secreto de l comunicaciones documentos privados p medio de “Interne conforme a lo dispues por el artículo 24 de			

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
		Constitución Política y lo artículos 1 y 9 de la Ley Registro, Secuestro Examen de Document Privados e Intervención las Comunicaciones, l 7425 del 9 de agosto 1994 y sus reformas. L proveedores del servi deberán garantizar inviolabilidad y el secre de aquellos dat transmitidos por l usuarios y de información personal q sea confidencial.			
Educación al consumidor sobre comercio electrónico seguro					
Derecho de devolución del consumidor en compras por Internet			Art.7 Competencia y derechos del consumidor. La interpretación y aplicación de las normas relativas a obligaciones y contratos electrónicos debe efectuarse de manera que no menoscabe la promoción de la competencia ni la efectiva defensa del		**ARTÍCULO 450.-** El comprador que al tiempo de recibir la cosa la examina y prueba a satisfacción, no tendrá derecho para repetir contra el vendedor alegando vicio o defecto de cantidad o calidad. El comprador

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
			consumidor; en este último caso se entienden incorporados todos los derechos y obligaciones de usuarios y consumidores previstos en la legislación nacional.		tendrá derecho a repetir contra el vendedor por esos motivos, si hubiere recibido la cosa enfardada o embalada, siempre que dentro de los cinco días siguientes al de su recibo manifieste por escrito al vendedor o a su representante vicio o defecto que proceda de caso fortuito o fuerza mayor o deterioro por la naturaleza misma de las cosas. El vendedor podrá exigir que en el acto de la entrega se haga un reconocimiento en cuanto a calidad y cantidad. Hecho ese reconocimiento en presencia del comprador o de su encargado de recibir mercadería, si éstos se dan por

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
					satisfechos, no cabrá ulterior reclamo. Si los vicios fueren ocultos, el comprador deberá denunciarlos por escrito al vendedor o su representante, dentro de los diez días a partir de la entrega, salvo pacto en contrario. La acción judicial prescribirá en tres meses contados desde la entrega. **ARTÍCULO 469.-** Si el comprador devuelve la cosa comprada y el vendedor la acepta, o si habiéndole sido devuelta contra su voluntad, no la hace depositar judicialmente dentro de los cinco días siguientes, con notificación del depósito al comprador, se

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
					presume que el vendedor ha consentido en la rescisión del contrato.
Legislación aplicable y jurisdicción competente donde reside el consumidor			Art.8. Prueba. La prueba de las obligaciones y contratos celebrados por vía electrónica se regirá por las reglas generales del Derecho común y en caso de duda deberá estarse a lo más favorable al consumidor o usuario. Art.9. Jurisdicción. En caso de controversias la jurisdicción costarricense será competente si al menos uno, el receptor o el prestador del servicio, tienen su domicilio en Costa Rica. En el supuesto de que alguna de las partes no tenga domicilio nacional deberá notificársele por vía consular la articulación o demanda	**ARTÍCULO 26.-** La prescripción y todo lo que concierna al modo de cumplir o extinguir las obligaciones que resulten de cualquier acto jurídico o contrato que haya de ejecutarse en Costa Rica, se regirá por las leyes costarricenses, aunque los otorgantes sean extranjeros, y aunque el acto o contrato no se haya ejecutado o celebrado en la República. **ARTÍCULO 27.-** Para la interpretación de un contrato y para fijar los defectos mediatos o inmediatos que de él resulten, se recurrirá a las leyes del lugar donde se hubiere celebrado el contrato;	**ARTÍCULO 477.-** Si el comprador rehusare, sin justa causa, recibir los efectos comprados, el vendedor podrá solicitar la resolución del contrato, con indemnización de perjuicios, o el pago del precio con los intereses legales, consignando las mercaderías a disposición del Juez competente del lugar indicado para la entrega, consignación que hará por los trámites establecidos para los actos de jurisdicción voluntaria, para que éste ordene su

Vacío	Ley 8454	Proyecto Ley 14029 de Acceso a Internet	Proyecto de Ley 16081 de comercio electrónico	Código Civil	Código Comercio
			interpuesta. Sin perjuicio de las medidas cautelares de bloqueo, cuando no sea posible determinar el domicilio de una de las partes, procederá el nombramiento de curador ad litem.	pero si los contratantes tuvieren una misma nacionalidad, se recurrirá a las leyes de su país. Artículo 1023. 2.- A solicitud de parte los tribunales declararán la nulidad absoluta de las siguientes cláusulas contractuales: d) La de reenvío a una ley extranjera para aplicarla a la ejecución o interpretación del contrato, con el fin de impedir que rijan los preceptos nacionales que protegen al consumidor;	depósito o venta por cuenta del comprador, según la naturaleza de la cosa. El vendedor podrá igualmente solicitar el depósito judicial, cuando el comprador retardare la recepción de los efectos; y en este caso, serán de cargo de éste los gastos de traslación al depósito y conservación de los mismos.
Comisión Internacional de Controversias					

ANEXO 7. Leyes Modelos de la CNUDMI

Ley Modelo de la CNUDMI sobre Comercio Electrónico

PRIMERA PARTE, COMERCIO ELECTRÓNICO EN GENERAL

CAPÍTULO I. DISPOSICIONES GENERALES

Articulo 1. **Ámbito de aplicación***

La presente Ley** será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto*** de actividades comerciales ****

Artículo 2. **Definiciones**

Para los fines de la presente Ley:

a) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, óptimos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax;

b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;

c) Por "iniciador" de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él;

d) Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no éste actuando a título de intermediario con respecto a él;

e) Por "intermediario", en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;

f) Por "sistema de información" se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3**. Interpretación**

1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

2) Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4. **Modificación mediante acuerdo**

1) Salvo que se disponga otra cosa, en las relaciones entre las partes que generan envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III podrán ser modificadas mediante acuerdo.

2) Lo dispuesto en el párrafo 1) no afectará a ningún derecho de que gocen las partes modificar de común acuerdo alguna norma jurídica a la que se haga referencia en el capítulo II.

CAPITULO II

APLICACIÓN DE LOS REQUISITOS JURÍDICOS A LOS MENSAJES DE DATOS.

Artículo 5. Reconocimiento jurídico de los mensajes de datos

No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.

Artículo 6**. Escrito**

1) Cuando la ley 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 ulterior consulta.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.

3) Lo dispuesto en el presente artículo no será aplicable a: [....] .

Artículo 7. **Firma**

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

3) Lo dispuesto en el presente artículo no será aplicable a: [...] .

Artículo 8. **Original**

1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:

a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

3) Para los fines del iniciso a) del párrafo 1):

a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y

b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

4) Lo dispuesto en el presente artículo no será aplicable a: [...] .

Artículo 9. **Admisibilidad y fuerza probatoria de los mensajes de datos.**

1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:

a) Por la sola razón de que se trate de un mensaje de datos; o

b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la

que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 10. **Conservación de los mensajes de datos**

1) Cuando la ley requiera que ciertos documentos, registro o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

a) Que la información que contengan sea accesible para su ulterior consulta; y

b) Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y

c) Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.

2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.

3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos. a), b) y c) del párrafo 1).

CAPÍTULO III COMUNICACIÓN DE LOS MENSAJES DE DATOS

Artículo 11. **Formación y validez de los contratos**

1) En la formación de un contrato, de no convenir las partes otra cosa, 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 sola razón de haberse utilizado en su formación un mensaje de datos.

2) Lo dispuesto en el presente artículo no será aplicable a: [...] .

Artículo 12. **Reconocimientos por las partes de los mensajes de datos**

1) En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

2) Lo dispuesto en el presente artículo no será aplicable a: [...] .

Artículo 13. **Atribución de los mensajes de datos**

1) Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador.

2) En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:

a) Por alguna persona facultada para actuar en nombre del iniciado respecto de ese mensaje; o

b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

3) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de datos proviene del iniciador, y a actuar en consecuencia, cuando:

a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o

b) El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

4) El párrafo 3) no se aplicará:

a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o

b) En los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.

5) Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el mensaje de datos recibido.

6) El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado y a actuar en consecuencia, salvo

en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos era un duplicado.

Artículo 14. **Acuse de recibo**

1) Los párrafos 2) a 4) del presente artículo serán aplicable cuando, al enviar o antes de enviar un mensaje de datos, el iniciador solicite o acuerde con el destinatario que se acuse recibo del mensaje de datos.

2) Cuando el iniciador no haya acordado con el destinatario que el acuse de recibo se dé en alguna forma determinada o utilizando un método determinado, se podrá acusar recibo mediante:

a) Toda comunicación del destinatario, automatizada o no, o

b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

3) Cuando el iniciador haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo.

4) Cuando el iniciador no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo razonable el iniciador:

a) Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y

b) De no recibirse acuse dentro del plazo fijado conforme al inciso a), podrá dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.

5) Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente. Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido.

6) Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

7) Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.

