# Indice

**Resumen**

Es conocido que el comercio electrónico ha venido a revolucionar y a dinamizar el escenario de las relaciones comerciales, cuyos aportes principales giran en torno a la rapidez y flexibilidad de los convenios entre las partes contratantes, que dejan los tradicionales esquemas del acuerdo presencial o documental, para dar paso los mecanismos de contrato electrónico.

Junto con esta dinámica, aparecen los temas del riesgo del negocio y de la responsabilidad de las partes contratantes, ya de la misma manera que evoluciona el comercio, se presentan formas más sofisticadas de cometer actos ilícitos, generando inseguridad tanto para quienes proveen productos electrónicos así como para los usuarios. En este sentido, son los oferentes de los servicios electrónicos, los que han soportado las consecuencias ante fraudes electrónicos, por ser, según la doctrina de la responsabilidad objetiva, los generadores del riesgo.

La firma digital aparece como un mecanismo que busca brindar seguridad tecnológica sobre la información que transita en las transacciones, minimizando la posibilidad de su sustracción. Aparejado a este desarrollo, se requiere de certeza jurídica, a fin de legitimar la operativa relacionada con la firma digital.

Se procurará determinar si tales elementos se cumplen y cuál sería el impacto sobre la percepción de la responsabilidad de las partes bajo un nuevo esquema.

**Palabras clave:**

Firma digital, autoridad de certificación, autoridad de registro, responsabilidad objetiva, responsabilidad subjetiva.

**Abstract**

It is known that electronic commerce has come to revolutionize and revitalize the scene of trade relations, whose main contributions revolve around the speed and flexibility of agreements between the contracting parties, leaving the traditional patterns of attendance or documentary agreement to allow the mechanisms of electronic contract.

Along with this dynamic, appears the subjects of business risk and responsibility of the contracting parties, and in the same way as trade evolves, there are more sophisticated ways to commit illegal acts, creating uncertainty for both suppliers and electronic products and for users. In this sense, are the providers of electronic services, which have borne the consequences of electronic fraud, because, they are, according to the doctrine of objective liability, the risk generators.

The digital signature appears as a mechanism that seeks to provide technological safety, on information that transit in electronic transactions, minimizing the possibility of theft. Accompanied by this development, legal certainty is required in order to legitimize the operations associated with digital signatures.

Will seek to determine if these elements are met, and what would be the impact on the perceived responsibility of the parties under a new scheme.

Key words:

Digital signature, certification authority, registration authority, objective liability, subjective liability

**"Análisis de la presunción de autoría en la Ley de Certificados, Firmas Digitales y Documentos Electrónicos de Costa Rica, como elemento limitador de la responsabilidad objetiva bancaria."**

Deivis Granados Oviedo[1]

## Introducción.

La dinámica que se ha venido presentando en los avances tecnológicos y particularmente, el impacto en el desarrollo de productos electrónicos sofisticados, ha permitido ofrecer al mercado, una gama de servicios que pretenden ajustarse prácticamente a las necesidades de usuarios cuyos gustos y preferencias, son cada vez más difíciles de satisfacer, precisamente por influencia de la competencia del medio comercial electrónico.

Una de las consecuencias, que puede enfocarse como virtud de la evolución tecnológica, es la posibilidad de realizar distintas transacciones en donde las partes de la relación, pueden encontrarse en distintos puntos del orbe y aún más, -el objeto del negocio,- encontrarse en un tercer punto. Consecuentemente, se prescinde cada vez más, de la posición clásica contractual de la comparecencia "cara a cara" de los contratantes, como una forma de constatación o identificación de los obligados en un negocio, rigiéndose ahora por una serie de validaciones electrónicas en tiempo real; siendo ésta una de las facilidades del comercio electrónico.

Paralelo a este desarrollo, ha sido necesaria la implementación de mecanismos que provean de seguridad, tanto electrónica como jurídica, a las partes involucradas en una relación de negocios electrónicos.

La aparición de la firma digital viene a constituirse en un medio que procura dar respuesta a dichas necesidades, sin que ello constituya por sí misma, una garantía absoluta de infalibilidad. Es por ello que interesa analizar la figura de la firma digital asociada a un medio físico, cuya ejecución está fijada en el corto plazo en nuestro país,

[1] Licenciado en Derecho. Candidato a Maestría en Derecho Empresarial, ULACIT. Correo electrónico: granadosod@bccr.fi.cr

contando ya con el marco regulatorio correspondiente y con la infraestructura y logística para su distribución a los interesados.

Por tanto, en razón de las posibles consecuencias jurídicas y patrimoniales, es importante la investigación de las responsabilidades aludidas en la ley, a fin de determinar si la figura de la firma digital constituye un elemento determinante, en la percepción de la responsabilidad en la relación bancaria e igualmente, dar pie a un cambio de apoyo doctrinario y una posible variación en el fallo de nuestros tribunales.

**Conceptualización de Comercio Electrónico.**

El término *comercio electrónico*, pese a resonar con mayor fuerza a partir de la década de los noventas, suele estar asociado -según los conceptos más abiertos- a situaciones o actividades de no tan reciente data, teniendo su origen prácticamente, en la redefinición del término *mensaje;* es así como este, luego de ser inscrito en un sentido común al traslado de información legible y comprensible para la mayoría de los individuos, tiende a redefinirse a partir de la influencia de los avances tecnológicos.

Debe tenerse en claro, que no se quiere desvirtuar el mensaje escrito de forma tradicional, dado que su relevancia es actual en todos los ordenamientos, que han sentado históricamente el valor y la prueba de los actos negociales en la claridad probatoria del documento físico. En muchos casos, como el costarricense, la aparición del documento digital no excluye el documento físico al menos no en este momento, pese a las tendencias de desmaterializar los documentos.

Esto permitirá la reflexión posterior acerca del traslado de los atributos de vinculación y prueba, que le han sido reconocidos al documento físico, hacia el documento electrónico, buscando para fines prácticos, su equivalencia.

La redefinición del mensaje, entonces, estriba básicamente en una apertura de contenido, de este modo, la ley modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil (CNUDMI) conceptualiza el mensaje de datos como *la información generada, enviada, recibida o archivada o comunicada por medios electrónicos.*

Tal amplitud permite entender de una manera u otra, que una gran mayoría de individuos, en algún momento han tenido y siguen teniendo, un contacto cotidiano con

este tipo de mensajería, que prácticamente, es la base del desarrollo del comercio electrónico.

Es conveniente precisar que para efectos del presente artículo, se entenderá como comercio electrónico, cualquier transacción comercial efectuada por medios electrónicos, desarrollado a través de redes (cerradas y abiertas), mediante la relación entre oferta y demanda, para lo cual se utilizan herramientas electrónicas y telecomunicaciones, con el objeto de agilizar el proceso comercial mediante la reducción, tanto de los tiempos de contacto y ejecución, como de los costos (Prigogine, 2000), permitiendo el flujo de bienes o servicios, tangibles o intangibles.

Cabe indicar, que la conceptualización del comercio electrónico suele estar permeada de distintos matices en función de las actividades que comprende, no obstante, en su esencia, consta de los mismos elementos, tales como la referencia a *las transacciones comerciales realizadas o basadas en sistemas electrónicos de procesamiento y transmisión de información, especialmente EDI (Electronic Data Interchange) e Internet (Interconnected networks* (Remolina, 2002).

Las actividades cubiertas por el comercio electrónico (Martínez, 2001), se clasifican en dos tipos: comercio electrónico indirecto, que requiere de factores externos para el intercambio efectivo de los productos o servicios y, comercio electrónico directo, mediante el cual, tanto el pago como la entrega se realizan por medio virtual y es en este ámbito donde se *aprovecha todo el potencial de los mercados electrónicos mundiales.*

**La banca y el comercio electrónico.**

Es claro, que para la existencia de este tipo de comercio, ha sido necesaria la creación de distintas plataformas y programas informáticos de flujo de información electrónica y que las características de las mismas, está en función de factores como los servicios que se pretendan brindar y del soporte económico de quienes quieran optar por desarrollar sus negocios por la vía electrónica, es así, que pueden encontrarse desde comerciantes individuales hasta grandes corporaciones inmersas en este tipo de transacciones, que se sustentan básicamente en la entrega del producto o servicio contra el pago correspondiente.

