CAPÍTULO II

MARCO TEÓRICO

1. - ANTECEDENTES DE LA INVESTIGACIÓN

Son innumerables los trabajos que se han dedicado al estudio de la firma electrónica dentro del comercio electrónico la mayoría de ellos centrados en el uso de técnicas criptográficas y la firma digital por ser los más conocidos y utilizados. Sin embargo, muy pocos consideran el uso de técnicas biométricas en la misma.

Federico Fumus durante el “II Congreso Internacional por Internet sobre Aspectos Jurídicos del Comercio Electrónico”, realizado en Agosto del 2001 en Argentina, presentó su ponencia denominada “Algunas Aproximaciones a la Firma digital” donde hace mención a que hay sistemas que toman como referencia parámetros biométricos.

Fumus indica que existe una corriente que considera que “estos métodos...” por sí solos no son utilizables para firmar digitalmente pues no conllevan un secreto no compartido”, no obstante lo cual...” pueden utilizarse en conjunto con la criptografía de clave pública para crear firmas digitales”. “

Fumus, sin embargo no descarta la posibilidad de que en un futuro

cercano y gracias al desarrollo de la tecnología biométrica estén disponibles técnicas que garanticen la autoría e integridad del mensaje con un nivel igual o superior al que registran los métodos criptográficos.

Aunque el autor hace la referencia con la intención de fortalecer su opinión relacionada con la adopción del principio de neutralidad tecnológica por parte de las legislaciones en materia de firma electrónica, la investigadora considera el tema de la firma biométrica muy interesante, por considerar que puede aumentar la seguridad jurídica del comercio electrónico, por lo cual se dedicará al estudio de la misma en la presente investigación.

Por su parte María Martín, en su artículo denominado “El Reconocimiento de los Medios Electrónicos en el ámbito Legislativo y Jurisprudencial. Especial consideración del R.D.Ley 14/1999, de 17 de septiembre, sobre Firma Electrónica y Proveedores de Certificación”, publicado en la Revista Electrónica de Derecho Informático (REDI), en el mes de diciembre de 1999; al analizar las definiciones de firma electrónica dadas por el Decreto-Ley español considera que la firma electrónica simple incluye: los passwords, PIN, escaneo digital de la firma autógrafa estampada sobre una pizarra digitalizadora, o técnicas biométricas, debido a que la firma simple es definida por el Decreto-Ley como el conjunto de datos asociados a otros datos electrónicos que sirven como medio para identificar al autor.

Martín, considera que las técnicas biométricas sirven exclusivamente para identificar al autor del mensaje.

Graciela Rolero en un artículo publicado en la página web Derecho Virtual Argentino y Titulado “Firma Digital: Consideraciones Técnicas y Jurídicas” en uno de sus partes que titula firma digital, hace referencia a que se imponen nuevos criterios de identificación, tales como el código o clave secreta, la huella digital, la lectura de pupila, el procesamiento del habla, firma digital, etc., pero al hablar de la huella dactilar y la voz solo se limita a describir muy brevemente en que consiste.

2. - BASES TEÓRICAS

Las bases teóricas se desarrollan en 3 vertientes; las bases jurídicas, las bases biológicas y las bases técnicas. Las primeras comprenden las teorías de la certeza y la seguridad jurídica y sus elementos teóricos con el fin de aplicarlos a los sistemas biométricos y la firma biométrica. Las bases biológicas por su parte parten del principio de la herencia poligénica y comprenden la descripción de los sistemas biométricos en general con la finalidad de conocer sus características, funcionamiento y de esta manera poder determinar su aplicabilidad en el comercio electrónico, cuyos elementos teóricos se desarrollan en las bases técnicas.

2.1. – BASES JURÍDICAS

2.1.1. - PRINCIPIO DE AUTONOMÍA DE LA VOLUNTAD DE LAS PARTES.

El principio de autonomía de la voluntad de las partes consiste en considerar que toda persona solamente puede obligarse en virtud de su propio querer libremente manifestado, es decir, solamente la voluntad del sujeto de derecho es apta para producir obligaciones.

Esto implica:

1. - Las partes pueden pactar entre ellas las prestaciones que deseen, lo que facilita el uso de los llamados contratos innominados.

2. - Las partes son libres de regular como bien lo quieran las prestaciones de un contrato; por lo que la mayoría de las normas legales en materia de contratos son supletorias de la voluntad de las partes y rigen solamente en los casos en que nada haya sido previsto por éstas. Igualmente las partes pueden derogar la mayoría de las normas del Código Civil, y aun establecer formalidades especiales distintas a las legales, o de las no contempladas en el ordenamiento legal; con la sola limitación de que estas normas no violen el orden público o las buenas costumbres.

2.1.2. - PRINCIPIO DE LA LIBERTAD DE PRUEBA

La principal finalidad de la prueba es lograr en el juez la convicción sobre

la existencia o inexistencia de los hechos que interesan al proceso, en forma que se ajusten a la realidad. Esto hace necesario que se otorgue libertad para que las partes y el juez puedan obtener todas las que sean pertinentes, con la única limitación de aquellas que por razones de moralidad, versen sobre hechos que la ley no permite investigar, o que resulten inútiles, por existir una presunción legal que las hace innecesarias como por ejemplo el caso en el cual se persiga probar lo presumido o cuando se intenta desvirtuar una presunción de derecho, o que sean claramente impertinentes o idóneos o aparezcan ilícitas por otros motivos.

2.1.3. TEORÍA DE LOS VICIOS DEL CONSENTIMIENTO

La teoría de los vicios del consentimiento está compuesta por:

1.- El error.

2.- El dolo.

3.- La violencia.

En esta investigación la autora se limitará a comentar solo el referido al error por considerar que es el que posee mayor relevancia para cumplir con los objetivos propuestos en el presente estudio.

El error como lo afirma Maduro “consiste en una falsa apreciación de la realidad, en creer falso lo verdadero y verdadero lo falso”.

Los efectos del error son:

1.- Nulidad del contrato.

2.- Indemnización de daños y perjuicios, pero para que pueda producir estos efectos debe tratarse de un error esencial, entendido este como aquel que es de tal magnitud que si la parte lo hubiese conocido o se hubiera percatado de la falsa apreciación en que incurría, no hubiese contratado.

El Código Civil Venezolano distingue dos tipos de error, a saber: el error de hecho y el error de derecho.

El error de derecho, es aquel que recae sobre la existencia, la circunstancia, los efectos y consecuencias de una norma jurídica; mientras que el error de hecho por su parte se clasifica en error en substancia que se refiere a las cualidades de una cosa y el error en la persona que recae sobre la identidad o cualidades de la persona en quien se ha contratado.

El error en la persona se encuentra establecido en el Artículo 1.148 del Código Civil en su párrafo segundo que dice:

> "...es también causa de anulabilidad el error sobre la identidad o las cualidades de la persona con quien se ha contratado, cuando esa identidad o las cualidades han sido la causa única principal del contrato".

La doctrina está de acuerdo, en que el error en la persona es relevante y producirá sus efectos (anulabilidad del contrato) sólo en los casos en que esa identidad o esas cualidades de la persona hayan sido la causa única o principal del contrato, es decir, sólo en ese caso el error en la persona será

considerado esencial, lo cual afectará la validez del contrato por estar presente en él, un vicio del consentimiento.

En el comercio electrónico, sin embargo, por tratarse de transacciones donde la presencia física no es necesaria, se hace aún más importante el establecer la identidad de las partes tanto para evitar los vicios del consentimiento; como para poder determinar las responsabilidades ante la participación de una persona en una transacción determinada, en caso de un eventual litigio.

2.1.4. - SEGURIDAD JURÍDICA

El derecho como lo afirma Recasens (1959), nace para "colmar una ineludible urgencia de seguridad y de certeza en la vida social". (p.220).