Artículo 15**. Tiempo y lugar del envío y la recepción de un mensaje de datos**

1) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos en nombre del iniciador.

2) De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:

a) Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar:

i) En el momento en que entre el mensaje de datos en el sistema de información designado; o

ii) De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar al entrar el mensaje de datos en un sistema de información del destinatario.

3) El párrafo 2) será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje conforme al párrafo 4).

4) 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 párrafo:

a) Si el iniciador o el 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 tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

5) Lo dispuesto en el presente artículo no será aplicable a: [...] .

SEGUNDA PARTE. COMERCIO ELECTRÓNICO EN MATERIAS ESPECÍFICAS

CAPITULO I. TRANSPORTE DE MERCANCÍAS

Artículo 16. **Actos relacionados con los contratos de transporte de mercancías**

Sin perjuicio de b dispuesto en la parte I de la presente Ley, el presente capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea exhaustiva:

a) i) indicación de las marcas, el número, la cantidad o el peso de las mercancías;

ii) declaración de la índole o el valor de las mercancías;

iii) emisión de un recibo por las mercancías;

iv) confirmación de haberse completado la carga de las mercancías;

b) i) notificación a alguna persona de las cláusulas y condiciones del contrato;

ii) comunicación de instrucciones al portador;

c) i) reclamación de la entrega de las mercancías;

ii) autorización para proceder a la entrega de las mercancías;

iii) notificación de la pérdida de las mercancías o de los daños que hayan sufrido;

d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato;

e) promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;

f) concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;

g) adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Artículo 17. **Documentos de transporte**

1) Con sujeción a lo dispuesto en el párrafo 3), en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 16 se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no se lleva a cabo el acto por escrito o mediante un documento.

3) Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o está adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o la utilización, de un documento, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

4) Para los fines del párrafo 3), el nivel de fiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

5) Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) artículo 16), no será válido ningún documento utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos. Todo documento que se emita en esas circunstancias deberá contener una declaración a tal efecto. La sustitución de mensajes de datos por documentos no afectará a los derechos ni a las obligaciones de las partes.

6) Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia, en un documento, esa norma no dejará de aplicarse a dicho contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en un documento.

7) Lo dispuesto en el presente artículo no será aplicable a: [...] .

NOTAS

* La Comisión sugiere el siguiente texto para los Estados que deseen limitar el ámbito de aplicación de la presente Ley a los mensajes de datos internacionales:

La presente Ley será aplicable a todo mensaje de datos que sea conforme a la definición del párrafo 1) del artículo 2 y que se refiera al comercio internacional.

** La presente ley no deroga ninguna norma jurídica destinada a la protección del consumidor.

*** La Comisión sugiere el siguiente texto para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en las situaciones siguientes: [....] .

**** El término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. La relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de facturaje ("factoring"); de arrendamiento de bienes de equipo con opción de compra ("leasing"); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Ley Modelo de la CNUDMI para Firma Electrónica 2001

(Aprobada por el Grupo de Trabajo de la CNUDMI sobre Comercio Electrónico en su 37º período de sesiones, celebrado del 18 al 29 de septiembre de 2000 en Viena).

Artículo 1. Ámbito de aplicación

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No derogará ninguna norma jurídica destinada a la protección del consumidor.

* La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

"La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [Y]."

** El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin que esta lista sea taxativa, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje (Afactoring@); arrendamiento con opción de compra (Aleasing@); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

Artículo 2. Definiciones

Para los fines de la presente Ley:

a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el
mensaje de datos;

b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

c) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

d) Por "firmante" se entenderá la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona a la que representa;

e) Por “prestador de servicios de certificación” se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;

f) Por “parte que confía” se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3. Igualdad de tratamiento de las tecnologías para la firma
Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 4. Interpretación
1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe.

2) Las cuestiones relativas a materias que se rijan por la presente Ley y que no estén expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que se inspira.

Artículo 5. Modificación mediante acuerdo
Las partes podrán hacer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 6. Cumplimiento del requisito de firma
1) Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan fiable como resulte apropiado a los fines para los cuales se generó o comunicó ese mensaje.

2) El párrafo 1) será aplicable tanto si el requisito a que se refiere está expresado en la forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3) La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) cuando uno de los objetivos del requisit o legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4) Lo dispuesto en el párrafo 3) se entenderá sin perjuicio de la posibilidad de que cualquier persona:
a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1), la fiabilidad de una firma electrónica; o
b) aduzca pruebas de que una firma electrónica n o es fiable.

5) Lo dispuesto en el presente artículo no será aplicable a: [Y].

Artículo 7. Cumplimiento de lo dispuesto en el artículo 6

1) [La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia] podrá determinar
qué firmas electrónicas cumplen lo dispuesto en el artículo 6.

2) La determinación que se haga con arreglo al párrafo 1) deberá ser compatible con las normas o criterios internacionales reconocidos.

3) Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 8. Proceder del firmante
1) Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) dar aviso sin dilación indebida a cualquier persona que, según pueda razonablemente prever, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:
i) sabe que los datos de creación de la firma han quedado en entredicho; o
ii) las circunstancias de que tiene conocimiento dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con su ciclo vital o que hayan de consignarse en él sean exactas y cabales.

2) El firmante incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

Artículo 9. Proceder del prestador de servicios de certificación

1) Cuando un prestador de servic ios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él sean exactas y cabales;

c) proporcionar medios de acceso razonablemente fácil que permitan a la parte que confía en el certificado determinar mediante éste:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar medios de acceso razonablemente fácil que, según proceda, permitan a la parte que confía en el certificado determinar mediante éste o de otra manera:

i) el método utilizado para identificar al firmante;

ii) cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8;

vi) si se ofrece un servicio de revocación oportuna del cert ificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que exista un servicio de revocación oportuna del certificado;

f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

2) El prestador de servicios de certificación incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

Artículo 10. Fiabilidad

A los efectos del apartado f) del párrafo 1) del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de un activo;

b) la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;

e) la periodicidad y el alcance de la auditoría por un órgano independiente;

f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; y

g) cualesquiera otros factores pertinentes.

Artículo 11. Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o

b) cuando la firma electrónica esté refrendada por un certificado:
i) verificar la validez, suspensión o revocación del certificado; y
ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12. Reconocimiento de certificados y firmas electrónicas extranjeros

1) Al determinar si un certificado o una firma electrónica produce efectos jurídicos, o en qué medida los produce, no se tomará en consideración:
a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni
b) el lugar en que se encuentre el establecimiento del expedidor o firmante.

2) Todo certificado expedido fuera *[del Estado promulgante]* producirá los mismos efectos jurídicos en *[el Estado promulgante]* que todo certificado expedido en *[el Estado promulgante]* si presenta un grado de fiabilidad sustancialmente equivalente.

3) Toda firma electrónica creada o utilizada fuera *[del Estado promulgante]* producirá los mismos efectos jurídicos en *[el Estado promulgante]* que toda firma electrónica creada o utilizada en *[el Estado promulgante]* si presenta un grado de fiabilidad sustancialmente equivalente.

4) A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de párrafo 2),

o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5) Cuando, sin perjuicio de lo dispuesto en los párrafos 2), 3) y 4), las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Anexo 8. Los 50 sitios más populares de Costa Rica en Internet

(actualizado al 30 de mayo 2004), según un sondeo efectuado por *La Nación*, basado en el *ranking* de Alexa.com (compañía subsidiaria de Amazon.com)

Sitio web	Dirección en Internet	Lugar en el ranking
Nación.com	www.nacion.com	8.349
Navégalo.com	www.navegalo.com	12.741
Tía Zelmira.com	www.tiazelmira.com	18.218
Costarricense.cr	www.costarricense.cr	20.895
Racsa	www.racsa.co.cr	20.991
Diario Extra	www.diarioextra.com	29.515
REPRETEL	www.repretel.com	38.324
Banco Nacional	www.bncr.fi.cr	38.869
Registro Nacional	www.registronacional.go.cr	39.499
Teletica Canal7	www.teletica.com	40.327
Unafut	www.unafut.com	46.935
Periódico Al Día	www.aldia.co.cr	47.392
Universidad Nacional	www.una.ac.cr	50.971
Neopostal	www.neopostal.com	53.675
Interligas.com	www.interligas.com	54.078
Costa Rica.com	www.costarica.com	55.200
Ticopage.com	www.ticopage.com	56.113
Mundo Motorizado	www.mundomotorizado.com	58.215
CR Autos	www.crautos.com	58.406
Universidad de Costa Rica	www.ucr.ac.cr	60.843
Terra Costa Rica	www.terra.co.cr	61.418
Banco de Costa Rica	www.bancobcr.com	63.941
A. M. Costa Rica	www.amcostarica.com	66.867
La Prensa Libre	www.prensalibre.co.cr	70.082
Costa Rica´s Travel Net	www.centralamerica.com	70.261
Grupo ICE	www.grupoice.com	75.008
Merca Hosting	www.mercahosting.com	78.263
Amnet (TV por cable)	www.amnet.co.cr	78.869
Aliter Corporation	www.alitercorp.com	82.806
Visit Costa Rica	www.visitcostarica.com	83.769
Banco Central de Costa Rica	www.bccr.fi.cr	88.619
Cable Virtual	www.cablevirtual.com	91.657
Conexión Vip.com	www.conexionvip.com	92.702
SuperPages CR	www.superpagescr.com	96.695
Alexandre Guimaraes	www.aguima.com	98.917
Economicos.com (Grupo Nación)	www.economicos.com	103.191
Radio Dos	www.radiodos.com	107.316
Empleos.Net	www.empleos.net	110.176
Solo nosotras.com	www.solonosotras.com	114.182
Radio Monumental	www.monumental.co.cr	120.376
Periódico Tico Times	www.ticotimes.net	128.759
Poder Judicial	www.poder-judicial.go.cr	131.478
Galadia.com	www.galadia.com	134.091
Costa Rica In Focus	www.zurqui.co.cr	139.989
Costa Rica Online Travel	www.costaricaonlinetravel.com	142.800
La República	www.larepublica.net	145.485
Novaq	www.novaq.com	146.690
Instituto Tecnológico	www.itcr.ac.cr	150.001
Everardo Herrera.com	www.everardoherrera.com	150.668
Radio Columbia	www.columbia.co.cr	150.812
Imprevia.com	www.imprevia.com	152.951