Estas posibilidades de aprovechamiento del desarrollo en el comercio electrónico, no han pasado inadvertidas para el sector bancario, que ha visto una excelente oportunidad, tanto de modificar los servicios que por tradición brinda, como de ofrecer otros productos novedosos y más sofisticados. Al respecto Cifuentes (2002), señala que la labor fundamental de la banca contemporánea en relación con su clientela y bajo el escenario propuesto por la dinámica del comercio electrónico, es *estructurar, facilitar y operar un sistema de pagos que permita la disposición y transferencia ágil de los recursos dinerarios.*

En este mismo sentido, el autor establece que bajo el papel de facilitador del comercio electrónico, la banca se sirve de dos grandes actividades generales: por un lado, el procesamiento de información relevante para una transacción financiera y por otro, la movilización efectiva de dinero o recursos, todo esto llevado a través de un sistema de pagos debidamente organizado.

Se podrá hablar de banca electrónica entonces, cuando además de incluir una proyección externa (mercadeo) mediante la cual se ofrezcan servicios automatizados, se considere la automatización en el manejo interno del banco y en relación con otras entidades.

Cifuentes, esquematiza los servicios en los que se evidencia la operativa de banca electrónica de la siguiente manera:

- Dispensación de efectivo: ya sea en cuanto a la disposición de fondos propios o por la concesión de un crédito.
- Disposición de efectivo: mediante una orden de pago, giro o transferencia de fondos.
- Generación de un medio de pago: como el caso de alimentación de las smart cards (tarjetas inteligentes), realización de prepago de servicios, conversión de dinero físico en “cyber-moneda”.
- Obtención o generación de información: como en el caso de confirmación de fondos, obtención de saldos, etc.

La disposición de dichos servicios presupone la utilización eventual de un *soporte institucional,* llámense tarjetas de débito, tarjetas de crédito o inteligentes, digitación de claves u otro medio que implique la utilización de una computadora.

Lo anterior implica que las entidades bancarias, de forma paralela a la construcción y desarrollo de las plataformas electrónicas y el software correspondiente a los servicios ofrecidos, desarrollen todo un esquema de seguridad en procura de protegerse a sí mismos como a sus clientes, ya que como se indicara supra, dentro de las facilidades que se brindan, se encuentra el desplazamiento o transferencia de fondos en tiempo real, es decir, de forma inmediata.

Dado que la relación banco-cliente es desbalanceada, en el tanto no hay un equilibrio de fuerza entre las partes –obviamente siendo el cliente la parte débil, - el papel de la confianza y la seguridad es fundamental para ambas partes, desde el punto de vista del negocio bancario, cuanto más confianza proyecte y cuanta más seguridad ofrezca, contará con una mayor ventaja comparativa para la atracción de clientes, por otro lado, está la conveniencia de la percepción de menor riesgo para el cliente, que deposita en una entidad *segura* sus haberes patrimoniales.

Esta seguridad va más allá de que el cliente aprecie una gestión de "buen padre de familia" por parte del banco, sino que este demuestre el esfuerzo óptimo para evitar perjuicios patrimoniales causados por terceros.

**El fraude electrónico.**

El desarrollo de las nuevas estructuras informáticas que sustentan la dinámica de los negocios electrónicos, introduce el tema de la vulnerabilidad en los esquemas de seguridad desarrollados por las instituciones bancarias. Pese a que existen diversas maneras por medio de las cuales se ha buscado dicho objetivo, se mencionarán tan solo dos, que han resultado ser las más representativas, cuyo eje principal es el contacto o manipulación de información.

La experiencia ha demostrado el surgimiento paralelo de formas de intrusión (por supuesto, no autorizada) en los sistemas, con propósitos de sustracción de información sensible desde las bases o reservorios informáticos de datos o bien, se acude a la suplantación de los proveedores de servicios para inducir al suministro de

información por parte de los clientes o usuarios de los servicios. Dicho de otra manera (Sarra, 2000), *en relación con los delitos contra la propiedad, deberían considerarse incluidos dos temas cruciales: 1) los accesos indebidos a sistemas o a computadoras, y 2) la apropiación de información en ellos contenida.*

Estas conductas delictivas son llevadas acabo por medio de personas que poseen los conocimientos especializados, que eventualmente cuentan con toda una organización de apoyo, dependiendo del propósito último de sus actuaciones.

De conformidad con la intención o fin de sus actividades intrusivas, se denomina *Hacker*[2] a todo aquel que por medio de la conexión a un computador, logra la forma de conectarse o acceder a una base de datos (Guerrero, 2003). Este tipo de individuos suele conformarse con el logro de haber ingresado a sistemas catalogados como seguros, dejando eventualmente en ellos evidencia de haberlos transgredido.

Por otro lado, se encuentran los llamados *Crackers*, que a diferencia del Hacker, *se apoderan de la información contenida en los sistemas a los cuales acceden indebidamente, la que en ocasiones, suele ser de gran valor económico para el poseedor, quien queda privado de su goce* (Sarra, 2000), por lo común, la información obtenida es negociada o vendida a terceros, que la utilizarán para la defraudación.

Una táctica de los especialistas informáticos de suplantar la identidad de los proveedores de servicios, es a través de lo que se conoce como *phishing*, entendido este término como el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales.

El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar como procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada (Glosario.net, 2009), no obstante, también puede estar acompañado de la emisión de programas informáticos concebidos para la captura y posterior envío de información, llamados *malware*.

Estos ataques masivos tienen el inconveniente del encubrimiento de su origen, que usualmente, es velado en distintos puntos del orbe; a modo de ejemplo, según las estadísticas (EFE, 2009), en Estados Unidos se origina la mayor cantidad de envíos de

[2] Este término es utilizado por primera vez a inicios de la década de los setentas.

phishing, acaparando más del 50%, pero a la vez, se reporta cerca del 62% de los ataques recibidos.

Ante un panorama como el descrito, las entidades bancarias han redoblado esfuerzos a fin de proveerse de seguridades informáticas contra estas actuaciones y procurar que sus clientes no se vean expuestos a la defraudación electrónica, a partir de la utilización de los distintos productos o servicios utilizados.

Complementariamente, se ha requerido de una respuesta legal acerca del tratamiento de este tipo de hechos ilícitos, pues no es suficiente que se tenga una solución informática para repeler o eliminar los fraudes, sin contar con un adecuado marco legal que pueda establecer las responsabilidades y consecuencias punitivas. Esto ha implicado abundantes discusiones en foros internacionales, principalmente en el seno de la Comisión de Naciones Unidas para Derecho Mercantil Internacional.

**La situación de la banca costarricense ante el fraude electrónico.**

La banca costarricense tanto pública como privada, ha experimentado la influencia de la competencia de la banca electrónica de otros entornos, por lo que se ha dado a la tarea de brindar las mismas facilidades electrónicas a sus clientes, de manera que hoy en día, han logrado diversificar sus servicios mediante la utilización de Internet, contando con la ventaja de la existencia de un sistema de pagos de vanguardia en América Latina, denominado Sistema Nacional de Pagos Electrónicos (SINPE), desarrollado a mediados de la década de los noventas por el Banco Central de Costa Rica.

Ello ha venido a disminuir significativamente, el tiempo de realización de diversas transacciones, que en otro momento tomaba varios días, hoy se realizan en línea.

Para el 2005, se estimaba que entre un 65% y un 75% de las transacciones bancarias se realizaban por algún medio electrónico y se registraban tan solo en cinco bancos, alrededor de 602.675 usuarios (Gobierno Digital, 2007).

No obstante, aparejada a esta evolución de los servicios bancarios electrónicos, el sistema bancario nacional también empieza a registrar los mismos perjuicios de los fraudes electrónicos como sus homólogos en otros entornos.

Dicha situación dispara la alerta general, por lo que los bancos empiezan a reforzar sus sistemas de seguridad en el tanto que empiezan a registrarse las primeras demandas en los tribunales costarricenses, promovidas por usuarios de los servicios bancarios que habían sufrido perjuicios patrimoniales, aduciendo la sustracción de información confidencial llámense: números de cuenta, de claves y contraseñas, incluyendo la duplicación fraudulenta de información consignada en dispositivos físicos como tarjetas de crédito, débito, facilitados o por parte de la institución bancaria que da el servicio.

El sector bancario es cuestionado por la recurrencia de distintos casos de hacking y phishing, perdiendo credibilidad ante sus clientes sobre la seguridad con las que mercadeaban sus servicios.