El hombre para vivir socialmente necesita saber cuales son sus deberes y derechos para con los demás integrantes de la sociedad, y precisa saber que sus derechos serán respetados, es decir, necesita la certeza de que esto ocurrirá, que las reglas se cumplirán forzosamente, que sus derechos serán defendidos de un modo eficaz.

> El derecho surge precisamente como instancia determinadora de aquello a lo cual el hombre tiene que atenerse en sus relaciones con los demás –certeza-; pero no sólo certeza teorética (saber lo que se debe hacer); sino también certeza práctica, es decir, seguridad; saber que esto tendrá forzosamente que ocurrir, porque será impuesto por la fuerza, si es preciso, inexorablemente. (Recasens, 1959,p.221)

Como puede observarse la seguridad jurídica debe verse desde una doble perspectiva la de la certeza teórica –que implica el conocimiento de la norma- y el de la certeza práctica- que implica que la norma será cumplida.

Merino, citado por Saquel (2001) distingue entre Certeza y Seguridad Jurídica y dice:

> Por certeza entendemos el conocimiento claro y seguro en orden a que los presupuestos o elementos estructurales de una relación jurídica se ajustan al sistema legal vigente, creemos en cambio que la seguridad jurídica consiste en la efectiva protección de la ley o los titulares de una relación jurídica de tal forma que el sujeto activo se encuentra garantizado en el ejercicio pacifico y en la eficacia de su derecho y el sujeto pasivo protegido en cuanto al real alcance y permanencia del deber que esa misma relación le impone.

La seguridad jurídica es el derecho de todos los ciudadanos, a gozar de la efectiva procuración e impartición de justicia a cargo de las autoridades.

Saquel (2001) por su parte la define como:

> La situación peculiar del individuo como sujeto activo y pasivo de las relaciones sociales, cuando estas relaciones se hallan previstas por un estatuto objetivo; conocido y generalmente observado. Es la seguridad de quien conoce o puede conocer lo previsto como prohibido, mandado y permitido por el poder público respecto de uno para con los demás y de los demás para con uno.

La seguridad jurídica entonces no sólo consiste en garantizar la libertad para contratar, el cumplimiento del contrato o el valor probatorio de la firma digital en los contratos electrónicos, sino que debe dar esa certeza práctica,

es decir, que todas las personas confíen en que sus derechos son protegibles y exigibles.

De manera que no es suficiente establecer en la Ley de Datos y Firmas Electrónicas el valor probatorio del documento electrónico, ni la validez de la firma electrónica, es necesario que las personas confíen en la norma, que tengan fe en dichas normas, que tengan la convicción de que esas normas efectivamente garantizaran sus derechos.

Ramos (1999) considera que los factores fundamentales de la seguridad jurídica en la red son:

1. - La Confidencialidad /privacidad: Debe asegurarse que el contenido del mensaje de datos no sea leído por persona no autorizada.

2. - Integridad: Que el mensaje no sea alterado, durante su recorrido por la red, o que los datos sean cambiados para cumplir los fines ilícitos de una de las partes.

3. - La autenticidad: Asegurar la identidad del remitente o signatario.

4. - El no repudio: Implica la autenticación y la integridad; hace referencia tanto al no rechazo en origen (que el signatario, no pueda negar un mensaje con un determinado contenido) como al rechazo en destino (que el destinatario no pueda negar la recepción de un mensaje con un determinado contenido).

Son precisamente estos factores los que hay que proteger para lograr una seguridad jurídica efectiva.

2.1.5.- FIRMA OLÓGRAFA

El Diccionario de la Real Academia Española (1992) define la firma como:

> Nombre y apellido o título de una persona que está pone con rúbrica al pie del documento escrito de mano propia o ajena para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en el se dice.

La Enciclopedia Jurídica OPUS (1994) al hablar de la firma dice que la firma acredita la comparecencia de la persona y la conformidad con los hechos y declaraciones que suscribe salvo haber sido obtenida por sorpresa, engaño o violencia; y es por esta misma razón que es exigida a las partes o a sus representantes en la totalidad de los negocios jurídicos escritos: contratos, testamentos, actas y demás documentos públicos o privados que deban tener alguna eficacia. De carecer de la firma los escritos se consideran simples borradores o proyectos.

Aunque en el Código Civil venezolano no existe una definición de firma se interpreta que al referirse a la firma se hace referencia a la ológrafa, ya que si se lee el único aparte del artículo 1.368 ejusdem este dispone que si el otorgante (del documento Privado) “...no supiere o no pudiere firmar, ...”, el instrumento deberá estar suscrito por persona mayor de edad que firma a ruego de aquél, y además, por dos testigos.

Igualmente el artículo 1.375 ejusdem al hablar del telegrama establece que:

> "...hace fe como instrumento privado, cuando el original lleva la firma de la persona designada en el como remitente, o cuando se prueba que el original se ha entregado o hecho entregar en la Oficina Telegráfica en nombre de la misma persona, aunque ésta no lo haya firmado, siempre que la escritura sea autógrafa."

En lo que se refiere a las Características de la firma Cuervo (1999) señala las siguientes:

Identificatíva: Sirve para identificar quien es el autor del documento

Declarativa: Significa la asunción del contenido del documento por el autor de la firma. Sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.

Probatoria: Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.

2.1.6. - FIRMA ELECTRÓNICA

Para lograr la seguridad jurídica en la red se ha creado lo que se conoce como Firma Electrónica.

Para Molina (1999) está "se podría entender como el método, signo o símbolo de naturaleza electrónica incorporado por su titular a un documento preparado para ser tratado por medio telemáticos, con cualquiera de las

finalidades previstas para la firma manuscrita ” (p.421)

Cuervo (1999), por su parte define la firma electrónica como “Cualquier método o símbolo utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones de la firma manuscrita” (p.242)

Las características de la firma electrónica son:

- Debe permitir la autenticación del signatario
- No puede ser generada más que por el emisor del documento, infalsificable e inimitable.
- Las informaciones que se generen a partir de la signatura electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla.
- La posible intervención del notario electrónico mejora la seguridad del sistema.
- La aposición de una signatura debe ser significativa y va unida indisociablemente al documento a que se refiere.
- No debe existir dilación de tiempo ni de lugar entre aceptación por el signatario y la oposición de la signatura. (Cuervo, 1999).

Por su parte el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas dictado el 10 de febrero del 2001 y publicado en la Gaceta Oficial número 37.148 de fecha 28 de febrero del 2001; define en el Art.2 la

Firma Electrónica como: “Información creada o utilizada por el signatario, asociada al mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado”.

Como puede observarse estas definiciones de firma electrónica son bastante amplias de manera que pueden incluirse en ellas infinidad de métodos entre los cuales se encuentran la firma digital, basada en métodos criptográficos (asimétricos) y la firma biométrica entre otras; porque lo importante es que cumplan con la finalidad propuesta que en el caso de la firma electrónica es la de proporcionar certeza sobre la identidad del autor, garantizar la integridad sobre el contenido del documento al que se asocia, que su titular posea el control exclusivo de la misma, la garantía del “no rechazo” por su autor y destinatario, y la confidencialidad. (Molina,1999)

2.1.7. - FIRMA DIGITAL

La firma digital consiste en un método basado en sistemas criptográficos asimétricos para de esta manera cumplir con su finalidad, que es la de garantizar la confidencialidad, integridad, autenticidad y no repudio elementos indispensables en la seguridad jurídica en la red.

El procedimiento consiste en extraer un “resumen” (hash) del mensaje, cifrar este resumen con la clave privada del remitente y añadir el resumen cifrado al final del mensaje; luego el mensaje más la firma, lo que constituiría 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 con la propiedad de que cualquier modificación del mensaje original, por pequeña que sea, dé lugar a un resumen diferente.