(Fuente: Ticopage.com, 2004)

Anexo 9. Propuesta de Proyecto de Ley Marco de Protección del Consumidor.

Capítulo I. Definiciones

Artículo 1.- Para los efectos de esta Ley, se entenderá por:

Anunciante: aquel proveedor de bienes o servicios que ha encargado la difusión pública de un mensaje publicitario o de cualquier otro tipo de información referida a productos o servicios;

Consumidor: toda persona natural o jurídica que como destinatario final adquiera, utilice o disfrute bienes o servicios, o reciba oferta para ello. Cuando la presente Ley aluda al consumidor, dicha denominación incluirá al usuario;

Contrato de adhesión: aquel contrato cuyas cláusulas hayan sido establecidas unilateralmente por el proveedor, sin que el consumidor haya discutido su contenido. La discusión o modificación de una o más cláusulas no modifica su carácter original;

Documento electrónico: manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático

Garantía: el compromiso que adquiere el productor o proveedor de un bien o servicio, durante un tiempo, del buen funcionamiento de algo que vende, y repararlo gratuitamente en caso de avería.

Información: los datos, instructivos, antecedentes, indicaciones o contraindicaciones que el proveedor debe suministrar obligatoriamente al consumidor al momento de efectuar la entrega del bien o la prestación del servicio;

Producto: Todo bien o servicio.

Productor: Para efectos de la responsabilidad por producto defectuoso, se entiende por productor todo aquel que fabrica un producto acabado, que produce una materia prima o que fabrica una parte integrante, y toda aquella persona que se presente como productor poniendo su nombre, marca o cualquier otro signo distintivo. Los importadores se reputan productores respecto de los bienes que introduzcan al mercado. Para los demás efectos de la presente Ley, el término productor estará comprendido en el de proveedor.

Promociones y ofertas: Ofrecimiento temporal de productos o servicios de manera gratuita o en condiciones especiales, como incentivo para el consumo. Se tendrá también por promoción, el ofrecimiento de productos con un contenido adicional a la presentación habitual, en forma gratuita o a precio reducido, así como el que se haga por el sistema de incentivos al consumidor, tales como rifas, sorteos, concursos y otros similares, en dinero, en especie o con acumulación de puntos.

Proveedor: toda persona natural o jurídica que participe de forma directa en la cadena de producción o distribución de bienes y servicios, por los que cobre precio o tarifa. Se entiende por tanto incluido quien produzca, fabrique, importe, preste un servicio, elabore, procese, transforme, o de cualquier forma extraiga, industrialice o transforme bienes intermedios o finales para la provisión de los consumidores, o quien distribuya, comercialice, provea, venda u ofrezca al público en general o a parte de él bienes o servicios destinados al consumo.

Publicidad: toda comunicación que pretenda influenciar a los consumidores en la decisión de adquirir un producto.

Publicidad engañosa: toda aquella publicidad que induzca a error, engaño o confusión.

Relación de consumo: Transacción comercial que se realiza entre un proveedor y un consumidor.
Servicio posventa: Servicio que asegura el mantenimiento preventivo y correctivo, el cumplimiento de la garantía y la reposición de partes, piezas y accesorios para bienes durables, por su tiempo de vida útil.

Capítulo II. Del Objeto, Principios y Ámbito De Aplicación
Artículo 2.- La presente ley es de orden público e interés social y de observancia en toda la República. Sus disposiciones son irrenunciables y contra su observancia no podrán alegarse costumbres, usos, prácticas, convenios o estipulaciones en contrario. La presente Ley tiene por objeto proteger, promover y garantizar la efectividad y el libre ejercicio de los derechos de los consumidores, así como salvaguardar su unidad y amparar el respeto a su dignidad y a sus intereses económicos, regulando las relaciones entre proveedores y consumidores, y procurando la equidad y la seguridad jurídica en las relaciones entre las partes incluyendo el ámbito del comercio electrónico.
Artículo 3.- Esta Ley es aplicable a las personas naturales o jurídicas de derecho privado, que tengan el carácter de productor o proveedor, en los términos del artículo primero de la presente Ley.
En lo no regulado por esta Ley, se acudirá a las normas existentes en el país donde resida el consumidor. En caso de duda en la interpretación de esta Ley, se la aplicará en el sentido más favorable al consumidor.
No se podrá renunciar anticipadamente a los derechos y obligaciones consagrados en esta Ley.
Artículo 4.- Las normas internas o supranacionales que traten de la protección del consumidor en sectores específicos de la economía se aplicarán preferentemente por especialidad, pero su interpretación deberá ser con base en los principios y el espíritu de la presente Ley.

Capítulo III. Sobre los Derechos de los Consumidores
Artículo 5.- Todo consumidor tiene los siguientes derechos:
1) Derecho a la protección de la salud, seguridad e intimidad.
i. Los bienes y servicios que se comercialicen, utilizados en condiciones normales o previsibles, no deben presentar riesgos para la salud y la seguridad. Si presentan tales riesgos deberán retirarse del mercado por medio de procedimientos rápidos y simples.
ii. Los proveedores no pueden utilizar los datos personales del consumidor en forma abusiva.
iii. Proteger el derecho de los consumidores de: acceso, oposición, rectificación, fijar el nivel de seguridad, uso conforme al fin de sus datos personales.
iv. Prohibición de interconexión de archivos para obtener un perfil de sus intereses o de su vida privada.
v. Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente.

2) Derecho a la protección de sus intereses económicos, con una distribución equitativa de riesgos y responsabilidades que refleje en especial la responsabilidad del proveedor al optar por medios electrónicos de comercio y

con inclusión, en particular, de las condiciones necesarias para que el consumidor pueda tomar decisiones ponderadas. En especial tendrán derecho a:
i. Protección frente contratos de adhesión con cláusulas abusivas, las condiciones abusivas de crédito, la solicitud de pago de mercancías no solicitadas y los métodos de venta agresivos.
ii. Protección frente a perjuicios causados a los intereses económicos por productos defectuosos o servicios insuficientes. Cumplimiento efectivo de la garantía.
iii. Servicio de posventa adecuado en bienes de consumo duraderos.
iv. Posibilidad de comparar y elegir libremente.
v. Asesoramiento y asistencia jurídica en caso de perjuicios sufridos por productos defectuosos.
vi. Justa reparación de daños y perjuicios, mediante procesos rápidos, eficaces y poco costosos.

3) Derecho a la protección contra prácticas de comercialización no solicitadas, engañosas y desleales, incluida la publicidad, y el apoyo a que se pongan a disposición del consumidor medios fiables para filtrar contenido de los sistemas de comunicación.
i. Protección a presentaciones y promociones de bienes o de servicios engañosos.
ii. Protección a la publicidad que induzca a error.
iii. Protección del consumidor contra publicidad comercial no solicitada enviada por correo electrónico.
iv. Protección del consumidor contra la violación de la privacidad de los cookies.

4) Derecho a la información y a la educación.
i. Información suficiente que permita al consumidor:
a. Conocer las características esenciales de los bienes y servicios que le ofrecen.
b. Efectuar una elección racional.
c. Utilizar dichos productos y servicios con seguridad y de manera satisfactoria.
d. Conocer el tiempo esperado de vida útil de un bien, según sus características de fabricación, en condiciones normales de uso y mantenimiento.
e. Identificación exacta y ubicación del proveedor.
f. Procedimientos para reclamos en caso de conflictos.
g. Probar la autenticidad de cada uno de los elementos de una transacción.
h. Conocer las medidas de seguridad que debe tomar en compras realizadas por medios electrónicos.

ii. Disponer medios educativos para los niños, jóvenes y adultos, para que puedan actuar como consumidores informados, capaces de elegir con claridad y conscientes de sus derechos y responsabilidades. En especial implementar a nivel escolar y colegial la materia de protección del consumidor, datos personales y seguridad en el comercio electrónico.