Tras un arduo debate jurídico, en cuanto a la posición o línea doctrinaria acerca de los alcances de las responsabilidad de las partes en relación bancaria (banco-cliente), punto esencial de las resoluciones judiciales, se emiten las primeras condenatorias de los tribunales nacionales en contra de los bancos para el año 2008, lo que terminaba de ubicarlos en una situación de presión extrema.

**El régimen de responsabilidad en la relación bancaria.**

Es evidente que la decisión tomada por los tribunales costarricenses y que ha sido de común aplicación en ordenamientos jurídicos como el español, argentino, venezolano, etc., lleva a la reflexión entorno al fundamento jurídico que llevó a determinar que la responsabilidad sobre los fraudes electrónicos denunciados, recae en la entidad bancaria demandada.

Se reconoce que sería inadecuado pensar de manera superficial, que cualquier demanda en materia de fraude electrónico, tendrá como consecuencia jurídica, la consecuente responsabilidad sobre el demandado y sus derivaciones en materia de resarcimiento.

A partir de aquí, se intenta brindar una descripción de las figuras de la responsabilidad objetiva y subjetiva, que permitirá conocer el fundamento doctrinario que priva a nivel internacional, en materia de fraudes electrónicos bancarios y la que puede llamarse *a priori*, la contrapropuesta.

La responsabilidad objetiva.

Dentro de la doctrina relativa a la responsabilidad, existen dos grandes líneas de pensamiento de conformidad con el análisis y relevancia de elementos como el daño causado, la culpabilidad o dolo del autor y las circunstancias subyacentes en hecho dañino, estas son la responsabilidad objetiva y la subjetiva.

Así, para la determinación de responsabilidad bajo la tesis objetiva, lo relevante es la presencia del daño y la relación de causalidad entre el hecho o acción ejercida y el daño. No es necesario analizar si quien realizó la acción lo hizo de una forma dolosa o negligente. De ese estudio no depende que se indemnice o no el perjuicio. Para indemnizar el perjuicio, sólo basta con demostrar la realización de una acción o la omisión y el nexo de causalidad entre ese actuar o esa omisión y el daño (Alessandri, 1981).

Esta figura – responsabilidad objetiva- ha contado con distintas acepciones durante la historia, dentro de las cuales podemos encontrar: *teoría del riesgo*, *teoría del riesgo creado, teoría del riesgo provecho, teoría del riesgo industrial*, etc., siendo más comúnmente conocido por las tres primeras denominaciones. De una forma muy breve, se dirá sobre estas que:

- Teoría del riesgo: la responsabilidad se asocia en cualquier circunstancia por realizar una actividad peligrosa para terceros; llega a considerarse aún el caso fortuito. Se ha criticado su imprecisión y la falta de planteamiento de la causa del problema a solucionar y de la cual surge la responsabilidad.

- Teoría del riesgo creado: en este caso, hay una atribución de los efectos de un acto al autor del mismo, responde por los riesgos que él mismo ha creado.

-Teoría del riesgo provecho: hace referencia a la distinción entre los hechos dañosos que son o no para su autor, fuente de provecho, de modo tal que sólo los primeros comprometen su responsabilidad. En tal sentido, hay una obligación de reparar los

daños producidos, aún sin culpa, por una actividad que se ejercía en propio interés y bajo la autoridad del que causa el daño; prácticamente conduce a afirmar que quien obtiene de una cosa o negocio el mayor provecho, debe soportar los riesgos.

Nuestros tribunales ante las demandas que se han presentado en materia de fraudes electrónicos, en los cuales ha mediado la relación banco-cliente, se han adherido en sus fallos a la posición objetiva, de modo que analizando dicha relación desde una perspectiva proveedor-consumidor, han concluido que a partir del cuadro fáctico presentado en las distintas demandas, la responsabilidad debe asumirla la entidad bancaria.

El Tribunal Contencioso Administrativo (2008), dentro de la fundamentaciones jurídicas que sustentaron la primera condenatoria a un banco estatal al resarcimiento correspondiente por un fraude informático, reitera la posición sostenida por la Sala Primera de la Corte en distintos fallos, indicando que quien ejerce o se aprovecha de una actividad con elementos potencialmente peligrosos o riesgosos para el cliente, debe soportar los inconvenientes derivados de la actividad. *El elemento imputación de esta responsabilidad viene a estar constituida primordialmente por lo que se conoce como el riesgo creado o la conducta creadora de este riesgo.*

Considera el mismo tribunal, que aún y cuando se hubiese demostrado la participación de un tercero en la comisión del ilícito, no sería un elemento sustancial para la liberación de responsabilidad por parte del banco. Enfatiza que el daño causado se presentó a partir de un medio que la institución bancaria proporciona y que es catalogado como riesgoso. Por lo tanto le compete al banco, brindar todas las medidas de seguridad hacia lo externo de él, por lo que no puede excusarse de manera alguna en la dificultad para que su principal destinatario o consumidor de los servicios, esté debidamente protegido.

Se establece desde una perspectiva de derecho del consumidor, que el comerciante o banco, para efectos del presente artículo, sólo podría relevarse de la responsabilidad en el tanto logre probar que el daño se originó por culpa o dolo del consumidor. Es decir, éste último no tiene que demostrar la culpa del comerciante, puesto que la misma se presume; es al comerciante a quien corresponde probar que es ajeno a la misma (Cámara de Comercio, 2008).

Este criterio ha quedado plasmado en la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor en su artículo 35, en el cual establece que el proveedor y comerciante deben responder concurrente e independientemente de la existencia de la culpa, si el consumidor resulta perjudicado en razón de la utilización del bien o servicio y los riesgos asociados.

La responsabilidad subjetiva.

La doctrina en materia de responsabilidad subjetiva, encuentra su fundamento en el análisis de la conducta del autor del daño, así, a diferencia de la responsabilidad objetiva, para determinar la responsabilidad no basta con la acreditación del daño, es necesario además, que el mismo se derive del actuar doloso o culposo del actor.

Tres son los elementos que deben confluir para establecer que se está en presencia de la responsabilidad subjetiva: el daño, la actuación dolosa o culposa del causante del daño y la relación de causalidad entre los dos elementos anteriores. Cuando se constatan todos los elementos, se genera el deber de indemnizar los perjuicios a la víctima del mismo.

En términos generales, la responsabilidad subjetiva se puede presentar de dos formas: directa o indirecta. La directa o por hecho propio, es aquella en que la conducta propia del sujeto o autor, le obliga al resarcimiento y; la indirecta o por hecho ajeno, el sujeto que realizó la actuación que ocasionó el daño, no es el mismo a quien posteriormente se responsabiliza.

Esta última forma está referenciada al deber o responsabilidad de vigilar las personas, animales u objetos que dependen del responsable y aún de su elección (Centro de Información Jurídica en Línea (CIJUL), 2008).

**Problemática de la vinculación del autor con el documento electrónico.**

Puede observarse, que la posición en la que se ha ubicado al sector bancario en virtud de los fallos judiciales fundamentados en la responsabilidad objetiva, ha forzado a buscar respuesta a dos grandes cuestionamientos: el primero, asociado a la posibilidad de desarrollar y proveer a los clientes o consumidores, un mecanismo y/o procedimiento

electrónico que garantice la seguridad en los servicios ofrecidos y segundo, ¿cómo vincular certeramente al usuario del servicio o producto, con los actos en los que son utilizados?

La respuesta a tales interrogantes parece inicialmente, sugerir un elemento de cambio en la imputación de la responsabilidad, imponiendo la reversión de la carga de la prueba entre las partes a la hora de dirimir un conflicto sobre fraude electrónico.

Equivalencia funcional.

Como se ha planteado, el comercio electrónico y la gama de servicios desarrollados con la evolución informática, descansan en la posibilidad de transmisión de datos, de la que es posible derivar la expresión de voluntad de una o de todas las partes contratantes, con el propósito de llevar a cabo una determinada transacción.

Esa voluntad puede entenderse como explícita, en el tanto un documento la contenga y sin mayor esfuerzo intelectivo se reconozca o bien, implícita, a partir de la realización del envío de la instrucción mediante el sistema electrónico correspondiente, constando de previo, la utilización de claves o contraseñas, según los niveles de seguridad asociado a los sistemas por los cuales se realiza la transmisión.