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.

Por otro lado 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), y el remitente no podría negar haberlo enviado (no repudio) ya que sólo él conoce su clave secreta.

2.1.8. - AUTORIDADES DE CERTIFICACIÓN

"Son aquellas entidades que merecen la confianza de otros actores en un escenario de seguridad donde no existe confianza directa entre las

partes involucradas en una cierta transacción". (Carrión, 2002)

El Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas prevé la figura de los proveedores de Servicios de Certificación y todo lo relativo a los certificados electrónicos. (artículos 31 al 44)

2.1.9. - PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

El Decreto-Ley prevé la figura de los Proveedores de Servicios de Certificación y en su artículo 2 los define como:

"Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley".

Los Proveedores de Servicios de Certificación son los sujetos que siguiendo el procedimiento legalmente establecido, obtengan de la Superintendencia de Servicios de Certificación Electrónica una autorización que le permita garantizar a los usuarios la autoría de un mensaje de datos, a través de la certificación de la integridad del mensaje.

Es muy importante señalar que los requisitos para ser Proveedores de Servicios de Certificación están establecidos en el artículo 31 del Decreto-Ley y son los siguientes:

> 1. - La capacidad económica y financiera suficiente para prestar los servicios autorizados como Proveedor de Servicios de Certificación. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gasto y de ingresos que permitan el desarrollo de esta actividad.

2. - La capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos.

3. - Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los Certificados Electrónicos que proporcione.

4. - Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

5. - Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación.

6. - En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen.

7. - Personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar.

8. - Las demás que señale el reglamento de este Decreto-Ley

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones previstas en este Decreto-Ley.

Asimismo, las actividades de los Proveedores de Servicios se encuentran establecidos en el artículo 34 del Decreto-Ley y son:

1. - Proporcionar, revocar o suspender los distintos tipos o clases de Certificados Electrónicos.

2. - Ofrecer o facilitar los servicios de creación de Firmas Electrónicas.

3. - Ofrecer servicios de archivos cronológicos de las Firmas Electrónicas certificadas por el Proveedor de Servicios de Certificación.

4. - Ofrecer los Servicios de archivo y conservación de mensajes de datos.

5. - Garantizar Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros.

6. - Las demás que se establezcan en el presente Decreto-

> Ley o en sus reglamentos.
>
> Los Certificados Electrónicos proporcionados por los Proveedores de Servicios de Certificación garantizarán la validez de las Firmas Electrónicas que certifiquen, y la titularidad que sobre ellas tengan sus Signatarios.

Igualmente las obligaciones de los Proveedores de Servicios de Certificación se encuentran establecidas en el artículo 35 ejusdem:

> 1. - Adoptar medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario.
> 2. - Garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione.
> 3. - Verificar la información suministrada por el Signatario para la emisión del Certificado Electrónico.
> 4. - Mantener en medios electrónicos o magnéticos, para su consulta, por diez (10) años siguientes al vencimiento de los Certificados Electrónicos que proporcionen, un archivo cronológico con la información relacionada con los referidos Certificados Electrónicos.
> 5. - Garantizar a los Signatarios un medio para notificar el uso indebido de sus Firmas Electrónicas.
> 6. - Informar a los interesados en sus servicios de Certificación, utilizando un lenguaje comprensible en su página en la Internet o en cualquier otra red mundial de acceso público, los términos precisos y condiciones para el uso del Certificado Electrónico y en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.
> 7. - Garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo confiable y seguro de dicha información.
> 8. - Garantizar la adopción de las medidas necesarias para evitar la falsificación de Certificados Electrónicos y de las Firmas Electrónicas que proporcionen.
> 9. - Efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los Certificados Electrónicos que proporcionen, así como de

> cualquier otro aspecto de relevancia para el público en general, en relación con dichos Certificados Electrónicos
>
> 10. - Notificar a la Superintendencia de Servicios de Certificación Electrónica cuando tenga conocimiento de cualquier hecho que pueda conllevar a su inhabilitación Técnica.
>
> El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la suspensión de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones establecidas en el presente Decreto-Ley.

La ley establece que se crea la figura de los proveedores de certificados electrónicos con el objeto de otorgar mayor seguridad en las comunicaciones y el comercio electrónico.

2.1.10. - CERTIFICADOS ELECTRÓNICOS

Por otro lado el Capitulo VII del Decreto-Ley se refiere a los Certificados Electrónicos y dice textualmente:

> Artículo 38. - El Certificado Electrónico garantiza la auditoria de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. El Certificado Electrónico no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.

La vigencia de este Certificado Electrónico será determinada por el Signatario y el Proveedor de mutuo acuerdo (artículo 39).

Asimismo el artículo 43 ejusdem establece que los Certificados Electrónicos deberán contener:

1. - Identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica.
2. - El código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica.
3. - Identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica.
4. - Las fechas de inicio y vencimiento del período de vigencia del Certificado electrónico
5. - La Firma Electrónica del Signatario.
6. - Un serial único de identificación del Certificado Electrónico.
7. - Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que este sometido el Certificado Electrónico.

2.2.- BASES TÉCNICAS

2.2.1. - COMERCIO ELECTRONICO

Internet por ser una red abierta permite la interacción de millones de personas en el ámbito mundial, en ella se consigue cualquier cantidad de productos, de cosas hasta inimaginables y todo está al alcance de la mano, porque no importa que tan lejos se encuentre una empresa, si está en línea se podrá comprar o vender desde la comodidad de su casa u oficina.

Los comerciantes han visto en la red la posibilidad de ofrecer sus productos a un número potencialmente ilimitado de clientes; además ésta brinda a las empresas beneficios adicionales como: Reducción de costos; acceso a nuevos mercados y por ende maximización de ingresos, ya que el establecimiento virtual está disponible 24 horas diarias y llega a un mayor

número de personas así como también facilita la igualdad de competencia entre pequeñas y grandes empresas.

Esto ha hecho que el comercio, como se conoce tradicionalmente avance y de paso a lo que se conoce como Comercio Electrónico entendido este como:

> Cualquier forma de transacción comercial o intercambio de información utilizando nuevas tecnologías de comunicación entre empresas, empresas y sus consumidores, y entre empresas y la administración pública así como los mecanismos de pago telemáticos, dinero digital, métodos de seguridad en el comercio on-line y operaciones bancarias cibernéticas (Paz, 1998,p.11).

El Comercio Electrónico abarca toda forma de transacción comercial, tanto organizacional como individual, que está basada en el procesamiento y transmisión electrónica de información (data), incluyendo texto, sonido e imágenes visuales. También se refiere a los efectos que el intercambio electrónico de información comercial puede tener en las instituciones y procesos que permiten y prácticamente gobiernan las actividades comerciales. Esto incluye el manejo o gerencia organizacional empresarial, las negociaciones comerciales y contratos, aspectos legales y regulatorios, adopción de acuerdos financieros y política fiscal entre otras.

La autora considera que una de las razones del auge de la Internet se debe precisamente a que es una red abierta donde no es necesario el contacto físico entre las partes intervinientes, que en efecto permite que las

personas o empresas, aún sin conocerse previamente puedan interrelacionarse, pero es este mismo hecho el que hace necesario que se creen sistemas de seguridad para garantizar los derechos de las partes involucradas en las diferentes transacciones, ya que al igual que en el mundo físico pueden suscitarse conflictos que pueden agravarse por el hecho de no conocer a la otra parte, o por no tener la seguridad de quien es esa otra persona con la cual estamos contratando provocando de esta manera una inseguridad jurídica que es necesario resolver.

2.2.2. - CRIPTOGRAFÍA

La firma electrónica basada en métodos criptográficos se presenta como la más conocida y por consiguiente la más utilizada hasta los momentos.