5) Derecho a la asociación y la representación (derecho a ser escuchados). Los consumidores tienen derecho a asociarse libremente con el fin de proteger sus derechos. El Estado tiene la obligación de consultar a las asociaciones de consumidores cuando se preparen decisiones que les conciernen.

6) Derecho a la no discriminación en el acceso a productos y servicios, con atención a las necesidades de los consumidores vulnerables.

Capítulo IV. De la Responsabilidad por Producto Defectuoso

Artículo 6.- Todo productor será responsable de los daños causados por los defectos de sus productos. Si el productor del producto defectuoso no pudiera ser identificado, cada proveedor del producto será considerado como su productor.

Artículo 7.- El perjudicado por un producto defectuoso deberá probar el daño, el defecto y la relación causal entre el defecto y el daño.

Artículo 8.- Si en la aplicación de la presente Ley, dos o más personas fueran responsables por el mismo daño, su responsabilidad será solidaria.

Artículo 9.- Un producto es defectuoso cuando no ofrece la seguridad a que una persona tiene legítimamente derecho, teniendo en cuenta su uso razonable. Un producto no se considerará defectuoso por la única razón de que posteriormente se haya puesto en circulación un producto más perfeccionado.

Artículo 10.- El productor no será responsable, si prueba una o varias de las siguientes circunstancias:

a) Que no puso el producto en circulación.

b) Que el defecto se debe a que el producto se ajusta a normas imperativas dictadas por los poderes públicos.

c) Que, en el momento en que el producto fue puesto en circulación, el estado de los conocimientos científicos y técnicos no permitía descubrir la existencia del defecto.

Sin embargo, el productor no se exonerará de responsabilidad si en el momento en que se causó el daño ya se tenía conocimiento del riesgo y no se tomaron las medidas adecuadas para evitarlo.

Artículo 11.- A los efectos del artículo 6, se entiende por daños:

a) Los daños físicos a las personas, como la muerte o lesiones corporales.

b) Los daños materiales por deterioro o destrucción de cosas que no sean el mismo producto.

El presente artículo no impide la posibilidad de reclamar otros tipos de indemnizaciones, según las disposiciones nacionales.

Artículo 12.- La acción de resarcimiento prevista en la presente Ley para reparar los daños, prescribirá en un plazo de 3 años a partir de la fecha en que el demandante tuvo, o debería haber tenido, conocimiento del daño, del defecto y de la identidad del producto.

Artículo 13.- El derecho que se le confiere al perjudicado para reclamar perjuicios causados por un producto defectuoso se extinguirá transcurridos veinte (20) años a partir de la fecha en que el productor hubiera puesto en circulación el producto mismo que causó el daño, a no ser que el perjudicado hubiera ejercitado una acción judicial contra el productor.

Capitulo V. De las Garantías

Artículo 14.- Los proveedores están en la obligación de dar garantía, cuando:

a) Se incumpla con la entrega material y jurídica del bien en el momento acordado.
b) Se hubiese ofrecido garantía sobre el producto y éste presenta alguna falla dentro de su término de vigencia.
c) El bien no sea apto para el uso al cual está destinado.
d) El contenido neto del producto resulte inferior al que debiera ser o menor al indicado en el envase o empaque.
e) El producto esté sometido a normas obligatorias de calidad, y no cumpla con éstas.
f) Un país haya determinado la obligación de brindar garantía sobre ciertos productos.
g) No se cumpla con lo informado, publicitado o acordado.

Artículo 15.- Los productos duraderos, que por su naturaleza están destinados para ser usados repetidamente por un período prolongado de tiempo, se presumirán con garantía. En caso de controversia, es deber del proveedor demostrar que le informó adecuadamente al consumidor que el bien no contaba con garantía.

Artículo 16.- El proveedor que deba cumplir con la garantía del bien, deberá:
a) Reparar y dejar en perfectas condiciones de uso el producto.
b) Cambiar el producto por uno nuevo.
c) Devolver el dinero.

En caso de reparación parcial del producto, correrá un nuevo término de garantía igual al inicial, desde el momento de su nueva entrega, para las partes que han sido reparadas o cambiadas. El resto del producto conservará su garantía inicial y sus términos.

En el caso de cambio total del bien, correrá un nuevo término de garantía igual al inicial, desde el momento de su entrega.

En caso de devolución del dinero, se deberá devolver en su integridad las sumas pagadas, y se cancelará cualquier obligación adicional que haya contraído el consumidor con el proveedor o con quien haya obtenido un crédito para la compra del producto.

Artículo 17.- La garantía deberá constar por escrito, y deberá informar adecuadamente el tiempo de duración, las condiciones especiales de ésta si las hubiere, y la forma de hacerla efectiva.

En caso de que no se diese la garantía por escrito, se presumirá que ésta es por el tiempo y condiciones normales y habituales para el tipo de producto y su relación con el precio pagado. La autoridad competente determinará las condiciones particulares de la garantía al momento de resolver cada caso individual. Igualmente establecerá la forma en que se deberá cumplir con ella, según el artículo anterior.

Capítulo VI. De la Información

Artículo 18.- Los proveedores deberán suministrar a los consumidores y usuarios información clara, veraz, suficiente y comprobable, en idioma del país al que se dirige la información, sobre los productos que ofrezcan y, sin perjuicio de lo señalado para productos defectuosos, serán responsables de todo daño que sea consecuencia de la inadecuada o insuficiente información. Además debe informar sobre las garantías de protección a los datos personales que solicite al consumidor.

Artículo 19.- Sin perjuicio de las reglamentaciones especiales, la información mínima comprenderá:
a) Las condiciones objetivas del producto, entre las cuales se encuentra las siguientes:
i. La relativa a las garantías que asisten al consumidor o usuario.
ii. Las instrucciones para el correcto uso o consumo, conservación e instalación del producto o utilización del servicio.
iii. Cantidad, peso o volumen, en el evento de ser aplicable.
iv. El precio. Todo proveedor que venda directamente o a través de Internet al consumidor está obligado a indicar el precio al público de los bienes o servicios que ofrezca según la reglamentación de la autoridad competente, o, a falta de ésta, podrá elegir según sus posibilidades o conveniencia el sistema de fijación en listas, distintivo específico en góndola o anaquel, página Web, o el sistema de fijación en los bienes mismos.
v. En los casos en que sea aplicable, se deberá indicar el precio por unidad de medida.
vi. En cualquier información sobre precios dirigida a los potenciales consumidores y usuarios se deberá indicar el precio total del producto, el cual incluirá cualquier cargo adicional a que hubiere lugar, como gastos de transporte o de entrega, indicación del pago de tributos, etc.
vii. La vida útil, cuando ello sea pertinente.
viii. Las especificaciones del bien o servicio. Cuando la autoridad competente exija especificaciones técnicas particulares, éstas deberán contenerse en la información mínima.

b) Relativas a la identificación del proveedor, procedimientos y otros:
i. Identidad del proveedor, su referencia en el registro mercantil,
ii. domicilio geográfico del proveedor de bienes o servicios,
iii. medios de contacto,
iv. la forma de pago, modalidad de entrega,
v. el plazo de la validez de la oferta,
vi. países a los que se dirige la publicidad,
vii indicación de la posible recopilación de datos del consumidor, su justificación y los derechos que posee el consumidor sobre ellos.
viii. advertencias sobre contenidos no aptos y a qué tipo de población se refiere.
ix. Mecanismos de comunicación rápida, fácil y efectiva con la empresa,
x. servicios de atención a procedimientos legales,
xi. dirección del domicilio legal de la empresa y sus directivos,
xii. los diferentes pasos técnicos que deben darse para celebrar el contrato,
xiii. si el prestador de servicios va a registrar o no el contrato celebrado, y si éste va a ser accesible,
xiv. los medios técnicos para identificar y corregir los errores de introducción de datos antes de efectuar el pedido.
xv. Procedimientos en caso de reclamo, legislación y jurisdicción aplicable.
xvi. Su código de ética en las relaciones comerciales electrónicas.

Artículo 20.- Cuando se expende al público productos con alguna deficiencia, usados o reconstruidos, deberá informarse claramente esta circunstancia al

consumidor y hacerlo constar en los propios artículos, página Web, etiquetas, envolturas o empaques, y en las facturas correspondientes.

Capítulo VII. De la Publicidad

Artículo 21.- La publicidad deberá ser clara, veraz, suficiente y comprobable. Está prohibida la publicidad engañosa. El anunciante será responsable de los perjuicios que cause la publicidad engañosa.

Artículo 22.- Las condiciones específicas anunciadas en la publicidad obligan al anunciante, en los términos de dicha publicidad.