La determinación de la voluntad manifestada en las transacciones o comunicaciones electrónicas, no es un tema que haya sido resuelto consensualmente por la doctrina, puesto que ha requerido la adecuación de los planteamientos tradicionales de la verificación de la voluntad contractual, particularmente la documental o escrita a las nuevas necesidades y es que la *doctrina tradicional describe el documento como cosas muebles y de ahí deduce que uno de los elementos integrantes de su estructura es la "corporalidad"(cosa mueble). Los otros son el sujeto y los signos de representación, es decir, el contenido* (Rengifo, 2002).

Uno de los principales esfuerzos, ha sido el reconocimiento legal de los documentos incorpóreos con los mismos atributos probatorios que los materiales. En este sentido Remolina (2002), señala que como consecuencia de la utilización de documentos electrónicos, se ha generado la necesidad de reexaminar los conceptos fundamentales o clásicos y extenderlos a un mundo digital.

Tal homologación se visualiza por medio de la aplicación del principio de *equivalencia funcional*, que básicamente procura analizar los propósitos y funcionalidades atribuidos al documento material y determinar de qué forma pueden ser cumplidos por el documento electrónico (Peña, 2001).

Del análisis de tal compatibilidad entre las funcionalidades de ambas especies de documento y sobre todo, de ser cumplidas por un mensaje de datos, *permitirían la atribución a ese mensaje de un reconocimiento legal equivalente al de un documento de papel que haya de desempeñar idéntica función* (Asamblea General de las Naciones Unidas, 1996). Es decir, se presenta la posibilidad del traslado de la seguridad y confianza que se le reconoce al papel a la transacción realizada en un ámbito electrónico.

Se hace la advertencia, que no existe un ordenamiento que muestre la migración total hacia un sistema que prescinde absolutamente de la representación física documental, puesto que ello supondría su correspondiente modernización o actualización de la legislación, se habla más bien, de una transición. Y es que precisamente, por las repercusiones legales que conlleva asociar la eficacia probatoria que por antonomasia han recaído sobre documento escrito al documento electrónico, genera una mayor reflexión por parte de los legisladores.

En consecuencia, se encuentran dentro de los textos normativos conceptos ampliados de lo que históricamente se ha conocido como documento. En el artículo 368 del Código Procesal Civil costarricense, por ejemplo, se amplía la definición y se establece que documento será además del escrito, los impresos, planos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas y todo objeto mueble al que se le asocie un carácter representativo o declarativo, se pretende un acercamiento a la desmaterialización pero sin prescindir del todo del esquema tradicional.

El aprovisionamiento de los atributos del documento material al electrónico se realiza por medio de ficciones jurídicas y soluciones técnicas (Martínez, 2001), estas buscan asegurar en cuanto al contenido y su trasmisión lo siguiente:

a- que el mensaje proviene de la persona que dice que lo envía, autentica la identidad del remitente y asocia el envío a este,

b- que no existió alteración en el camino, por lo que el mensaje se mantiene totalmente íntegro,

c- que el emisor no podrá negar su envío y el destinatario su recepción, el *no rechazo o no repudio es aquel servicio de seguridad que garantiza que una parte interviniente en una transacción no pueda negar su actuación,*

d- además, se ha garantizado la confidencialidad, especialmente en transmisiones con información sensible, protegiéndolas de revelaciones o accesos de personas no autorizadas.

Las anteriores cualidades están ligadas a propuestas de seguridad de la información, que en términos generales pueden resultar adecuadas para minimizar los riesgos o incertidumbres que rodean la transmisión de datos, a partir de su implementación en sistemas o dispositivos informáticos seguros.

Complementariamente, los lineamientos de seguridad descritos supra, establecen o pretenden establecer, una relación directa entre el mensaje o transmisión con el remitente del mismo. Dentro de estos lineamientos, el principal obstáculo a superar está constituido por la posibilidad de repudio de las actuaciones, ya que ante la negación de las mismas, se estaría ante la eventualidad de que el supuesto autor logre eximirse de responsabilidad.

Como ha de recordarse, en materia de fraude electrónico este es uno de los argumentos a evidenciar en el ámbito de la responsabilidad objetiva, a fin de debatir la demostración del nexo incuestionable entre el hecho y su autor.

Bajo un esquema documentario tradicional, existe una figura que reúne en buena medida, las funcionalidades de identificación y autoría ante un contrato o transacción, ésta es la firma, a la que históricamente se le atribuido la característica de ser la expresión de voluntad y conformidad del autor en los actos en que medie.

Se expresa de seguido, de qué forma en el ambiente electrónico se ha buscado también su equivalente con el propósito de dar respuesta a la necesidad urgente de contar con un medio incuestionable de vinculación, entre los actos y su autor.

**La Firma Digital.**

Es importante de forma precedente al análisis del tema de la firma digital, -como la propuesta electrónica actual de seguridad y vinculación en los términos indicados anteriormente-, que se presente una breve retrospectiva del concepto de la firma y de las propiedades jurídicas asociadas a ella.

En términos muy amplios, se ha dicho (Sarra, 2000) que firma *es cualquier rasgo hecho con la intención de expresar el consentimiento a la manifestación de voluntad vertida en el instrumento.* Por otro lado, se indica (Borda, 1970) que la firma es la forma en la que habitualmente un individuo escribe su nombre y apellido con el propósito *de asumir las responsabilidades inherentes al documento que suscribe.*

De acuerdo con los distintos momentos históricos, a la firma se le han asignado una serie de atributos o valores jurídicos, dentro de los más comunes se encuentran:

a- Consentimiento: la firma denota o expresa consentimiento sobre lo expresado en el documento, con el propósito de asignarle determinados efectos jurídicos.

b- Solemnidad: el firmar un documento está asociado a cierto nivel de reflexión acerca de las responsabilidades, derechos o consecuencias jurídicas emanadas del documento, por lo que supone que el firmante no asumiría compromisos de manera inconsciente.

c- Prueba: la firma implica la autenticación de lo consignado en el documento, es decir, identifica al signatario con el documento, por lo que le sería indudablemente, atribuible.

d- Forma: en determinadas ocasiones, en las que se esté frente a actos formales o ad solemnitatem, la firma constituye un elemento de validez.

Ahora bien, dependiendo del ordenamiento jurídico y del caso en particular, una firma podría estar representada mediante el nombre propio, un rasgo distintivo como por ejemplo la rúbrica, una huella digital, etc. *En esencia, la naturaleza de todas estas maneras de firmar es la misma: ellas expresan la autoría de la declaración de voluntad del signatario; lo que difiere es su representación* (Sarra, 2000).

Antecedentes de la firma digital.

El antecedente causal de la firma digital descansa en la necesidad, en virtud del desarrollo tecnológico en materia de comercio electrónico, de proveer un ambiente que contara con un nivel de certidumbre necesaria *para generar obligaciones y vínculos jurídicos semejantes a los que se daban en el entorno tradicional* (Gutiérrez, 2002).

Es a partir de la creciente tendencia del uso de distintas tecnologías de la información, especialmente en la década de los noventas, que el tema de seguridad informática empieza a motivar una serie de estudios y foros a nivel internacional para lograr aquel objetivo.

Esta misión tuvo como catalizador, la promulgación de la *Ley Modelo de la CNUDMI sobre comercio electrónico y otros medios conexos de comunicación de datos*, aprobada por la Asamblea General de las Naciones Unidas en junio de 1996. Desde ese momento, el grupo denominado *Grupo de Trabajo de Comercio Electrónico* enfocó sus esfuerzos en la búsqueda de un *Régimen Uniforme sobre Firmas Electrónicas*, que llegó a ser aprobado como Ley Modelo en junio de 2001.

De esa manera, la Ley Modelo sobre comercio electrónico viene a convertirse en una guía para el legislador de los países asociados, donde la propuesta de reglas o fórmulas jurídicas de la ley, estaban encaminadas a crear un ambiente de seguridad jurídica en materia de transacciones electrónicas.

De acuerdo con Gutiérrez, por medio de técnicas llamadas firmas electrónicas, *la tecnología se encarga de ofrecer mecanismos para que algunas o todas las características de las firmas manuscritas se puedan cumplir en un entorno electrónico*, claro está, por medio del suministro de los equivalentes funcionales de la firma manuscrita.