La Criptografía, del griego kripto (oculto) y graphein (escribir), es definida por la Real Academia Española (1992) como: “El arte de escribir con clave secreta o de modo enigmático” (p.421).

Esta ha evolucionado desde las antiguas técnicas de transposiciones y sustituciones de símbolos ya utilizadas en la antigua civilización griega y romana a los métodos basados en algoritmos matemáticos de claves simétricas; –el cual está basado en claves privadas donde tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave tanto para cifrar como para descifrar el mensaje-; y la de claves asimétricas; la cual

fue inventada en 1976 por los matemáticos Whit Diffie y Martín Hellman, donde se utilizan dos claves; una privada -con la cual se cifra el mensaje - y una pública -con la cual se descifra mensaje-.

Como puede observarse un sistema criptográfico define dos procesos de transformación. En el primero, denominado proceso de cifrado, se le aplica al texto o información original una función que hace que el contenido del mensaje sea ininteligible para quienes no son los destinatarios del mismo. Mientras que en el segundo proceso, llamado proceso de descifrado, el destinatario le aplica al mensaje cifrado la función reciproca que recupera el contenido original.

El Sistema de criptografía asimétrica o de clave pública es el que ha resultado más beneficioso para garantizar la seguridad jurídica de las transacciones realizadas a través de Internet, en este método se utilizan parejas de claves con la propiedad de que lo que se cifra con una de las claves sólo se pude descifrar con la otra clave de la pareja. De manera que cada Interlocutor hace pública una de sus claves (será su clave pública) y mantiene en secreto la otra (su clave privada). La clave privada puede guardarse en el ordenador del usuario o en una tarjeta inteligente.

Por la propiedad de las parejas de claves antes citadas, 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. 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 cual es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación.

2.2.3.- MODELO DE MAIO Y MALTONI

A continuación se describirá el sistema de firma biométrica propuesto por Maio y Maltoni (1.999)

Este es uno de los primeros intentos concretos para llevar a Internet la autenticación por medio biométricos.

Este ha sido denominado por sus autores como “A SECURE PROTOCOL FOR ELECTRONIC COMMERCE BASED ON FINGERPRINTS AND ENCRYPTION” (Protocolo Seguro para Comercio Electrónico basado en Huellas Dactilares Y Criptografía); el mismo utiliza tecnología biométrica pero se apoya en el modelo de confianza en las Autoridades de Certificación; funciona de la siguiente manera:

Existen 3 partes:

1. - El Cliente

2. - El Vendedor

3. - El Certificador; quien debe asegurarse de la veracidad de las intenciones expresadas por el cliente y el vendedor con el objetivo de mantener estrictamente confidencial los modelos e imágenes de huellas dactilares.

En este modelo (véase el Cuadro N° 1) los terminales que permiten llevar a cabo el comercio electrónico están equipados con un escáner de huella dactilar en-línea (modulo del cliente). Cada cliente tiene una tarjeta donde su modelo de huella dactilar es almacenada en forma cifrada.

Cada vendedor que pueda llevar a cabo el comercio electrónico tiene un par de claves una privada y una pública y un computador personal corriendo el software administrador de la transacción (modulo vendedor).

El certificador por su parte también tiene un par de claves (públicas y privadas). En el sitio del certificador un servidor corre el software del administrador de la transacción (modulo certificador), el cual es responsable de validar todas las transacciones, además, el servidor del certificador está equipado con un escáner de huella dactilar en línea y un escritor de tarjetas, el cual, es necesario para almacenar los modelos en las tarjetas durante el registro del usuario.

Cada cliente que pueda realizar el comercio electrónico debe ser inicialmente sometido a una sesión de registro donde su modelo de huella

dactilar es creado, digitalmente firmado por el certificador y almacenado en una tarjeta para él.

La firma digital del certificador en el modelo de huella dactilar es necesaria para prevenir que usuarios fraudulentos intenten crear un nuevo modelo válido usando sus propios dedos, y el cifrado dado por la clave pública del certificador garantiza que sólo el certificador pueda descifrar el modelo de huella dactilar del cliente.

Por lo tanto, el modelo de huella dactilar no es guardado en una base de datos central, pero éstos son distribuidos a los clientes.

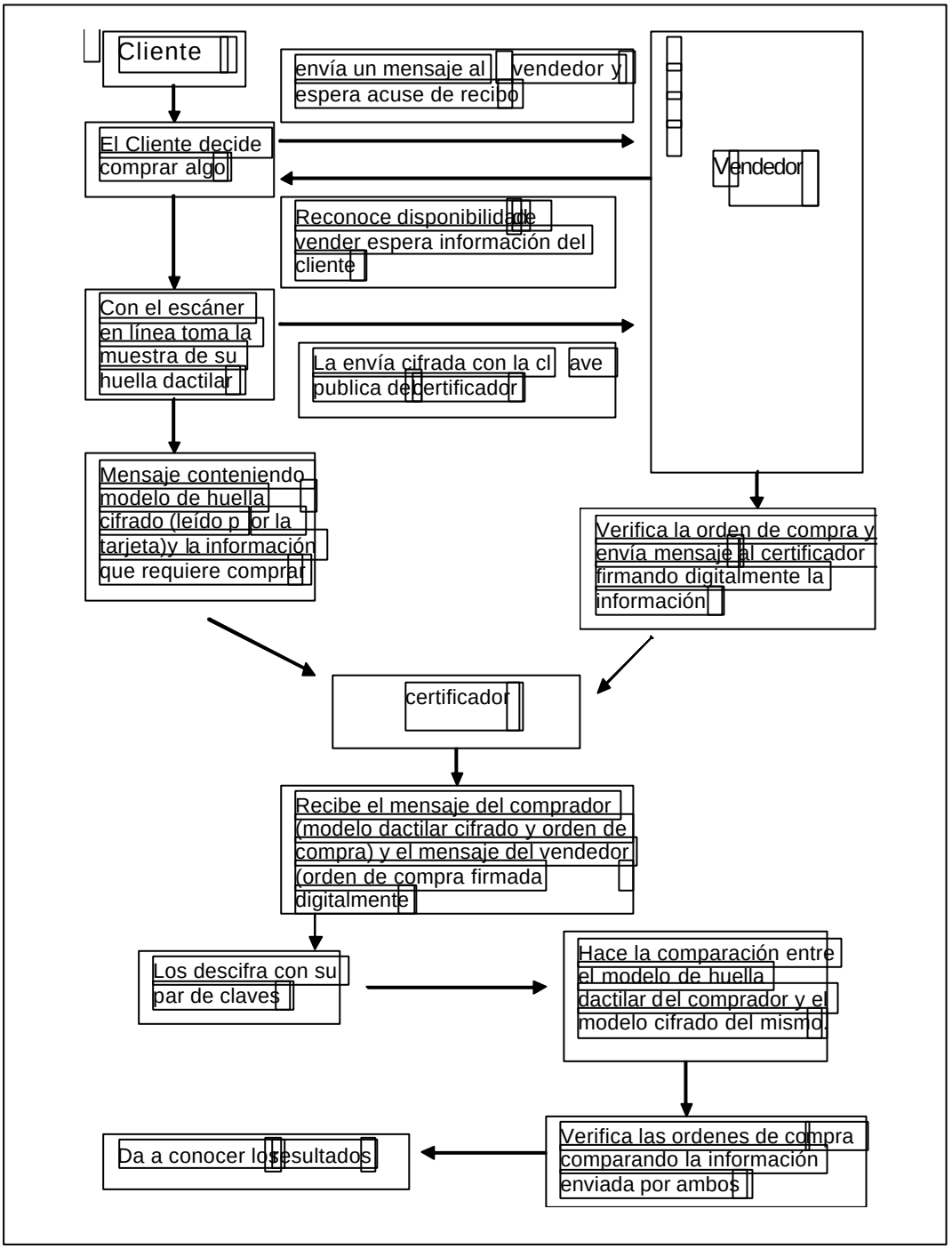
El cifrado aplicado al modelo de huella dactilar protege la información para que no pueda ser descifrada por nadie (ni siquiera por el portador) excepto el certificador haciendo de esta manera la tarjeta inservible en caso de perdida o robo.