El anunciante deberá tener a disposición de la autoridad competente toda la sustentación de las afirmaciones objetivas que haga en su publicidad, por un periodo no inferior a un (1) año después de retirada la publicidad del mercado.

Artículo 23.- Publicidad de promociones y ofertas. La publicidad de las promociones y ofertas, debe contener información clara y suficiente sobre todas las condiciones de tiempo, modo y lugar de las mismas.

Para poder utilizar publicidad anunciando una promoción o una oferta, deberá existir comparativamente una ventaja para el consumidor que si hubiese adquirido el producto sin que existiera la promoción u oferta.

Los términos de las promociones y ofertas obligan a quien las realice y debe indicar la fecha de vigencia de la misma. De no indicarse su fecha de iniciación, se entenderá que rige a partir del momento en que fue puesta en conocimiento del potencial consumidor o usuario. La omisión de la fecha hasta la cual está vigente, hará que la promoción se entienda válida por tiempo indefinido hasta que se dé a conocer la revocatoria de la misma, por los mismos medios e intensidad con que se haya dado a conocer originalmente.

La expresión “hasta agotar inventarios” podrá ser utilizada para indicar la vigencia de la promoción u oferta, siempre y cuando se señale el número de artículos disponibles para la promoción.

La publicidad debe indicar a qué tipo de población se dirige y en cuáles países es válida.

Artículo 24.- Respeto a la privacidad. No enviar publicidad, a través de medios electrónicos, a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla. Se incluye la publicidad enviada por correo electrónico. No utilizar información sobre consumidores con fines mercadotécnicos o publicitarios. No distribuir las direcciones electrónicas ni ninguna información personal del consumidor sin consentimiento del titular. Respetar la privacidad del consumidor en relación con el uso de cookies. Tener una política de privacidad y divulgarla en la página principal del sitio del proveedor o productor

Capítulo VIII. De los Contratos de Adhesión

Artículo 25.- Queda prohibido establecer o renovar relaciones de consumo a partir del ofrecimiento de productos no solicitados por el consumidor cuya declinación o rechazo deba ser expresamente comunicado. Si con el ofrecimiento se incluye el envío del producto, el consumidor no estará obligado ni a la conservación, ni a gestionar, ni a pagar la devolución de lo recibido.

Artículo 26.- Para la validez de los contratos de adhesión deberán cumplirse las siguientes condiciones:

Sin perjuicio de lo dispuesto para las cláusulas prohibidas, el proveedor debe haber informado suficiente, anticipada y expresamente al adherente sobre la

existencia, efectos y alcance de las condiciones generales. En los contratos escritos se utilizará el idioma del país al que se dirige. No se podrán hacer remisiones a textos o documentos que no sean de conocimiento público.
Las condiciones generales del contrato deben ser concretas, claras y completas. En el escrito del contrato, los caracteres deberán ser legibles a simple vista. Las cláusulas ambiguas o confusas se entenderán a favor del consumidor.
No incluir espacios en blanco.
No debe remitir a otros textos que no se faciliten al consumidor.
En los contratos electrónicos deben tener la firma digital de ambas partes. Y en los casos de compra y venta que exija capacidad contractual, deben ambas partes consignar su firma digital certificada.
Establecer cláusulas de protección al consumidor en los contratos de adhesión realizados por medios electrónicos, que garanticen que el proveedor se hará responsable de las pérdidas que sufra el consumidor por violación de la seguridad de los datos durante la transmisión en la Red.
Una copia fiel del contrato debe ser entregada al consumidor.
En compra y venta por Internet, el consumidor tiene un plazo de 10 días para devolver un bien o servicio adquirido a través de Internet o de rescindir el contrato, contados a partir de la recepción del bien o servicio, y sin responsabilidad para él.

Artículo 27.- Están prohibidas las cláusulas que producen un desequilibrio injustificado y significativo en perjuicio del consumidor y las que, en las mismas condiciones, afecten el tiempo, modo o lugar en que el consumidor puede ejercer sus derechos. Para establecer la naturaleza y magnitud del desequilibrio, serán relevantes todas las circunstancias relacionadas con la transacción particular que se analice. A manera indicativa y no taxativa, son cláusulas prohibidas:
- Las que permitan al proveedor modificar unilateralmente el contrato o sustraerse de sus obligaciones.
- Las que prevean la prórroga de un contrato de duración determinada si el consumidor no se manifiesta en contra.
- Las que desconozcan normas generales para servicios con menoscabo de los intereses del consumidor y que se encuentren reguladas legalmente.
- Las que limiten la responsabilidad del productor o prestador del servicio por productos o servicios defectuosos.
- Las que impliquen renuncia de los derechos del consumidor o usuario.
- Las que inviertan la carga de la prueba en perjuicio del consumidor o usuario.
- Las que trasladen al consumidor o un tercero que no sea parte del contrato, la responsabilidad del productor, proveedor o prestador de servicio.
- Las que establezcan que el proveedor no reintegre lo pagado si se resuelve el contrato cuyo objeto no se ha realizado.
- Las que prevean la posibilidad de cesión del contrato por parte del prestador de servicio o proveedor sin el consentimiento del consumidor o usuario.
- Las que vinculen al consumidor al contrato, aun cuando el proveedor no cumpla sus obligaciones.
- Las que concedan al proveedor la facultad de terminar unilateralmente si el objeto del contrato se ajusta a lo estipulado en el mismo.

- Las que, presentes los supuestos de ley, impida al consumidor resolver el contrato o excepcionar el incumplimiento del proveedor.
- Las condiciones generales de los contratos de adhesión que no reúnan los requisitos señalados en esta Ley.
- Las que incluyan pago de intereses o tasas no autorizadas legalmente.
- En los contratos de promesa de compraventa, las cláusulas que autoricen modificación unilateral del contrato de compraventa respectivo o modifiquen la oferta.
- Las que presumen cualquier manifestación de voluntad del consumidor, cuando de ésta se deriven erogaciones a su cargo.
-Las que indique que la legislación aplicable y la jurisdicción competente sea la de otro país distinto de donde el consumidor resida, para los casos de compra y venta por Internet.

Artículo 28.- El hecho de que una o varias cláusulas de un contrato hayan sido negociadas, no obsta para la aplicación de lo previsto en este capítulo.
Artículo 29.- La nulidad o ineficacia de una cláusula no afectará la totalidad del contrato, en la medida en que éste pueda subsistir sin las cláusulas nulas o ineficaces.

Capítulo IX. Ventas A Distancia o por Medios Electrónicos
Artículo 30.- El proveedor que realice operaciones a distancia, empleando medios en los cuales se concreten operaciones no presenciales, como los realizados por medios electrónicos, o en otras condiciones en que sea imposible documentar concomitantemente la transacción, deberá:
a) Informar al consumidor sobre: su identificación, domicilio geográfico, medios de contacto, y su referencia en el registro mercantil.
b) En casos de compra y venta por Página Web, solicitar la firma digital certificada para que un consumidor pueda acceder a páginas Web de contenidos no aptos para cierta población.
c) Cerciorarse de que la entrega del bien o servicio se realice efectivamente en la dirección indicada por el consumidor o usuario y que éste ha sido plena e inequívocamente identificado.
d) Permitir que el consumidor o usuario haga reclamos y devoluciones en los mismos términos y por los mismos medios de la transacción original.
e) Cubrir los costos de empaque, seguros ordinarios, manejo y transporte, los cuales deberán estar incluidos en el precio de venta.
f) Mantener los registros necesarios y poner en conocimiento del consumidor o usuario, el asiento de su transacción y la identidad del distribuidor final y del productor del bien.
g) Firmar digitalmente los contratos de adhesión realizados por medios electrónicos y entregar una copia fiel de este al consumidor, para las compras y ventas realizadas por Internet.

Artículo 31.- En todas las operaciones que se realicen usando medios en los cuales se concreten operaciones no presenciales o en condiciones en que sea imposible documentar la transacción, el consumidor podrá revocar su aceptación dentro de los 10 días hábiles siguientes a la entrega del bien o el cierre de la transacción, lo último que ocurra. Las restituciones

correspondientes deberán hacerse dentro de los 5 días siguientes a la devolución del producto.

Artículo 32.- En los contratos celebrados a distancia, telefónicamente, por medios electrónicos o similares, el productor o prestador de servicio deberá dejar constancia de la aceptación del adherente a las condiciones generales a través de medios inequívocos y observando las normas que los regulan.

Artículo 33.- En una compra y venta por Internet, se considerará el perfeccionamiento del contrato en el momento en que el contrato electrónico haya sido aceptado por el consumidor y esta aceptación haya sido recibido por el proveedor, el cual debe enviar el acuse de recibo al consumidor.

Artículo 34.- En una compra y venta por Internet, se considerará el lugar de perfeccionamiento del contrato donde resida el consumidor.