Aspectos técnicos en la conformación de la firma digital.

Se ha presentado el principio de equivalencia funcional como fundamento de la asociación de los atributos del documento escrito y su correspondiente vínculo con su autor mediante la firma para con el documento electrónico. De este modo se enfatiza en el artículo noveno de la Ley de Certificados, Firmas Digitales y Documentos

Electrónicos, en donde se enfatiza el valor y eficacia probatoria del documento electrónico, amén del reconocimiento de la eficacia de la firma digital.

No obstante, esta ficción jurídica recae sobre un mecanismo informático llamado *firma electrónica*, que conlleva un desarrollo informático con distintos agentes participantes.

Concepto de firma digital.

Se entenderá 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 electrónico* (Ley de Certificados, Firmas digitales y Documentos Electrónicos No.8454, 2005).

Otra definición con un carácter más técnico (Rengifo, 2002), nos indica que la firma digital *consiste en la transformación de un mensaje empleando un criptosistema asimétrico*[3] *tal que una persona que 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.*

Permite además, asegurar la inalterabilidad del mensaje en el transcurso de la transformación; de haber sucedido una modificación, esta sería detectable, pues en la verificación numérica por un procedimiento matemático desde la clave pública, se brinda un valor que sólo pudo haber sido obtenido a partir de la clave privada.

De la última definición pueden extraerse una serie de componentes, que brevemente se describen para efectos de tener una noción muy general de la estructura de la firma digital, dado que el presente artículo no tiene como objetivo la exposición de todos los elementos técnicos que componen la firma digital, sino los más relevantes para el tema en desarrollo. Dentro de estos, se encuentran:

[3] Un criptosistema asimétrico es un algoritmo o serie de algoritmos (cálculos matemáticos) que son utilizados para generar y asociar un par de claves confiables (clave pública y clave privada). Se diferencia de la criptografía simétrica por que en los cálculos utilizados por este procedimiento, sólo se genera una clave.

a. La criptografía: ciencia que trata del enmascaramiento de la comunicación de forma tal que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto (Microsoft® Student 2009 [DVD]. Microsoft Corporation 2008).

b. Clave pública y clave privada: son combinaciones de cálculos matemáticos asociados a través de la función de una sola vía basada en la dificultad de multiplicación inversa (Rengifo, 2002). Es la clave pública la que eventualmente puede compartirse, de modo que quien la posea, puede corroborar la firma, verificando que el documento ha sido firmado por quien tenga acceso a la clave privada.

Los certificados digitales.

El contar con las claves, no resuelve del todo el problema de la identificación de quién es el emisor del mensaje, puesto que el receptor debe tener certeza de la veracidad misma, es decir que no medie suplantación de quien facilitó la clave pública, esto propone la necesidad de la autenticación de identidad.

Ello se logra por medio de la obtención de una certificación digital de la firma, suministrada por un tercero de confianza, denominado entidad de certificación, por lo que una *firma digital se considerará certificada cuando haya sido emitida al amparo de un certificado digital vigente, expedido por un certificador registrado* (Ley 8454, art.8).

El certificado es *un documento electrónico que contiene un conjunto de información a la que se ha fijado una firma digital por alguna entidad que es reconocida y en la que confía alguna comunidad de usuarios de certificados* (Martínez, 2001).

Este instrumento permite, según la ley citada, garantizar, confirmar o validar por medios técnicos, la vinculación jurídica entre un documento, una firma digital y una persona y por otro lado, la integridad e inalterabilidad del documento y la firma digital asociada.

La utilización de la certificación digital, en el ámbito de la prueba, establece un nuevo enfoque, dado que permite establecer presunciones de autenticidad basadas en

medios tecnológicos. En razón del nivel de tecnología y las exigencias demandadas a las entidades de certificación –de las que hablaremos de seguido- convierte a la presunción, en casi irrefutable (Peña, 2003).

**Las Autoridades de Certificación (CA).**

Las Autoridades de Certificación[4] o certificadores, son entidades públicas o privadas, dedicadas a la emisión de certificados que contienen información acerca de hechos o circunstancias del sujeto del certificado, que vinculan un par de claves con una persona determinada, cubriendo la necesidad de una tercera parte de confianza al tener la obligación inicial, de dar fe acerca de la identificación del suscriptor[5].

Las CA pueden ser cerradas, en el tanto ofrezcan la certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor sin exigir remuneración por ello, y pueden ser abiertas, si ofrecen servicios propios de intercambio de mensajes entre la entidad y el suscriptor o bien, recibe remuneración por la prestación de servicios.

Dentro del esquema de las CA, estas pueden desempeñar distintos papeles; pero son las públicas quienes pueden actuar como Autoridad de Certificación Raíz (CA Raíz) de la estructura de certificación de un país, de modo que tiene la atribución de certificar al resto de CA privadas.

De conformidad con la organización prevista en la Ley 8454 y las circunstancias de nuestro país, la CA Raíz se encuentra a cargo del Ministerio de Ciencia y Tecnología (MICIT) y la única CA en el país está ubicada en el Banco Central de Costa Rica en virtud de contar con dos ventajas importantes: una infraestructura con altas seguridades físicas y una plataforma electrónica robusta y certificada en el tratamiento de la información, como lo es el SINPE.

[4] El grupo de trabajo sobre comercio electrónico de la UNICITRAL en su reunión 31, criticó la utilización del término “autoridad” y propuso en su lugar “entidad”, dejando a cada Estado la decisión de someterlo o no, a un régimen jurídico de autorización. En Costa Rica se sigue el esquema de “autoridades”, en ordenamientos como el español, se habla de “entidades” por considerarse neutral.

[5] Según el apartado 1.3.3 del documento denominado Política de Certificados para la Jerarquía Nacional de Certificadores Registrados (Política de Certificados), el suscriptor es el usuario final a quien se le ha emitido un certificado por una CA; el suscriptor puede ser un individuo o una organización.

Si bien es cierto, instituciones públicas o privadas, personas jurídicas o físicas están facultadas por ley para establecer los mecanismos de certificación, a fin de constituirse en una CA (arts. 11 y siguientes de la Ley 8454), deben cumplir con una serie de requisitos indispensables, legales y técnicos, a fin de validar su posición de tercera parte de confianza.

Estos requisitos se clasifican, según Martínez, básicamente de la siguiente forma:

a. Requisitos técnicos: donde debe contarse con la utilización de sistemas seguros y de confianza para el desarrollo de sus actividades, considerando también, la implementación de planes contingentes.

b. Requisitos de personal, que debe ser competente, tanto desde el punto de vista de la gestión como de la técnica y de confianza,

c. Requisitos financieros y de garantía, para efectos de desarrollar el negocio y para afrontar una eventual responsabilidad por daños.

Las Autoridades de Registro (RA).

En algunas ocasiones las CA requieren de la participación de otros entes a fin de obtener la información esencial y requerida de los suscriptores de la firma digital, para ello, se apoyan en el trabajo que realizan las Autoridades de Registro o registrantes que son *instituciones de inferior rango que las autoridades de certificación, encargadas de facilitar las pruebas de identificación y de comprobar la identidad de los potenciales usuarios* (Sarra, 2000).

Deben entonces las RA, establecer los mecanismos de validación de dicha información, dependiendo del tipo de certificado requerido y con base en las políticas vigentes, por lo que está fuera de su accionarla emisión de certificados.

En nuestro país, al existir una sola estructura de certificación, la firma digital obtenida de una CA, es válida en los distintos escenarios transaccionales donde esta es aceptada, pues se trata de una tecnología común.

De lo expuesto anteriormente y desde el punto de vista de negocio, podrían visualizarse la participación directa o indirectamente de una RA: primero, que una

institución busque ofrecer servicios, a los cuales se accede mediante una firma digital por lo que se requiere la participación de una RA o segundo, que la institución oferente se constituya, con arreglo de la ley, en una RA, ya que sería incoherente, que alguna institución, por ejemplo bancaria, indique a sus clientes que deben registrarse en una RA de alguno de sus competidores.

**De las responsabilidades de los participantes.**

La obtención de una firma digital, está sujeta a una serie de tratamientos que parten de la verificación de la identidad del suscriptor o solicitante hasta la vinculación de la misma con las claves correspondientes y su inclusión en el dispositivo físico designado (llámese tarjeta inteligente,[6] o token usb[7], etc.).