Por su parte cada vendedor que pueda realizar el comercio electrónico debe ser inicialmente registrado por el certificador quien le asignará un par de claves (pública y privada).

Los pasos para una transacción electrónica siguiendo el modelo Maio/Maltoni serían:

CUADRO N° 1

MODELO DE MAIO Y MALTONI



Fuente: García (2002)

2.3. – BASES BIOLÓGICAS

2.3.1. – PRINCIPIO DE LA HERENCIA POLIGÉNICA

Las características físicas de los individuos están determinadas por los genes y algunos rasgos por la interacción de estos genes con el medio ambiente.

A diferencia de las plantas el cuerpo humano esta compuesto por 23 pares de cromosomas que son los encargados de definir la información genética de cada individuo, lo que significa que determinadas características están controladas por dos o más genes distintos y esto es lo que se conoce como Rasgos Poligénicos.

Desde el momento de la concepción cada organismo es influido por el medio ambiente y la expresión de cualquier gen es siempre el resultado de la interacción del gen y del ambiente.

El genotipo representa la constitución genética de un individuo; este queda fijado en el momento de la fecundación y, salvo que ocurra una mutación, es inmodificable. El fenotipo es invariable y esta sujeto a cambios continuos durante toda la vida del organismo.

El ambiente que rodea a un gen esta formado por factores genéticos incluidos todos bs demás genes del genotipo, sus efectos e interacciones, y por todos los factores no genéticos, sean físicos o sociales, que tienen la

capacidad de reaccionar mutuamente con el genotipo. En un momento determinado de la vida, un organismo representa la suma de todas las interacciones entre los genes y el ambiente que se han producido desde la fecundación.

Las huellas dactilares son rasgos que están controlados por una multiplicidad de genes por lo cual constituyen un ejemplo de Herencia Poligénica.

Los dibujos de las huellas dactilares fueron estudiados sistemáticamente por primera vez en el siglo XIX, cuando el fisiólogo Purkinje separó nueve clases de dibujos básicos, parecidos al sistema que se emplea hoy. Mas tarde, Francis Galton admitió que las huellas dactilares eran hereditarias e inmutables durante toda la vida, convirtiéndose así en valiosos marcadores genéticos.

> Las huellas dactilares quedan establecidas en los tres primeros meses del desarrollo embrionario y son el resultado de factores genéticos y ambientales. Esto significa que todo el mundo, incluidos los gemelos idénticos, tiene un solo grupo de huellas dactilares. Aunque los gemelos idénticos tengan el mismo grupo de genes y hayan estado dentro del mismo útero, cada uno de ellos ha estado sometido a ambientes ligeramente distintos. Estos factores ambientales distintos son los responsables de la aparición de dibujos dactilares diferentes (Cummings, 1995,p.449).

Las huellas dactilares están formadas por crestas de la piel llamadas crestas cutáneas. Durante el desarrollo embrionario, estas crestas forman grupos de asas, espirales y arcos. Esos mismos dibujos se forman con las

crestas de las palmas de las manos, las plantas y los dedos de los pies.

Las huellas dactilares se dividen en asas, espirales y arcos y se clasifican por el numero de crestas de los 10 dedos de las manos. Las huellas dactilares se miden fácilmente y con objetividad y una vez determinadas ya no sufre influencias sociales, ni ambientales.

Las huellas dactilares constituyen los rasgos métricos mayormente utilizados en la identificación de personas porque las huellas dactilares son perennes, inmutables y diversiformes, es decir, después que se forman en plantas de manos y pies, durante los primeros meses de vida uterina permanecen invariables durante la existencia y solo se borran hasta la completa desintegración de la piel producida por la muerte.

2.3.2. - BIOMETRÍA

La palabra biometría deriva de las voces griegas “Bio” que significa “vida” y metría que significa “medida” o “medición”.

La Real Academia Española (1992) define la biometría como “el estudio mensurativo o estadístico de los fenómenos y procesos biológicos” (p.207).

Por su parte Lapedes (1981) la define como el “uso de las estadísticas para analizar observaciones de fenómenos biológicos”. (p.245)

Morales y Ruiz (2000) definen la biometría como “la ciencia que se dedica

a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento".

Las características anatómicas son aquellos aspectos que son relativamente estables durante el transcurso de la vida de un individuo tales como son las huellas digitales, o el patrón del iris; mientras que los rasgos del comportamiento son menos estables, debido a que dependen de la disposición psicológica de la persona, como por ejemplo la firma.

La verificación biométrica por medio de características físicas comenzó a finales del siglo XIX cuando Alphonse Bertillon, demostró que nadie tiene las mismas huellas dactilares en 1880, pero al igual que las huellas dactilares existen otras partes del cuerpo que son igualmente mensurables, tales como cara, manos, retina, y voz.

Con el avance de la informática todas estas características están siendo estudiadas para ser adaptadas a las nuevas tecnologías, es decir, se están estudiando para ser utilizadas en sistemas biométricos, de manera que las tareas que antes se hacían manualmente ahora se podrán realizar de forma automatizada para de esta manera garantizar una mayor seguridad en la identificación de las personas.

2.3.3. -SISTEMAS BIOMÉTRICOS

Los sistemas biométricos "son métodos automatizados de verificación

o reconocimiento de la identidad de una persona basada en su fisiología o las características de su comportamiento". (Biométrica, 2000)

Para que una característica anatómica pueda ser utilizada con éxito por un sistema biométrico debe ser:

Universal: cualquier persona posee esa característica.

Única: la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña.

Permanente: la característica no cambia en el tiempo.

Cuantificable: la característica puede ser medida en forma cuantitativa. (Morales y Ruiz, 2000)

Por otra parte todo sistema biométrico debe tomar en cuenta:

1. - El desempeño; que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonables.

2. - Aceptabilidad: que indica el grado de disposición de la gente a aceptar un sistema biométrico en su vida diaria, ya que el sistema no debe representar peligro alguno para los usuarios y debe inspirar confianza en los mismos.

3. - Fiabilidad, que refleja cuan difícil es burlar al sistema. El sistema

biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz, prótesis de ojos, etc. Algunos sistemas incorporan métodos para determinar si las características bajo estudio corresponden o no a la de una persona viva. Los métodos empleados son ingeniosos y usualmente más simples de los que se puede imaginar. Por ejemplo, un infrarrojo para chequear las venas de las manos detecta flujos de sangre caliente y lectores de ultrasonido para huellas dactilares revisan estructuras subcutáneas de los dedos. (Morales y Ruiz, 2000).

2.3.4.- SISTEMAS MODERNOS DE BIOMETRÍA

Los sistemas modernos de biometría por computadora se emplean para dos funciones básicas:

1. – Identificación; en está función se descubre a un individuo mediante una búsqueda exhaustiva en la base de datos; lo que requiere una comparación del tipo uno a muchos para establecer la identidad del individuo. El sistema debe responder a la pregunta: ¿Quién eres tú?

2. – Verificación; este sistema comprueba la identidad de algún individuo comparando la característica sólo con los templates del individuo; esto requiere una comparación uno a uno para determinar si la identidad reclamada por el individuo es verdadera o no. El sistema debe responder a la pregunta ¿Eres tú quien dice ser?