Artículo 35.- En el caso de compra y venta por Internet, el proveedor debe utilizar servidores y mecanismos seguros para realizar las transacciones de comercio electrónicas, y confirmar las órdenes de compra por e-mail o por teléfono cuando son por grandes cantidades de dinero. El proveedor es responsable de las pérdidas que sufra el consumidor por violación de la seguridad de los datos durante la transmisión en la Red.

Capítulo X. Normas Procedimentales

Artículo 36.- Los países deberán promover porque sus Autoridades Administrativas encargadas de vigilar el cumplimiento de la presente Ley, cuenten con facultades para:

a) Solicitar a las personas naturales y jurídicas el suministro de datos, informes, libros, documentos electrónicos y papeles de comercio que se requieran para el correcto ejercicio de sus funciones;

b) Practicar visitas de inspección con el fin de verificar el cumplimiento de las disposiciones legales cuyo control le compete y adoptar las medidas que correspondan, conforme a la ley

c) Interrogar bajo juramento y con observancia de las formalidades previstas para esta clase de pruebas en el Código de Procedimiento Civil, a cualquier persona cuyo testimonio pueda resultar útil para el esclarecimiento de los hechos durante el desarrollo de sus funciones.

d) Suspender temporalmente la producción y/o comercialización de un bien o servicio por peligro inminente a la salud y seguridad de los consumidores, mientras se adelanta la investigación administrativa correspondiente.

e) Ordenar el decomiso y destrucción de productos que no cumplan con las Normas Técnicas Obligatorias, Reglamentos Técnicos o que representen un riesgo para la salud, seguridad y privacidad de los consumidores.

f) Sancionar con multa, orden de retiro de un producto o cierre temporal o definitivo de un establecimiento de comercio, cuando se demuestre la infracción a cualquiera de las obligaciones establecidas en la presente Ley. Las sanciones se graduarán según la infracción cometida.

g) Ordenar la publicación de avisos de rectificación o informativos, en la forma que determine la entidad administrativa competente.

h) Tomar las medidas pertinentes para prevenir daños mayores a los consumidores.

i) Exigir al proveedor el cumplimiento de la garantía.

j) Realizar procedimientos de conciliación o arbitraje de forma rápida y eficaz.

Artículo 37.- Las Autoridades competentes establecerán y fomentarán los mecanismos alternativos de solución de conflictos para los casos de protección del consumidor, procurando una atención profesional, ágil y económica.
Artículo 38.- Las Autoridades competentes velarán porque los procedimientos establecidos para ordenar el cumplimiento de la garantía sean los más expeditos, simples y económicos posibles, sin perjuicio de las normas procesales en materia de indemnización de perjuicios.
Artículo 39.- Los países deben tener como principios rectores en la implementación de políticas de protección del consumidor, la descentralización territorial de las facultades de ordenar el cumplimiento de las garantías, y la concentración en las investigaciones por producto defectuoso en la autoridad especializada.

Capítulo XI. De la Jurisdicción
Artículo 40.- La jurisdicción internacional derivada de los conflictos que surjan en los temas de que trata la presente Ley en que las dos partes tengan domicilio en diferentes países, se aplicarán las siguientes reglas:
1. En cuanto el domicilio.
a) El lugar de domicilio en las personas físicas será la residencia habitual o el centro principal de sus negocios, en ese orden.
b) El lugar de domicilio de las personas jurídicas será la sede principal de la administración o el lugar donde funcionen sus filiales, sucursales, establecimientos, agencias o cualquier otra especie de representación, en ese orden.
2. Tendrán jurisdicción internacional las demandas entabladas por el consumidor, y lo podrá hacer en su lugar de domicilio.
3. De acuerdo con las normas civiles sobre pruebas aportadas en el exterior, el proveedor que no tenga ningún tipo de representación en el país donde fue demandado, podrá contestar la demanda, presentar pruebas, interponer recursos, así como realizar actos procesales en los que se requiera la participación del Juez en los de su propio domicilio, los cuales deberán remitir lo actuado a los Jueces competentes en el país donde se sigue la causa.
4. La ley procesal aplicable será la del país donde se presente la demanda.
5. La solicitud de reconocimiento de una sentencia se hará, por intermedio de las Autoridades competentes de cada uno de los países.

Capítulo XII. De los Mecanismos Alternativos de Solución de Conflictos
Artículo 41.- La Comisión Nacional del Consumidor es competente para adelantar audiencias de conciliación en las controversias que le sometan los particulares respecto de la aplicación de la presente Ley. Las Actas de Conciliación serán obligatorias para las partes, y constituirán un título legal y suficiente para solicitar su ejecución, conforme a las disposiciones internas de cada país.
Artículo 42.- Se crea la Comisión Internacional de Controversias conformada a nivel internacional encargado de dirimir los conflictos entre proveedor y consumidor cuando las partes son de países distintos. Las autoridades competentes del grupo de países reglamentarán su funcionamiento y procedimientos mediante Resolución.
Artículo 43.- Los particulares podrán acordar someter a arbitraje, por el Tribunal o por la Comisión Internacional de Controversias, los conflictos que se

susciten por la aplicación o interpretación de aspectos contenidos en contratos de carácter privado y regidos por la presente Ley.
Artículo 44.- Cuando las partes pacten someter las controversias a un procedimiento arbitral en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje

Capítulo XIII. Del Sistema de Intercambio Rápido de Información
Artículo 45.- Se crea el Sistema de Intercambio Rápido de Información, encargado de centralizar y difundir la información que se tenga en cualquier país de la producción, importación o comercialización de productos defectuosos, así como divulgar en sitios oficiales de los Estados, la lista de proveedores reales que venden bienes y servicios a distancia o por medios electrónicos, como Internet. La Comisión Internacional de Controversias reglamentará su funcionamiento mediante Resolución.

Capítulo XIV. Disposiciones Finales
Artículo 46.- La Comisión Internacional de Controversias promoverá la creación de una Asociación de Consumidores a nivel Internacional que vigile desde el sector privado el libre comercio y el respeto a los derechos de los consumidores de todo el mundo (o grupo de países al que pertenecen)
Artículo 47.- En lo no dispuesto por esta Ley se aplicará las normas de protección que mejor convenga a los intereses del consumidor.

Anexo 10. Disposiciones de Organismos Internacionales en los aspectos de seguridad.

Ley Modelo CNUDMI	Unión Europea	OCDE	Estados Unidos
a- Definiciones técnicas: se establece definiciones de lo que se entiende por firma electrónica, certificado, mensaje de datos, firmante, prestador de servicios de certificación y parte que confía, en el artículo 2 de la Ley Modelo sobre Firmas Electrónicas. b- Neutralidad Tecnológica: se refiere a que las legislaciones no estén atadas a una tecnología específica, establecida en el artículo 3 de la Ley Modelo sobre Firma Electrónica del 2001. c- Equivalencia Funcional: se refiere a que se les asigne el mismo valor a los documentos y firmas electrónicas que a los equivalentes en papel, indicado en los artículos 6, 7 y 8 de la ley modelo de Comercio Electrónico de las Naciones Unidas, CNUDMI de 1996. d- Autonomía de la Voluntad: que las partes son soberanas para determinar las formas de actuar y de contratar electrónicamente, establecido en el artículo 4 de la Ley Modelo de Comercio Electrónico de 1996. e- Condiciones de fiabilidad: La Ley Modelo sobre Firmas Electrónicas establece en el artículo 6 que la firma electrónica se considerará fiable si cumple las siguiente condiciones: 1) Datos de creación de la firma correspondientes al firmante en forma exclusiva, 2) Datos de creación de la firma estaba bajo control exclusivo del firmante en el momento de la firma, 3) Posibilidad de detectar cualquier alteración a la firma posterior al momento de la firma, 4) Posibilidad cierta de detectar cualquier alteración a la información posterior al momento de la firma. Se deja a salvo, tanto la posibilidad de demostrar, por otros medios, dicha fiabilidad, como la prueba en contrario de ella, e incluso la inaplicabilidad de todo el artículo a hipótesis a determinar	Directiva 1999/93/CE, del 13 de diciembre de 1999, sobre un Sistema Común para las Firmas Electrónicas. a- Constituye un marco jurídico homogéneo y adecuado para el uso de las firmas dentro de la comunidad. b- La libertad contractual regula toda aplicación en entornos cerrados o redes locales. c- Los prestatarios de servicios de certificación podrán ofrecer sus servicios sin la obligación de autorización previa. d- Consagra un marco jurídico para todos los certificados y servicios que preste la entidad certificadora. e- Validez e igualdad de la firma electrónica a la firma tradicional. f- Permite a los prestatarios de servicios de certificación avalar los certificados de terceros países de la misma forma que garantizan a sus propios certificados. g- Prohíbe limitar el número de entidades certificadoras. h- Limita la utilización de los datos obtenidos. La difusión de datos personales debe ser autorizada por el titular de los mismos. Queda prohibido que los datos puedan obtenerse o tratarse con fines distintos sin el consentimiento de su titular. i- Establece los requisitos de los certificados reconocidos y los requisitos de los proveedores de los servicios de certificación. j- Consagra el principio de la buena fe: Los estados miembros deben velar por que el proveedor de los servicios de certificación, que emita un certificado reconocido, sea responsable ante cualquier persona que de buena fe confíe en el certificado, en relación a: 1) La exactitud de toda la información contenida en el certificado. 2) La conformidad de todos los requisitos que exige la ley. 3) La garantía de que, en el momento de la emisión del certificado reconocido, obra en	Marzo de 1997 publicó su recomendación para el establecimiento de políticas sobre Criptografía con el fin de promover el uso de la criptografía para favorecer la confianza en las redes y sistemas de información y garantizar la seguridad de los datos y la protección a la vida privada. En el 2002 la OCDE adoptó directrices para la seguridad de los sistemas y redes de información. Estas Directrices constituyen una base de trabajo fundamental hacia una cultura de seguridad para toda la sociedad. - Concienciación: Las partes involucradas deben ser concientes de la necesidad de garantizar la seguridad de los sistemas y redes de información y de las acciones que pueden emprenderse para reforzar la seguridad. - Responsabilidad: Las partes son responsables de la seguridad de los sistemas y redes de información. - Reacción: Las partes involucradas deben actuar rápidamente y con espíritu de colaboración para prevenir, detectar y dar respuesta a los incidentes de seguridad. - Ética: Cada una de las partes involucradas deben respetar los intereses legítimos de las demás partes involucradas. - Democracia: La seguridad de los sistemas y redes de información deben ser compatibles con los valores fundamentales de una sociedad democrática. - Evaluación de los riesgos: Las partes involucradas deben hacer evaluaciones de los riesgos. - Diseño e implementación de la seguridad: Las partes involucradas deben	La primera ley en materia de Firma Digital en el mundo fue la denominada “Utah Digital Signature Act”, publicada en mayo de 1995 en el Estado de UTAH, en Estados Unidos. Su objetivo es facilitar mediante mensajes electrónicos y firmas digitales las transacciones, procurar las transacciones seguras y la eliminación de fraudes y establecer normas uniformes relativas a la autenticación y confiabilidad de los mensajes de datos, en coordinación con otros Estados. Su ámbito de aplicación son las transacciones mediante mensajes electrónicos, su confiabilidad, así como las firmas digitales. Esta ley, define a la Firma Digital como la transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde

Ley Modelo CNUDMI	Unión Europea	OCDE	Estados Unidos
en cada legislación. f- Proceder del prestador de servicios de certificación: el artículo 9 de la Ley Modelo sobre Firmas Electrónicas establece una serie de cargas y obligaciones para estos sujetos que intervienen en la creación de las firmas electrónicas: actuar conforme declaraciones de normas y prácticas que haga; actuar con diligencia razonable para asegurar la veracidad y exactitud de las declaraciones que más importan al ciclo vital del certificado; dar medios razonablemente accesibles al tomador del certificado, para que determine, mediante el propio certificado, una serie de elementos esenciales (identidad del prestador del servicio, existencia de un control de datos de creación de firma por parte del firmante en el momento en que se expidiera el certificado, validez de dichos datos, etc.) g- Reconocimiento de certificados y firmas electrónicas extranjeros: El artículo 12 de la Ley Modelo sobre Firmas Electrónicas establece la previsión de que todo certificado y firma electrónica, expedidos, creados o utilizados fuera del Estado, tengan los mismos efectos que los expedidos, creados o utilizados dentro del Estado, siempre y cuando se observe un grado de fiabilidad sustancialmente equivalente de unos con otros.	poder del titular identificado en el mismo el dispositivo de creación de firma correspondiente al dispositivo de verificación dado o identificado en el certificado. La principal disposición de la Directiva establece que la firma electrónica avanzada basada en un certificado reconocido equivale a una firma manuscrita y es admisible como prueba en procedimientos judiciales. Sin embargo, se reconoce eficacia jurídica y probatoria a la firma electrónica aunque no sea avanzada, es decir, siempre que se base: en un certificado (aunque no sea reconocido), expedido por un prestador de servicios de certificación (aunque no sea acreditado), esté creada por un dispositivo de creación de firma (clave privada, aunque no sea seguro). La directiva 2000/31/CE de 8 de junio de 2000 sobre el comercio electrónico prevé que los Estados deben vigilar que su sistema jurídico pueda hacer posible la existencia de los contratos por vía electrónica.	integrar la seguridad como un elemento esencial de los sistemas y redes de información. - Gestión de la seguridad: Las partes involucradas deben adoptar un enfoque global de la gestión de la seguridad. - Reevaluación: Las partes involucradas debe examinar y reevaluar la seguridad de los sistemas y redes de información e introducir las modificaciones apropiadas en sus políticas, prácticas, medidas y procedimientos de seguridad.	que se efectuó la transformación. Se equipara el valor probatorio de un mensaje de datos con el de papel siempre y cuando contenga una firma digital confirmada mediante la clave pública contenida en un certificado que haya sido emitida por una autoridad certificadora. No se contempla el reconocimiento de certificados extranjeros, solo se menciona que la División puede reconocer la autorización emitida por Autoridades Certificadoras de otros Estados. Comité de Seguridad de la Información de la División de Comercio Electrónico de la American Bar Association (ABA) emitió en agosto de 1996 la “Guía de Firmas Digitales”. El 15 de agosto de 1997, la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme (NCCSL), elaboró la “Uniform Electronic Transactions Act” (UETA), la cual se aprobó el 30 de julio de 1999. El 4 de agosto del 2000 se aprobó la “Uniform Computer Information Transactions Act” (UCITA), la cual se encuentra en proceso de adopción por los diversos Estados de la Unión Americana. El 24 de enero de 2000 el Congreso de los Estados Unidos aprobó la “Electronic Signatures in Global and National Commerce Act” (Ley de

Ley Modelo CNUDMI	Unión Europea	OCDE	Estados Unidos
			Comercio Electrónico y Firma Electrónica para el Comercio Nacional e Internacional). El 30 de junio el 2000 la presidencia emite la "Electronic Signatures in Global and National Commerce Act" (E-Sign Act.) vigente a partir del 1 de octubre del 2000 (otorgando a la firma y documento electrónico un estatus legal equivalente a la firma autógrafa y al documento en papel).

Anexo 11. Disposiciones de Organismos Internacionales en los aspectos de protección de datos.

Principios de Protección de Datos

OCDE (2002)	Naciones Unidas (1990)	Consejo de Europa (1981)	Unión Europea (1995)
Principios	Los principios básicos reconocidos por la Recomendación 45/95 se resumen en los siguientes (Naciones Unidas, 1990):	El día 28 de enero de 1981, se adopta el Convenio 108 del Consejo de Europa. Este Convenio, de acuerdo con Puentes (2005), es el primer instrumento internacional de carácter vinculante. Sus principios:	La Directiva 95/46/CE, es el texto de mayor relevancia en el marco de la protección de datos en el ámbito Europeo, de acuerdo con Puente (2005), al regular la materia en toda su extensión e implicar su adopción la homogenización de las normas de protección de datos de todos los Estados miembros.
Principio de limitación en materia de recopilación de datos: se debe establecer límites para la recogida de datos, la obtención debe ser por medios lícitos con el consentimiento del sujeto. Principio de la calidad de los datos: datos deben ser relevantes para el propósito de su uso y en la medida de lo necesario, deben ser exactos, completos y actuales. Principio de la especificación de la finalidad de la recopilación: se debe especificar en qué se usarán los datos. Principio de limitación de uso: los datos no deben ser usados para otros propósitos, excepto cuando se tenga el consentimiento del titular o por imposición legal o de las autoridades.	Principio de legalidad y lealtad: la información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni utilizados para otros fines. Principio exactitud: obligación de los responsables de comprobar periódicamente la exactitud y pertinencia de los datos y garantizar su completitud. Además de actualizar los datos sometidos a tratamiento. Principio de especificación de la finalidad: especificar para qué se utilizarán los datos, informar a la persona interesada y mantener los datos por un período especificado de acuerdo con el fin.	Calidad de los datos: los datos debe ser obtenidos de forma leal y legítima, para los fines determinados, adecuados, pertinentes y no excesivos, exactos y actuales, mantenidos por el tiempo necesario para el cumplimiento de los fines. Y deben identificar a la persona a quien conciernen los datos.	La calidad de los datos: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados. La legitimación del tratamiento: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento.