En ese proceso participan distintas instancias, por lo que a cada una de ellas se les atribuye distintas responsabilidades derivadas de las funciones que se les ha asignado por ley, sin dejar de lado las responsabilidades que le competen al mismo usuario, durante el proceso de acreditación y posterior a la entrega del dispositivo de firma digital.

La necesidad de clarificar y definir el tema de las responsabilidades de las partes involucradas en el sistema de uso de certificados, es *una de las cuestiones críticas y esenciales para el desarrollo y buen funcionamiento del sistema por las consecuencias que de ello se derivan* (Martínez, 2001).

En términos generales, se puntualizan las responsabilidades de los actores enunciados: CA, RA y suscriptores. Considérese que la asignación de cargas u obligaciones está en función del ordenamiento jurídico que se estudie, no obstante, se brindan algunos puntos de común aceptación:

[6] Se suele denominar *tarjeta inteligente o smart card* a una tarjeta de plástico u otro material, similares a las tarjetas de crédito o débito, con la particularidad de habérsele incorporado una unidad de procesamiento o "chip".

[7] Un *token* es un dispositivo físico, similar a las denominadas "llaves maya", utilizado para guardar información, incluyendo la llave privada del suscriptor y que se conecta al puerto USB del computador.

En cuanto a las Autoridades de Certificación o Entidades de Certificación:

Es evidente que las CA tienen un papel preponderante en la gestión de la firma digital, su responsabilidad *está vinculada a los amplios deberes establecidos por la ley, los cuales las convierten en custodios de la información suministrada por los usuarios, además les obligan a implementar sistemas de seguridad adecuados para que los mecanismos de firmas y certificados sean confiables* (Peña, 2003). De acuerdo con el punto 9.4.4 del documento Política de Certificados para la Jerarquía Nacional de Certificadores Registrados (en adelante Política de Certificados), las CA tienen el deber de asegurar que la información privada no puede ser comprometida o divulgada a terceras partes.

La responsabilidad de las CA se proyecta tanto para los prestadores de servicios como para los suscriptores o terceros que confíen en los certificados, según Peña, una persona que sufra un perjuicio en una transacción en la que pueda probar su actuación basada en un certificado digital, podría demandar no solamente al comerciante (proveedor del servicio), sino también a la entidad de certificación.

Cuando una entidad de certificación emite un certificado, estaría comprometiéndose a declarar que:

a. No hay falsas declaraciones en el certificado conocidas u originadas por la CA.
b. No existen errores de transcripción en los datos por lo que estos fueron consignados tal y cual se recibieron de los suscriptores.
c. El certificado cumple con todas las exigencias, según se establece en la normativa asociada (Martínez, 2001).

Lo anterior con el propósito de establecer la exactitud y el cumplimiento con los estándares recomendados en la emisión de certificados digitales. Por lo tanto, se le ha asignado la responsabilidad de validar la identidad del solicitante, suministrada directamente o por medio de las RA.

Una vez emitido el certificado con base en la información consignada en la solicitud, la CA se encargará de enviarlo a la RA para que esta lo entregue al suscriptor.

*El proceso de descarga o instalación del certificado respectivo por parte de la CA (…) constituirá la aceptación del certificado* (Apartado 4.4.1 Política de Certificado).

En cuanto a las Autoridades de Registro:

Como se había anticipado, las RA pueden brindar el servicio de recopilación de información proveniente de los suscriptores y dar fe de su veracidad como primeros receptores de la documentación, por lo que se constituyen en responsables de la identificación y autenticación del solicitante.

Su responsabilidad es la de garantizar, según el punto 9.6.2 de la Política de Certificados:

a. Que no se presentan distorsiones en la información contenida en el certificado.

b. Que no existen errores en la información del certificado que fue introducida por la RA, y

c. Que los dispositivos y materiales requeridos cumplen con los requisitos establecidos.

En cuanto al procedimiento común, es responsable del registro y verificación de la identidad del solicitante y el posterior envío de la solicitud a la CA y una responsabilidad no menos importante, informar al suscriptor de sus deberes y responsabilidades.

De la responsabilidad del suscriptor:

El suscriptor, como usuario de la firma digital y por lo tanto, del certificado correspondiente, es sujeto de obligaciones en dos momentos: primero, está obligado a presentar toda la documentación que se requiera a fin de que la acreditación de su identidad no permita duda alguna, independientemente si se trate de una persona física o jurídica que esté realizando la solicitud de emisión de un certificado digital.

Segundo, según lo establecido en el apartado 4.1.2 del documento Política de Certificados, el suscriptor debe firmar un acuerdo en el que constan sus deberes y responsabilidades asumidas en la utilización del certificado.

Dentro de las políticas que regulan las prácticas de certificación, se suele asociar al suscriptor, la aceptación de otra serie de deberes referidos al resguardo y utilización del certificado que encierra la clave privada. Según Martínez, el suscriptor *asume un deber de mantener el control de su clave privada y tomar precauciones razonables para prevenir la pérdida, revelación, modificación o uso no autorizado.*

Con relación al ámbito de la responsabilidad del suscriptor o usuario de la firma digital, se procurará ahondar un poco más en el siguiente apartado en razón de la importancia que conlleva en la reflexión de fondo de este artículo.

**De la presunción de autoría y responsabilidad del suscriptor o usuario de la firma digital.**

Conforme al tema de las responsabilidades y funciones de los distintos participantes en la emisión de una firma digital y su correspondiente certificado asociado, se pretende dar énfasis a la responsabilidad que se le atribuye al usuario de la firma digital, a la luz del planteamiento inicial de este texto, en razón de su posición como un consumidor o usuario de servicios ante una entidad oferente, pero ahora transformada con la inclusión de un tercero que se encarga de proveer seguridad en la relación, llámese Autoridad de Certificación.

Se indicó que el suscriptor debe cumplir con las obligaciones de brindar la información requerida, y cumplir con el formalismo de la solicitud, pero que además, una vez emitido el respectivo certificado, estaba obligado a una serie de responsabilidades atinentes al uso y resguardo de su clave privada.

Sobre este tema se expresó en el cierre del apartado anterior, que el suscriptor debe tomar las medidas correspondientes para la salvaguarda de la información privada de su clave y para ello, las CA con base en las prácticas de certificación, procuran brindarse de una protección mediante el establecimiento de cláusulas de responsabilidad.

Esa práctica, ha llevado al punto del establecimiento de cláusulas limitativas o exonerativas de la responsabilidad, derivado del grado de incertidumbre de un panorama mundial, donde las responsabilidades se pueden tornar en ilimitadas, amén de la

carencia de un marco jurídico claro en esta materia; situación aunada a los distintos litigios presentados y los eventuales por enfrentar, lo que genera una actuación sumamente cauta por parte de las CA.

Un exceso de protección en este sentido, puede devenir en un acentuamiento del desbalance entre los contraprestadores de una relación y por supuesto, en contra principalmente, de la parte más débil, por lo que aplica el principio general de que nadie puede exonerarse absolutamente, de las consecuencias de las obligaciones que contrae.

Al suscriptor de la firma digital se le compele a proteger la clave privada, pues debido al reconocimiento jurídico y legal de las firmas digitales, se le asocia la autoría y responsabilidad de toda transacción en la que medie la firma digital y se ha dicho que *el uso seguro y eficaz de la criptografía asimétrica depende (…) de que la clave privada sea mantenida en secreto y utilizada sólo por la misma persona o entidad que es identificada en el correspondiente certificado de clave pública* (Martínez, 2001).

Esta posición llega a plantearse o alegarse en contra de aquel suscriptor que pierde el control sobre la privacidad de la firma digital, pues la atribución de autoría se le seguiría imputando. La falta de observancia de las medidas de seguridad sobre la utilización de la firma, puede tener como consecuencia, la revocación del certificado digital.

**La firma digital en Costa Rica.**

A inicios de la presente década, en el ordenamiento costarricense, se comienza a analizar el tema de la seguridad y su regulación en las transacciones comerciales, lo que viene a ser acelerado por el incremento del uso tecnológico y por la serie de ilícitos informáticos que se evidencian en casi todo el mundo.

En consecuencia, se ve la necesidad de contar de contar con la implementación de un marco normativo, acorde con los mecanismos imperantes de seguridad informática de la información. Por ello se genera la búsqueda de la promulgación de una ley en materia de certificación y firma digital.