Todos estos sistemas trabajan básicamente de la misma manera; se componen de un hardware y un software, el primero captura la característica concreta del individuo y el segundo interpreta la información y determina su aceptabilidad o rechazo, todo en función de los datos que han sido almacenados por medio de un registro inicial de las características biométricas que mida el dispositivo en cuestión. Este registro inicial o toma de muestra es lo que determina la eficacia del sistema.

En el caso de las huellas dactilares, un usuario coloca el dedo en un sensor que hace la lectura digital en su huella, después, el programa guardará la información como un modelo; la próxima vez que ese usuario intente acceder al sistema deberá repetir la operación y el software verificará que los datos corresponden con el modelo.

El mismo principio rige para la identificación por el iris / retina, con ayuda de videocámara, el rostro, la mano completa, etc. Las tasas de exactitud en la verificación dependen en gran medida de dos factores; el cambio que se puede producir en las personas, debido a accidentes o a envejecimiento, y las condiciones ambientales, como humedad en el aire, suciedad y sudor en especial en la lectura que implique el uso de las manos.

2.3.5.- INDICADORES BIOMÉTRICOS

Los indicadores biométricos más utilizados son:

1. - Escáner del ojo.

Los ojos no son comúnmente utilizados para identificar personas, sin embargo, la identificación de personas a través de los ojos es considerada más prometedora que la huella dactilar ya que el iris posee 266 características, mientras que la huella dactilar solo posee 40. (Britannica, 2000)

Son dos las principales tendencias en la identificación del individuo utilizando el ojo.

a.- Escaneo de la retina: la retina es la parte de atrás del ojo que reacciona a la luz y ayuda a interpretarla antes de que el cerebro la reciba. Cada retina tiene un patrón único para cada ser humano, incluyendo los gemelos idénticos. La retina es una característica física que esta determinada por factores genéticos y por esto desarrolla algunos patrones al azar. La retina sólo puede ser destruida por serias heridas. (Britannica, 2000).

El sistema de escaneo de la retina consiste en iluminar al ojo utilizando un haz de luz de baja intensidad a través de la pupila, y analizar los patrones de los vasos de sangre detrás de la retina. El patrón es reflejado hacia la cámara la cual lo captura, codifica y analiza. Aunque la variación de los vasos de sangre no es tan grande y esta puede cambiar durante la vida de la persona, cada patrón es unívoco. (López, 1999).

El problema con este sistema es que las personas se sienten incomodas al tener una cámara examinando las venas en sus ojos (Britannica, 2000), es decir, el reconocimiento de una retina requiere un contacto cercano de la persona con el dispositivo de reconocimiento, lo que puede desconcertar a ciertos individuos debido al hecho de tener su ojo sin protección frente a un "aparato".

b.- Reconocimiento del iris; este tipo de biometría es considerada la más prometedora. El iris es la parte coloreada del ojo y esta conformado por fibras, surcos y pecas, sus patrones son creados mediante la interconexión de tejidos. Cada ser humano posee un iris diferente ya que éste está conformado por 266 características. (Britannica, 2000).

El sistema de reconocimiento de iris puede tomar el color y ciertas características unívocas del iris desde una distancia relativamente cómoda para el usuario, sin tener que proyectar un haz de luz directamente al ojo. Esto se puede hacer ya que los patrones de iris se encuentran en la superficie del ojo y no en su parte interna (López, 1999).

La cámara toma la imagen del ojo, y excluye todo tipo de obstrucción tales como párpados, lentes e incluso lentes de contacto. (Britannica, 2000).

Como es de suponer el iris es uno de los elementos que mejor identifican cada ser humano; la probabilidad de conseguir dos iris con las mismas características es:

1,000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000, menores que de conseguir dos huellas digitales (López, 1999).

2. - Escáner de Rasgos Faciales:

El rostro fue el punto de referencia de Alphonse Bertillon. Bertillon fue capaz de identificar a las personas por facciones que raramente cambian como por ejemplo la forma de las orejas, independientemente de la barba o los diferentes cortes de pelo. Bertillon sin embargo tuvo problema diferenciando entre gemelos idénticos y personas que se parecían, por lo que este sistema fue reemplazado por la clasificación de huellas dactilares de Richard Edward Henry.

El rostro puede cambiar con el tiempo o por heridas lo que es un problema; algunas personas creen que la geometría de la cara puede ser burlada por fotos, sin embargo esto no es verdad. Algunas veces dos cámaras son usadas en dos ángulos diferentes lo que permite al sistema detectar estas fotos. (Britannica, 2000).

La verificación y reconocimiento facial es una de las áreas de mayor interés en la biometría; este reconocimiento involucra más que simplemente examinar el rostro contra una foto en la base de datos.

Una técnica mide rasgos faciales y desarrolla correlaciones estadísticas; como por ejemplo el medir la anchura de su boca y la distancia entre sus

ojos. Existen también técnicas que emplean las redes neurales para recibir los rasgos de los ojos, de la nariz, el pelo y analizarlos todos dentro de un mismo texto.

Este sistema funciona analizando la imagen en video o en una fotografía e identificando las posiciones de varias decenas de nodos en el rostro de una persona. Estos nodos, en su mayoría entre la frente y el labio superior, no se ven afectados por la expresión o la presencia de vello facial.

Estos sistemas pueden ser capaces de considerar el envejecimiento, condiciones psicológicas de la persona, y otros factores como lo son los lentes, maquillaje barba y producir resultados favorables (López, 1999).

3. - Escáner de la voz.

La identificación de personas a través de la voz, es utilizada a diario, por ejemplo algunas veces se reconoce a las personas basados en sus voces cuando se contesta el teléfono.

El reconocimiento de voz es considerado el menos invasivo, lo cual lo hace popular.

Los sistemas de reconocimiento de voz funcionan analizando las características vocales fundamentales del individuo.

Estos sistemas registran el discurso y analizan el tono y las inflexiones del

hablante.

Los sistemas basados en el reconocimiento de voz presentan algunos problemas ya que la voz cambia con el ánimo de las personas y algunas enfermedades como la gripe o la congestión nasal, además los ruidos exteriores, pueden causar algunos problemas. Sin embargo, nuevas tecnologías están evadiendo este problema y están siendo más exactos, pero a pesar de que estos sistemas son más exactos la verificación por reconocimiento de voz esta siendo usada conjuntamente con otras formas de reconocimiento biométrico como por ejemplo el rostro o la huella digital. (Britannica, 2000).

4. - Reconocimiento a través de la geometría de la mano.

La geometría de la mano nunca ha sido utilizada como rasgo para identificar personas. La geometría de la mano es ampliamente aceptada por el público por considerarse poco invasiva; sin embargo solo puede ser usada para la verificación y no para la identificación, porque no se ha determinado si las manos son únicas para cada ser humano. (Britannica, 2000).

Esta tecnología consiste en digitalizar la forma, el tamaño y otras características (como la longitud de los dedos) de parte o de la totalidad de la mano.

Este tipo de reconocimiento suele usarse asociado a otro tipo de

identificación como por ejemplo una tarjeta.

5. - La huella dactilar

La huella dactilar es una de las características anatómicas ampliamente aceptada como indicador biométrico, esta ha sido utilizada por los seres humanos para la identificación de personas por más de cien años.

Las huellas dactilares tienen 40 características. Cada ser humano tiene un tipo de huella dactilar único que además no cambia durante toda la vida del individuo, por lo cual son consideradas pruebas legitimas de evidencia criminal en cualquier corte del mundo.

> Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen en forma paralela (colinas, ridges, lines y furrows). Sin embargo, estas líneas se interceptan y a veces terminan en forma abrupta. Los puntos donde estas terminan o se bifurcan se conocen técnicamente como minucias. (Morales y Ruiz, 2000).