OCDE (2002)	Naciones Unidas (1990)	Consejo de Europa (1981)	Unión Europea (1995)
Principio de la participación individual: se refiere al derecho de acceso y de rectificación.	Principio de acceso de la persona interesada: derecho a conocer, sin demoras ni gastos excesivos, los datos tratados y sus potenciales destinatarios y a que se proceda a la rectificación supresión de los datos cuyo tratamiento sea ilícito, injustificado o inexacto.	Garantías complementarias para las personas concernidas: derecho a conocer, acceder, modificar.	El derecho de acceso del interesado a los datos: para ejercer la rectificación, supresión o bloqueo de los datos cuando no correspondan.
Principio de salvaguardia de la seguridad: se debe dar protección razonable de seguridad a los datos contra pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación.	Principio de seguridad: con la finalidad de proteger los tratamientos contra riesgos naturales o su pérdida accidental, como humanos, como accesos no autorizados, el uso fraudulento de los datos o contaminación de virus informáticos.	Seguridad de los datos: Se deben tomar medidas apropiadas de seguridad.	La confidencialidad y la seguridad del tratamiento: el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizado. La información a los afectados por dicho tratamiento: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernen.
Principio de transparencia: se debe tener una política general de transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales, contar con medios ágiles para determinar la existencia y naturaleza de datos personales, el propósito de su uso e identificar y ubicar al controlador de los datos.	Principio de no discriminación: por el que se establece una regla general de prohibición del tratamiento de datos referidos al origen racial, la vida sexual, las opiniones religiosas o políticas o la participación en asociaciones o sindicatos.	Categorías particulares de datos: No pueden tratarse los datos que revelen origen racial, opiniones políticas, convicciones religiosas u otras, datos relativos a la salud, vida sexual, condenas penales.	Se prohíbe el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

OCDE (2002)	Naciones Unidas (1990)	Consejo de Europa (1981)	Unión Europea (1995)
	Facultad para hacer excepciones: Limitación de las excepciones a los principios, por razón de la protección de la seguridad nacional, el orden público, la salud o la moral pública y los derechos y libertades de terceros.	Se admiten excepciones que deben ser prevista por la ley de la Parte y que sea para proteger la seguridad del Estado.	Las excepciones y limitaciones de los derechos anteriores solo en caso de salvaguarda de la seguridad y defensa del Estado o la protección del interesado.
	Supervisión e imposición de sanciones: cada parte debería designar una autoridad imparcial e independiente de supervisión del cumplimiento de los principios y la posibilidad de imposición de sanciones penales o de otra índole por la contravención de los mismos.	Sanciones y recursos: Cada Parte se compromete a establecer sanciones y recursos contra las infracciones. El Convenio crea una estructura institucional permanente e impone a los Estados miembros la obligación de designar una autoridad que habrá de tener competencias para garantizar la aplicación de los principios del Convenio en el Derecho interno, cooperar con las restantes autoridades designadas e intercambiar información.	La notificación del tratamiento a la autoridad de control: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.
Principio de responsabilidad: el controlador de los datos es responsable del cumplimiento de las medidas que hagan efectivos los principios anteriores.			
	Transferencias internacionales: debería existir un flujo libre de datos de carácter personal entre Estados que establezcan garantías comparables de protección de la vida privada.		Establece las condiciones para la transferencia internacional de datos personales.

OCDE (2002)	Naciones Unidas (1990)	Consejo de Europa (1981)	Unión Europea (1995)
		Compromiso de las Partes: Cada Parte tomará las medidas necesarias para hacer efectivos los principios básicos para la protección de datos. Protección amplia: No se debe limitar la facultad de cada Parte de conceder una protección más amplia que la prevista en este Convenio.	
			El derecho del interesado a oponerse al tratamiento: el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. Esta Directiva establece que sus disposiciones "se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero" (Directiva 95/46/CE, 1995, p. 11
			Otras disposiciones relacionadas con la materia de protección de datos: Directiva 1999/93/CE: Establece el marco común de firma electrónica. Su artículo 8 indica que se debe cumplir con la directiva 95/46/CE. Directiva 97/66/CE relativa al tratamiento de datos personales y a la protección a la intimidad en el sector de telecomunicaciones.

OCDE (2002)	Naciones Unidas (1990)	Consejo de Europa (1981)	Unión Europea (1995)
			Directiva 2002/58/CE sobre privacidad y las comunicaciones electrónicas, ésta deroga la directiva 97/66/CE adicionando otros temas. Carta de Derechos Fundamentales de la Unión Europea: establece el derecho a la protección de los datos personales en su artículo 8. Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000 sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos de la Comunidad y sobre la libre circulación de estos datos. Decisión 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999: Plan Plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Decisión 854/2005/CE de 11 de mayo de 2005, el Consejo creó el Programa Saber Internet Plus, con el objetivo de favorecer una utilización más segura de Internet y las nuevas tecnologías en línea.

Transferencia Internacional de Datos

Organismo	Disposiciones
OCDE	Directrices sobre protección de la privacidad y flujo transfronterizos de datos personales de 1980: Capítulo de Principios básicos de aplicación internacional: restricciones en el flujo y la legitimidad.
Consejo de Europa	Convenio 108 del Consejo de Europa: artículo 12 establece sobre el flujo transfronterizos de datos de carácter personal. 8 de noviembre de 2001 se emitió un Protocolo adicional del Convenio 108.
Unión Europea	Directiva 95/46/CE: Capítulo IV regula la transferencia de datos personales a terceros países.

Anexo 12. Jurisprudencia de la Sala sobre protección de datos personales.

Voto	Asunto
2609-91, 2680-94	En contra de los archivos criminales administrados por el Organismo de Investigación Judicial. Se considera el suministro de informaciones conservados en esos archivos a terceras personas (desviación del fin original del tratamiento de datos) como lesivo al principio de legalidad y a la dignidad de la persona.
1261-90	Reconoce el derecho a la intimidad y el derecho a acceder al amparo para protegerlo. En esta sentencia, la Sala anuló por inconstitucional la posibilidad de intervenir, inclusive con fines de investigación policial, las líneas telefónicas.
9080-94	La Sala Constitucional avaló la negativa de la institución aseguradora de vehículos de mostrar los datos declarados por quien sufrió una colisión, inclusive a la parte contraria en el mismo accidente automovilístico. La sentencia declaró el carácter confidencial de esos datos resguardados por el asegurador.
4147-97	La Sala acogió el recurso de amparo planteado por quien exigió del patrono que le mostrara el expediente personal abierto durante el proceso de reclutamiento de personal. En esta sentencia el tribunal afirma un principio esencial en el derecho de la autodeterminación informativa: el derecho al acceso a los datos personales acopiados en una investigación.
4154-97	Habla expresamente del hábeas data y su regulación, planteando que el objeto de este recurso es la protección de la persona para conocer o rectificar la información pública o privada que exista sobre ella.
1345-98	La Sala Constitucional reconoce los peligros de la sociedad informatizada. Una empresa suministró a un banco información sobre una persona, contra la cual existía, según la empresa, una deuda incobrable. En realidad, la deuda estaba prescrita y el recurrente así exigía que se aclarara en la base de datos.
8996-2002	Mismo sentido que 1345-98.
1345-99	Abre la posibilidad de una tutela de acceso, con base en el derecho a la autodeterminación informativa, para que la gente pueda conocer las informaciones que sobre ellas se encuentren registradas, e incluye una descripción de los derechos que lo asisten.

Voto	Asunto
5802-99	La Sala se pronuncia en cuanto al deber de excluir del archivo policial las reseñas de personas absueltas o sobreseídas definitivamente en un proceso penal. Indica la Sala que “Mantener su ficha en el archivo no solo roza con el derecho a la autodeterminación informativa, sino también con el principio de inocencia. Primer fallo donde la Sala abordó los principios que regulan el tratamiento de datos personales, y dio cabida a que el ciudadano pueda controlar la forma en que se realiza el tratamiento de datos personales, dentro de la tutela procesal del hábeas data
6481-99	La Sala considera también confidenciales los datos presentados por un tercero en la oferta dentro de una licitación pública, y rechaza la petición de tener acceso a ellos.
2885-2002	La Sala obligó a la empresa excluir de sus archivos datos sobre los parientes de quien solicita el crédito, pues esto se desvía de la finalidad del archivo.
6783-2002	La Sala obligó a una empresa que aclarara la identidad de una persona cuyos datos constaban en el archivo. El problema surgió porque la empresa de datos suministra a un banco el historial crediticio de una persona, pero al no constar ningún número de identificación, y por existir la posibilidad de personas con igual nombre, no es posible determinar exactamente si se trata de quien gestiona el crédito.
10438-2002	Mismo sentido que 6783-2002.
3820-2000	La Sala declaró con lugar un recurso de amparo a favor de un periodista que reclamaba tener acceso a los pasaportes diplomáticos de varios funcionarios del servicio exterior. El acceso debe darse no solo a los periodistas, sino a toda persona que lo solicitara.
4802-2002	Con lugar el tener acceso a la lista de personas autorizadas por el Ministerio de Obras Públicas y Transportes para brindar el servicio de transporte público.
3489-2003	La Sala obliga a un banco estatal, en aras de la transparencia, a revelar la información de las cuentas corrientes que tienen a su nombre los distintos partidos políticos y las sociedades anónimas que utilizaron para canalizar los fondos de la campaña electoral.