Aprendiendo de los avances de otros ordenamientos, se recogen los principios y lineamientos vigentes en latitudes europeas y suramericanas, brindando un asidero para

lo que se plantearía por medio del expediente No.14.276 conocido por la Asamblea Legislativa, y bajo el cual se analizó el proyecto de ley sobre la firma digital.

Según los ponentes del texto, la *regulación propuesta pretende mantener la armonía con los elementos principales de la regulación internacional sobre el tema, brindando el marco jurídico adecuado y viable para la contratación electrónica, y en general, las relaciones jurídicas basadas en la comunicación mediante medios informáticos o telemáticos, sean o no de índole comercial*.

Fue así como en octubre de 2005, no sin pocas discusiones, se publicó la Ley No.8454[8], que regula la figura de la Firma Digital y toda la estructura de implementación en Costa Rica, brindando el marco regulatorio de un servicio que apenas empieza a dar sus primeros pasos en un plan piloto, programado por el Banco Central con algunos de sus empleados (Agüero, 2009). Existen algunos bancos como el Banco Popular, que estarían dispuestos a facilitar gratuitamente, la firma digital para algunos de sus clientes, máxime que las primeras incursiones de uso programadas para la firma, se realizarán en transacciones electrónicas bancarias.

Debe considerarse que ante la magnitud de la utilización de la firma digital, existen dos elementos adicionales que no pueden obviarse:

a. Que un factor primordial para la efectividad de la firma digital, es de tornar su uso en *práctico y difundido, por lo tanto, la tecnología más avanzada busca que cada persona pueda tener en su identificación, por ejemplo la cédula de ciudadanía, un número de identificación digital que pueda ser utilizado en transacciones y actividades cotidianas* (Peña, 2003). Esta meta es visionada en el desarrollo de la firma digital en Costa Rica, que se proyecta que a un mediano plazo se incorpore el respectivo dispositivo en las cédulas de identidad, sin embargo, en el corto plazo, se incursionará inicialmente, con la utilización de una tarjeta inteligente (smartcard).

b. Conforme las características de la estructura de emisión de firmas digitales en Costa Rica, en las que se identifica sólo una CA, el usuario de una firma digital estaría en la posibilidad de utilizarla en los distintos servicios que las diferentes entidades

[8] Ley No.8454 Ley de Certificados, Firmas Digitales y Documentos Electrónicos publicada en el Diario Oficial La Gaceta No 197, del 13 de octubre de 2005.

brinden o en los negocios de distinta naturaleza que lo requieran, ya que se trata de una misma tecnología de certificación.

Este avance tecnológico-jurídico involucra la introducción de elementos nuevos en las transacciones electrónicas; consecuentemente, con la responsabilidad del suscriptor de la firma digital, surge la inquietud de determinar si el esquema de la responsabilidad objetiva, que ha imperado en las relaciones –bancarias para nuestros efectos- según el fallo de nuestros tribunales y las disposiciones en materia de protección al consumidor persiste, o bien, aporta el fundamento fáctico y jurídico suficiente para cambiar la perspectiva, tomando ahora en cuenta, la tesis de la responsabilidad subjetiva.

Se retoma entonces, mediante un ejercicio más reflexivo, el planteamiento propuesto al inicio de este documento, sobre el esquema de las responsabilidades en la relación de un usuario de servicios bancarios frente a la empresa bancaria, pero ahora contando con las funcionalidades de la firma digital para los servicios ofrecidos por la banca, cuyo certificado digital es expedido por un tercero (CA) y con la eventual participación de una RA como facilitador de información del suscriptor.

Se parte de un ejercicio de valoración de las condiciones presentes en el actual ordenamiento costarricense, ya que por la novedad del tema de firma digital en Costa Rica, no se cuenta con jurisprudencia que sugiera la orientación hacia una posición u otra, de la cual se derive además, la asimilación jurídica de los alcances de los certificados y firmas digitales.

La seguridad tecnológica y jurídica.

Uno de los componentes principales a considerar desde el punto de vista del usuario de la firma digital, es el riesgo, elemento fundamental para la determinación de la responsabilidad objetiva, y tal como se estableció se mitiga con certeza y seguridad, tanto tecnológica como jurídica.

a. Seguridad tecnológica.

El factor de seguridad, introducido por la tecnología implícita en la generación del certificado y firma digital, permite un alto grado de certeza respecto a la inviolabilidad e integración de la información.

Como ejemplo, según algunos cálculos se indica que la derivación de una clave privada a partir de una clave pública, implicaría que el número de claves por verificar sería de $1.9 \times 10^{29}$, *se tendría teóricamente que hoy se demorarían más de 1000 años todos los posibles computadores existentes funcionando al mismo tiempo, de forma continua y trabajando para solucionar el mismo problema, para poder probar todas las soluciones posibles* (Zubieta, 2002). Debe entenderse por supuesto, que a medida que el poder informático aumenta, se presentan nuevos y más complejos procedimientos para realizar cálculos matemáticos, de manera que la brecha se acorta.

En el tanto que en la emisión del certificado y firma digital impere el seguimiento de los estándares electrónicos, y las recomendaciones internacionales en materia de seguridad de la información, los suscriptores podrían contar con un servicio que provee seguridad electrónica.

b. Seguridad jurídica.

La seguridad jurídica ha de manifestarse por medio de la creación legislativa, de instrumentos normativos que tutelen el interés de las partes que se involucran, tanto en la emisión de la firma certificada como en la posterior utilización de dicho instrumento.

El marco normativo en nuestro país, como se ha dicho, lo provee la Ley 8454 además de las distintas regulaciones reglamentarias, de políticas y directrices emitidas por el MICIT; esta normativa consigna las reglas que han de seguir los distintos participantes en la emisión y suscripción de la firma digital.

Según Carlos Melegatti, subgerente del Banco Central y propulsor del proyecto de Firma Digital en Costa Rica, la seguridad jurídica viene dada en el tanto, anteriormente algunos servicios brindados por los bancos, no contaban con una ley que los respaldara, como sí la tiene la Firma Digital (Agüero, 2009).

**El suscriptor de la firma digital y la presunción de autoría y responsabilidad según el artículo 10 de la Ley 8454.**

Con respecto al artículo 10 de la Ley 8454, donde se establece el cargo dado por ley al usuario, la norma establece la *Presunción de autoría y responsabilidad* del suscriptor de la firma digital certificada, de manera que *todo documento, mensaje*

*electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.*

Por consiguiente, la normativa costarricense establece el vínculo de autoría de los mensajes o transacciones realizadas por medio de una firma digital, lo que sobrelleva el enfrentamiento por parte del suscriptor, de las responsabilidades que se deriven de ellas y en consecuencia, el no repudio por parte del suscriptor de las actividades generadas, que lo ubicaría en una situación de difícil solución si se presentase un fraude electrónico, cuyo perjuicio patrimonial opera en su contra o bien, de un tercero que confirma y valida el mensaje electrónico.

Se han establecido las razones por las cuales se le asocia al suscriptor, la autoría de un documento o transmisión de datos asociada a una firma digital, por lo que se puntualiza la *presunción de responsabilidad* y el requerimiento de *prueba en contrario* que expresa la ley en el artículo supra mencionado.

Esta delimitación obedece a la consideración de la ley, que estaría estableciendo la responsabilidad subjetiva en el uso de la firma digital, que implica la reversión de la carga de la prueba y la imputación de la responsabilidad, independientemente de un comportamiento doloso o culposo del suscriptor.

La presunción es definida como un *hecho que la ley tiene por cierto sin necesidad de que sea probado* (Microsoft® Student 2009 [DVD]. Microsoft Corporation 2008), ello quiere decir que cualquier acto y sus consecuencias son atribuibles a un determinado individuo por disposición de ley.

Para el suscriptor de una firma digital, corresponde entonces, afrontar la responsabilidad de los actos derivados de la utilización de dicho instrumento, salvo que pueda demostrar que no fue él quien generó la transmisión o estampó la firma.

En el caso de un daño patrimonial para el suscriptor, o para un tercero confiante de la firma digital sobre un mensaje o transacción realizada electrónicamente, forzaría al primero, -con el propósito de buscar la exoneración de la responsabilidad-, a probar aspectos como:

- que hubo un vicio en su voluntad por lo que no existiría un consentimiento de firmar, así que correspondería la aplicación de los principios sobre validez y eficacia del acto,

- demostrar que no hubo un uso desautorizado de la firma por un tercero, por lo que cumplió con el compromiso de resguardar diligentemente el acceso a ella, aunque ha de considerarse que aún bajo tales circunstancias según lo consigna la ley, las consecuencias le son achacables.