Las huellas dactilares están formadas por crestas de la piel, llamadas crestas cutáneas que formas grupos de **asas**;- cuando las líneas comienzan de un lado del dedo, llegan hasta un tope aproximadamente en el centro de la yema del dedo y regresan hacia el mismo lado.-, **espirales**; - cuando las líneas forman círculos aproximadamente concéntricos al centro de la yema-, y **arcos**; -cuando las líneas comienzan al costado del dedo, y llegan al centro de la yema pero ahora siguen hacia el otro lado del dedo, formando

precisamente un arco que pasa por la zona central de la yema -., Son precisamente estas características las que se toman en cuenta los sistemas biométricos para hacer la identificación o verificación.

Otros puntos singulares de una huella dactilar son aquellos donde la curvatura de los ridges es máxima. Estos puntos reciben el nombre de cores y deltas.

Las características más interesantes que presentan tanto las minucias como los puntos singulares cores y deltas es que son “únicos” para cada individuo y permanecen inalterados a través de su vida. A pesar de esta variedad de minucias (18 tipos distintos de minucias han sido enumerados) las más importantes son las terminaciones y bifurcaciones de ridges.

Para poder identificar a una persona mediante las minucias de su huella es necesario poder representar estas ultimas para poder compararlas. La representación estándar consiste en asignar a cada minucia su posición espacial (x, y) y su dirección q, que es tomada con respecto al eje x en el sentido contrario a los punteros del reloj.

Para reconocer una huella dactilar se procede desde una escala gruesa a una fina. En primer lugar, se clasifica a la huella, es decir, se asigna a una clase previamente determinada de acuerdo a la estructura global de los ridges. El objetivo de esta etapa es establecer una partición en la base de datos con huellas. En general la distribución de las huellas en las distintas

clases es no uniforme, esto obliga a subclasificar a la huella en estudio, es decir, generar un nuevo conjunto de clases a partir de las ya definidas. Luego se procede a la comparación a escala fina. Este proceso recibe el nombre de matching. El proceso consiste en comprobar si el conjunto de minucias de una huella coincide con el de otra. (Morales y Ruiz, 2001)

3. BASES LEGALES

3.1. - DECRETO LEY DE MENSAJE DE DATOS Y FIRMAS ELECTRÓNICAS.

El Decreto-Ley número 1.204 de fecha 10 de febrero del 2001, publicado en la Gaceta Oficial Numero 37.148 del 28 de febrero del 2001, tiene como objeto el otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material que pueda ser atribuida a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados electrónicos.

Entre los principios que guían al Decreto es necesario destacar el Principio de Neutralidad Tecnológica que consiste en no acoger una determinada tecnología para las firmas y certificados electrónicos.

El Principio de Equivalencia funcional mediante el cual se equiparan las

instituciones del mundo virtual con las instituciones del mundo físico, haciéndolas equivalentes solo en lo que respecta a los efectos y consecuencias. Y por ultimo,

El Principio de Autonomía de la Voluntad de las Partes, en vista que el régimen establecido en el decreto-ley es supletorio y solo será aplicable en el caso que las partes no hayan acordado previamente un procedimiento, partiendo de la premisa que se trata de derecho privado donde rige en principio de voluntad de las partes, que consiste en que dada individuo solo puede obligarse en virtud de su propio querer libremente manifestado, y que el contrato es ley entre las partes, donde la única limitante que tienen las mismas es que sus actos no vayan contra la moral, las buenas costumbres o en contra el orden público.

3.2.-PROYECTO DE LEY DE COMERCIO ELECTRÓNICO

El proyecto de “Ley que regula el transporte electrónico de datos y autenticación en línea” es considerado por la autora como una primera aproximación a la regulación del comercio electrónico en Venezuela. Este constituye un antecedente de la actual ley de Mensaje de datos y firmas electrónicas, en vista de que la mayoría de las disposiciones del proyecto tratan temas que están establecidos en la Ley.

Este proyecto de Ley está compuesto por cuatro títulos que se describirán a continuación:

Título I: Consideraciones Generales; comprende 2 artículos el primero relativo al ámbito de aplicación y literalmente dice:

> ”Esta ley regula la eficacia y valor jurídico de todo tipo de información en forma de mensaje de datos dentro del ámbito de las actividades comerciales tal y como las mismas son definidas por el Código de Comercio Venezolano. Esta ley fijará las normas técnicas que deberán cumplirse para que una firma electrónica sea considerada valida, así como los protocolos y estándares de seguridad que se requieran para un adecuado funcionamiento del sistema certificatorio. Esta Ley regulará además, todo lo relativo a la firma electrónica, los entes de certificación y cualquier otra materia que incida en la utilización de los documentos electrónicos.”

El artículo 2 es un glosario de términos.

Título II: Se divide en dos capítulos a saber: Capitulo I, referente al Reconocimiento legal de los Mensajes de datos. Principios generales. Artículos 3 al 10. y el Capitulo II, relativo a la formación y validez de los contratos. Artículos 11 al 16.

Título III. Este título se refiere al Comercio Electrónico en materias especificas consta de un solo capitulo referido al transporte de mercancías. Artículos 17 y 18.

Título IV que consta de cuatro capítulos relativos a: Capitulo I: Firmas Electrónicas; Capitulo II: Entes de Certificación; Capitulo III: Certificados Electrónicos; Capitulo IV: De la Superintendencia de Entes de Certificación; y el Capitulo V: relativo a la Reglamentación y vigencia.

Como puede observarse la mayoría de los temas que trata el proyecto son establecidos en la Ley de Mensaje de datos y firmas electrónicas, por lo que la autora considera que el proyecto es un antecedente del Decreto-Ley.

3.3. - LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS

La Ley Especial contra los Delitos Informáticos de fecha 4 de septiembre del 2001 y que fue publicada en la Gaceta Oficial Nº 37.313 de fecha 30 de octubre del 2001, es una ley cuya normativa es amplia porque tiende a la protección integral de los sistemas que utilicen tecnologías de información, previniendo y sancionando los delitos que puedan llegar a cometerse contra esos sistemas o cualquiera de sus componentes, así como el uso de dichas tecnologías (art.1).

La finalidad de esta ley, es la prevención y punición de los delitos informáticos, según lo que la propia ley define por tales, no sólo por el fin sino también por el medio empleado para cometer el delito.

La ley consta de cuatro títulos. El primero trata los aspectos generales de la ley, fija los objetivos y define los términos empleados, así como establece qué tipo de sanciones empleará.

El título segundo, tipifica los distintos delitos que se pueden cometer contra la tecnología de la información. El título tercero, se refiere a las disposiciones comunes aplicables y el Titulo cuarto se refiere a la entrada en vigencia de la ley.

3.4. - LEGISLACIÓN INTERNACIONAL DE FIRMAS ELECTRÓNICAS

En el ámbito mundial las diferentes legislaciones se han abocado a la resolución de este problema, así vemos como ya la mayoría de los países tienen ya leyes sobre la materia.

Algunos de estos son:

Alemania : Digital Signature Ordinance (Signaturverordnung - SigV).

España: Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

Perú: Ley Nº 27269: Ley de Firmas y Certificados Digitales.

Ley Nº 27291**:** Ley que modifica el Código Civil permitiendo la utilización de los Medios Electrónicos para la Comunicación de la Manifestación de Voluntad y la Utilización de la Firma Electrónica.

Ley Nº 27310: Ley que modifica el artículo 11º de la Ley Nº 27269 .

Argentina: Resolución Nø45/97 de la Secretaría de la Función Pública dependiente de la Jefatura de Gabinete de Ministros. Referente a Infraestructura de Firma Digital y Documento Electrónico

Resolución de la Secretaría de la Función Pública Nø 194 /98, (B.O. 4/12/98); relativa a los Estándares sobre Tecnología de Firma Digital para la

Administración Pública Nacional.

Decisión Administrativa 102/2000. Prorrógase el plazo establecido por el Decreto Nø 427/98, mediante el cual se autorizó el empleo de la firma digital para aquellos actos del sector público nacional que no producen efectos jurídicos individuales en forma directa.

Política de Certificación: Resolución de la Secretaría de la Función Pública Nø 212/98, (B. O. 6/1/1999)

Proyecto de Ley. Dictamen contenido en la Orden del Día Nø 2651/01 de la H. Cámara de Diputados de la Nación Media Sanción en Diputados:15 de agosto de 2001

Documento Electrónico. LEY Nº 11.672, Complementaria Permanente de Presupuesto (T.O. 1999 por el decreto Nø 689/99). Ver Art. 45. Envío del 30/10/2001

Proyecto de Código Civil y Comercial. Decreto 685/95.Disposiciones sobre Firma Digital

Ley 25.506 de Firma Digital

Comunidad Económica Europea: 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.

Austria: Ley Federal de Firma Electrónica.

Federal Electronic Signature Law. (Signature Law - SigG).

Italia: Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999. Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513. Este trata lo relativo al Documento Informático -Validación - Firma Digital.

Chile: Ley que regula el Uso de la Firma Digital y los Documentos Electrónicos en la Administración del Estado

Proyecto de Ley sobre Documentos Electrónicos

Francia: Tecnologías de la Información Y Firma Electrónica

LOI no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (1)

Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

Japón: Ley sobre Firmas Electrónicas y Servicios de Certificación

Law Concerning Electronic Signatures and Certification Services.

Estados Unidos: Enmienda al Capitulo 57 de Las Leyes Consolidadas-Ley de Tecnología Estatal (New York)

Estados Unidos: Firma Digital

Electronic Signatures in Global and National Commerce Act.

Portugal: Firma Digital y Documentos Electrónicos

Decreto-Lei nº 290-D/99, de 02.08 (Suplemento). Aprova o regime jurídico dos documentos electrónicos e da assinatura digital

Colombia: Mensajes de Datos del Comercio Electrónico - Firmas Digitales - Entidades de Certificación - Otras Disposiciones.

Poder Público - Rama Legislativa. Ley 527 de 1999

Resolución 26930 del 26 de Octubre de 2000 de la Superintendencia de Industria y Comercio del Ministerio de Desarrollo Económico de la República de Colombia "Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores"

Decreto Nro 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.

Brasil: Comercio Electrónico, Firma Digital y Validez del Documento Electrónico

(Anteproyecto de Ley). Anteprojeto de Lei da Ordem dos Advagodos Do Brasil Ementa: Dispäe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências. InstruçÆo Normativa SRF nº 156, de 22 de dezembro de 1999:regula los Certificados Electrónicos

Comercio Electrónico, Validez del Documento Electrónico y Firma Digital (Proyecto de Ley , Cámara de Diputados). Câmara dos Deputados. Projeto de Lei Nø 1.589, De 1999. (Do Sr. Luciano Pizzatto e outros)

Brasil: Firma Digital- Certificación Digital

Medida Provisória No 2.200-2, De 24 de Agosto De 2001. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos

Ecuador: Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Finlandia: Ley de Servicios Electrónicos en la Administración Pública. Act on Electronic Service in the Administration

República Checa: Ley de Firma Electrónica. The Electronic Signature Act

República Dominicana: Proyecto de Ley Comercio Electrónico - Firma Digital

Venezuela: Ley de Mensaje de Datos y Firmas Electrónicas. Decreto Nº 1.204 10 de febrero de 2001

Panamá: Ley No.43 del 31 de julio de 2001,que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos

Guatemala: Proyecto de Ley para la Promoción del Comercio Electrónico y Protección de la Firma Digital

Singapur: Comercio Electrónico**.** Electronic Transaction Act. 1998

Malasia: Digital Signature Bill 1997

Naciones Unidas: Ley modelo de la CNUDMI sobre las firmas electrónicas (2001)

República Oriental del Uruguay: Ley Nº 15. 921 de 17 de diciembre de 1987 artículo 2, con la modificación introducida por Ley Nº 17.292 de 25 de enero de 2001, artículo 65.

Ley de Seguridad Social Nº 16.713 de 3 de septiembre de 1995. Titulo III - Del Banco de Prevision Social y del Registro de Historia Laboral

Ley Nº 17.243 de 29 de junio de 2000. (Ley considerada con Declaración de Urgencia - Art. 168 Nral. 7 de la Constitución de la República.)

Decreto Nº 65/998 de 10 de marzo de 1998. Reglaméntase la Implantación de Medios Electrónicos de Transmisión, Almacenamiento y Manejo de Documentos en la Administración Pública.

Decreto Nº 312/998 de 3 de noviembre de 1998. Establécese que la declaración jurada de las mercaderías ante la Dirección Nacional de Aduanas, en las operaciones Aduaneras de entrada, salida y tránsito, se realizará y solicitará por el declarante, en el Documento Único Aduanero.

Proyecto de Ley sobre Firma Electrónica

Medios de prueba - Código Civil y Código Procesal. LEY Nº 16.603 de 19 de octubre de 1994

4. - DEFINICIÓN DE TÉRMINOS BÁSICOS.

Biometría: Es el estudio mensurativo de las diferentes característica física o psicológicas de un individuo con la finalidad de identificarlo.

Sistemas Biométricos: Es un sistema automatizado que reconoce

determinada característica física o psicológica y la verifica de manera automática.

Indicador Biométrico: Es la característica anatómica o psicológica mediante la cual se puede reconocer a un individuo. Esta debe ser universal, única, permanente y además cuantificable.

Huella Dactilar: Es la marca que dejan los surcos de la piel que se toman al final de los dedos de las manos porque ahí son más nítidos y definidos.

Firma Electrónica: Es la información utilizada por el signatario asociada a otros datos electrónicos (mensaje) la cual lo relaciona con el mensaje de datos. Esta comprende la firma digital y la firma biométrica.

Efectividad: Se considerara efectivo aquel sistema que cumpla con los requisitos mínimos para ser considerado sistema biométrico y que además se adecue a las necesidades legislativas para que la firma biométrica sea considerada valida.

Firma Biométrica: Es el uso de determinada característica física (huella digital) o psicológica (voz) junto con técnicas avanzadas de criptografía asociada con otros datos electrónicos (mensaje) que permiten relacionar el mensaje con su autor garantizando la confidencialidad e integridad del mensaje.

Seguridad Jurídica: por seguridad jurídica se entenderá esa certeza

práctica de que la norma será cumplida, será esa confianza que el ciudadano le tiene al sistema y a la norma porque está seguro de que la misma garantizará eficientemente sus derechos.

Comercio Electrónico: Paz lo define como Cualquier forma de transacción comercial o intercambio de información utilizando nuevas tecnologías de comunicación entre empresas, empresas y sus consumidores, y entre empresas y la administración pública así como los mecanismos de pago telemáticos, dinero digital, métodos de seguridad en el comercio on-line y operaciones bancarias cibernéticas.

CUADRO N° 2

MATRIZ DE ANÁLISIS

CATEGORIA	SUBCATEGORIA	UNIDAD DE ANÁLISIS
Firma biométrica	Características	Unicidad Universalidad Permanencia Cuantificabilidad
	Esencia jurídica	Firma Firma electrónica
	Funcionamiento	Modelo de Maio y Maltoni
	Efectividad	Identificación de personas Utilidad
Seguridad	Criptografía	Definición Criptografía Simétrica Criptografía Asimétrica
	Entidades de certificación	Requisitos Actividades Obligaciones
Comercio electrónico	Transacción comercial nacional	Ley de datos y firmas electrónicas
	Transacción comercial internacional	

Fuente: García (2002)