Además de ellos, por el principio de la reversión de la prueba, debería demostrar un posible yerro en el proceso de estructuración de su firma digital, o que hubo una fuga de información, que se presentó un error en el proceso de incorporación de la misma por parte de la RA o de la CA o eventualmente, el acceso no autorizado que haya vulnerado las bases de datos de los certificadores.

Lo anterior indica que la seguridad jurídica para los efectos del suscriptor de la firma digital, se restringe prácticamente a los siguientes aspectos: enterarle de los requisitos de suscripción; su obligación de resguardo y cuido de la firma; e informarle de la imputación de la responsabilidad sobre las actuaciones, envíos de datos o realización de transacciones en las que media un certificado digital a su nombre.

**Conclusiones.**

- La creación de la firma digital como instrumento que coadyuva a la agilización del comercio electrónico, ha venido a realizar un aporte importante en el tanto impulsa a la desmaterialización de los instrumentos que históricamente, se han utilizado para brindar eficacia a los negocios. Ello gracias a la ficción jurídica de atribuir la equivalencia funcional de los atributos probatorios del documento escrito.

- La construcción de un certificado digital y su implementación con la firma digital, a partir de la aplicación de estándares de seguridad de la información reconocidos y desarrollados internacionalmente, provee un mecanismo de muy alta seguridad frente a las vulnerabilidades que poseían instrumentos o dispositivos anteriores. Por lo que la robustez que muestra la firma digital para el sector bancario, entre otros, constituye un factor que incrementa la confianza en las operaciones electrónicas.

- No obstante, el elemento de seguridad aportado por la firma digital responde parcialmente a la eliminación de los factores esenciales que fundamentan la imputación de la responsabilidad objetiva, tal es el caso del riesgo. Este se disminuye por las particularidades algorítmicas de su construcción, mas sin embargo, aparecen nuevos factores de riesgo como la posibilidad de fuga de información, errores materiales en la consignación de información, etc., debido a la participación de distintos actores en la emisión y distribución de los dispositivos.

- Por otra parte, se determina que la facilidad que brindarían instituciones bancarias de proveer el dispositivo de forma gratuita a sus clientes podría interpretarse como una exposición al riesgo, máxime que al momento no cuentan con el envío de mensajes certificados de confirmación.

- La ley 8454, que regula la Firma Digital en Costa Rica, es omisa en cuanto a la protección del suscriptor de la firma desde la perspectiva del consumidor o usuario de servicios, más bien, por presunción de ley, obliga al usuario a que, en caso de requerir desmentir la utilización de la firma en un determinado acto o

transacción, tener que probar hechos o actos realizado por distintos participantes, llámense: Autoridades de Registro, Autoridades de Certificación, instituciones bancarias, etc., lo que acentúa el desbalance existente en la relación de un usuario ante cualquiera o todos los actores dichos. La carga de la prueba para el usuario tiende a tornarse en una imposibilidad material.

- La eficacia de la firma digital, descansa en fortalezas, tanto tecnológicas como jurídicas, no obstante, no se consideran lo suficientemente amplias para desestimar la objetivación de la responsabilidad, por lo que se ha requerido de la necesidad de acudir a la presunción legal a fin de dar un giro al ámbito de la responsabilidad. Martínez (2002) señala que la opción por una responsabilidad objetiva o subjetiva es una decisión de política legislativa, y a la luz del artículo 10 de la ley 8454, parece intuirse cuál ha sido la decisión del legislador costarricense.

## Bibliografía.


- Sentencia 708 (Tribunal Contencioso Administrativo 19 de setiembre de 2008).
- Agüero, M. (15 de junio de 2009). Clientes del Popular y Central Directo estrenarán firma digital. *La Nación* , pág. 27A.
- Alessandri, A. (1981). *De la responsabilidad extracontractual en el Derecho Civil.* Santiago: Imprenta Universal.
- Asamblea General de las Naciones Unidas. (1996). *Resolución 51/162.*
- Borda, G. (1970). *Tratado de derecho civil argentino. Parte general.* Buenos Aires: Perrot.
- Cámara de Comercio. (2008). *Cámara de Comercio de Costa Rica.* Recuperado el 22 de mayo de 2009, de www.camara-comercio.com/images/public/documents/doc/Responsabilidad.doc -
- Centro de Información Jurídica en Línea (CIJUL). (2008). Recuperado el 22 de mayo de 2009, de http://aslegalcr.com/blog/wp-content/uploads/2008/01/1411_responsabilidad_civil_subjetiva_extracontractual.pdf
- Cifuentes, M. (2002). Una mirada introductoria al mundo de la Banca Electrónica. En D. d. Universidad Externado de Colombia, *Memorias: Comercio Electrónico* (págs. 68,77,78). Colombia: Dpto. Publicaciones, Universidad Externado de Colombia.
- CNUDMI. (s.f.). *www.uncitral.com.* Recuperado el 12 de mayo de 2009, de www.uncitral.com
- EFE. (2009). *AOL.noticias*. Recuperado el 15 de mayo de 2009, de http://www.aol.es/noticias/story/Espa%C3%B1a-registra-el-3-por-ciento-de-los-ataques-%22phishing%22-a-la-banca-en-el-mundo/3378274/index.html
- *Glosario.net*. (2009). Recuperado el 12 de mayo de 2009, de http://tecnologia.glosario.net/terminos-viricos/phishing-9807.html
- *Gobierno Digital*. (2007). Recuperado el 15 de mayo de 2009, de http://www.gobiernofacil.go.cr/gobiernodigital/informes/PROSIC2007/cap10.pdf
- Guerrero, M. (2003). La ciberdelincuencia: La Ley Patriótica y los efectos globales en las regulaciones nacionales y en particular el caso colombiano. En U. d. Andes, *Derecho de Internet & Telecomunicaciones* (pág. 100). Colombia: LEGIS.

- Gutiérrez, M. (2002). Consideraciones sobre el tratamiento jurídico del comercio electrónico. En U. d. Andes, *Internet, Comercio Electrónico & Telecomunicaciones* (pág. 177). Colombia: Legis Editores S.A.

- (2005). *Ley de Certificados, Firmas digitales y Documentos Electrónicos No.8454.*

- Martínez, A. (2001). *Comercio electrónico, Firma digital y Autoridades de certificación.* Madrid: Gráficas Rogar S.A.

- Microsoft® Student 2009 [DVD]. Microsoft Corporation 2008. (s.f.). Criptografía (comunicaciones).

- Ministerio de Ciencia y Tecnología (MICIT). (2008). *Política de Certificados para la Jerarquía Nacional de Certificadores Registrados.* San José: MICIT.

- Peña, D. (2001). *Aspectos legales de internet y del comercio electrónico.* Bogotá: Dupré Editores.

- Peña, D. (2003). *El contrato electrónico y los medios probatorios.* Bogotá: Depto. de publicaciones Universidad Externado de Colombia.

- Peña, D. (2003). *Responsabilidad y Comerico Electrónico. Notas sobre el daño y el riesgo en la sociedad de la información.* Bogotá: Dpto. de Publicaciones Universidad Externado de Colombia.

- Prigogine, I. (2000). Comercio Electrónico. En A. Sarra, *Comercio Electrónico y Derecho* (págs. 279, 280). Buenos Aires: Astrea.

- Remolina, N. (2002). Desmaterialización, documento electrónico y centrales de registro. En U. d. Andes, *Internet, Comercio Electrónico & Telecomunicaciones* (págs. 6,7,13). Colombia: Legis.

- Rengifo, E. (2002). Comercio Electrónico, Documento Electrónico y Seguridad Jurídica. En U. E. Colombia, *Comericio Electrónico* (pág. 36). Bogotá: Universidad Externado de Colombia.

- Rica, A. L. (2005). *Código Procesal Civil.* San José: Investigaciones Jurídicas S.A.

- Sarra, V. (2000). *Comercio electrónico y Derecho.* Buenos Aires: Astrea.

- Zubieta, H. (2002). *Los mensajes de datos y las entidades de certificación.* Colombia: LEGIS.