UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO

Acreditada por Resolución CEUB 1126/02

MONOGRAFÍA

"DOCUMENTOS ELECTRÓNICOS Y DELITOS DE FALSEDAD DOCUMENTAL"

(Para optar el Título Académico de Licenciatura en Derecho)

INSTITUCIÓN: FISCALÍA DE DISTRITO DE LA CIUDAD DE LA PAZ.

POSTULANTE: **MARIANELA GUTIERREZ**

TUTOR ACADÉMICO: **DR.**

TUTOR INSTITUCIONAL: **DR.**

LA PAZ – BOLIVIA
2011

DEDICATORIA

El presente trabajo es dedicado a:

Dios que hizo posible que pueda culminar mis estudios; a mis padres Rolando y Mary, a mi hermana Francia y a mis sobrinas Yoselin y Yamel, ya que son el pilar fundamental en mi vida, inspirándome día a día a seguir adelante en el desarrollo de mis actividades.

AGRADECIMIENTOS

Especial agradecimiento a la Casa Superior de Estudios "Universidad Mayor de San Andrés" específicamente a la Carrera de Derecho, misma que me cobijó en los años de vida universitaria brindándome la educación adecuada para ejercer mi vida profesional.

Asimismo; agradecer a la parte administrativa, docentes y compañeros que han sido fuente permanente de fuerza e inspiración a lo largo de mi estadía en esta importante Institución Educativa Estatal.

INDICE GENERAL

CAPITULO II

LOS DOCUMENTOS ELECTRÓNICOS

CAPITULO III

FIRMA ELECTRONICA, FIRMA DIGITAL,

CERTIFICADOS ELECTRONICOS Y DIGITALES

CAPITULO IV

DELITOS DE FALSEDAD DOCUMENTAL

CAPITULO V

BIEN JURIDICAMENTE PROTEGIDO

CAPITULO VI
FALSEDAD EN DOCUMENTO ELECTRÓNICO

PROLOGO

El presente trabajo monográfico presenta las investigaciones de los dos últimos años sobre los delitos que le dan nombre. Sólo una parte de los estudios sobre la falsedad documental electrónica ha sido publicada con anterioridad.

Los avances tecnológicos y el gran desarrollo del uso del Internet, han hecho que, primero las empresas y después los ciudadanos y la administración, estén haciendo cada vez mas uso de las telecomunicaciones y de las nuevas tecnologías.

En todo los Países del mundo se ha vuelto indispensable adaptar las leyes vigentes a las nuevas concepciones técnicas y tecnológicas, con el fin de dar respuestas a las necesidades derivadas de la practica jurídica y a las exigencias propias de un mundo globalizado, en los asuntos comerciales, civiles, entre otros.

Las pruebas electrónicas de dichas transacciones, son susceptibles de ser aportadas en un proceso determinado, y luego se pueden ver afectadas en su valoración deficiente por parte del juez. Esto, porque no existen criterios o requisitos que guíen la actividad valorativa de la evidencia digital a nivel nacional e internacional, dejando tal acción al libre albedrío de la razón y de la sana critica. Prerrogativas estas, que si bien son útiles y suficientes en determinados casos, en el campo de la informática y mas específicamente del documento electrónico, teniendo en cuenta su especialidad, requieren una valoración mas clara y detalladas que cualquier otro medio probatorio.

Los estudios sobre los documentos electrónicos y la falsedad documental a través de estos, responden a las transformaciones dogmáticas que estos delitos han experimentado en los últimos tiempos en nuestro país y a los procesos recientes que han tenido lugar en América y Europa, que han centrado la atención en estos tipos penales.

Muchos podrían preguntarse: ¿es segura la red para realizar transacciones con contenido económico y jurídico? Evidentemente la seguridad total no existe, pero ello no debería ser motivo de preocupación, ya que también en el comercio ordinario y en las transacciones convencionales tampoco existe seguridad plena.

Es una realidad inobjetable, que la red se inicio con sencillas páginas Web a un costo mínimo y con escasos niveles de seguridad. Pero a medida que su uso era más acentuado, se han ido realizando sistemas de pago, transacciones aun rudimentarias.

Pero hoy se puede afirmar que existen implantados sistemas capaces de garantizar altos niveles de seguridad en la red, mayores incluso que en el negocio tradicional, ya que además de protección frente a riesgos, cubierta por entidades de seguros, existen mecanismos de seguridad que permiten el acceso a ciertos usuarios, sistemas de control de accesos, defensas contra hackers, etc. Y precisamente la utilización de las nuevas tecnologías en las transacciones comerciales y los inconvenientes que se planteaban desde el punto de vista jurídico, ha llevado a los legisladores a la creación de sistemas seguros de garanticen la autenticidad, la integridad y la confidencialidad de los datos que se transmiten a través de la red.

Como ya se sabe, las pruebas procesales están orientadas principalmente a convencer al juzgador de la existencia de un hecho. Y al ser el correo electrónico, la firma digital, un casette de video, etc., realidades materiales, instrumentos naturalmente aptos para Instituto de la Judicatura de Bolivia informar por medio del sentido de la vista, se puede afirmar que todos estos documentos son verdaderas fuentes de prueba.

En este contexto este trabajo resulta sumadamente útil para informarnos y actualizarnos acerca de esta temática. Con este trabajo deseo también expresar mi más profundo agradecimiento a quienes colaboraron en la elaboración de este trabajo monográfico.

INTRODUCCIÓN

Al hablarse de documentos informáticos o electrónicos se alude a casos en que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad quizás ya expresada en las formas tradicionales, y en que la actividad de un computador o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales.

Si analizamos la noción tradicional de documento referida al instrumento en el que queda plasmado un hecho que se exterioriza mediante signos materiales y permanentes del lenguaje, vemos como el documento electrónico cumple con los requisitos del documento en soporte de papel en el sentido de que contiene un mensaje (texto alfanumérico o diseño gráfico) en el lenguaje convencional (el de los bits) sobre soporte (cinta o disco), destinado a durar en el tiempo.

El documento electrónico es admisible en los países de sistema de libre apreciación de la prueba, conforme a las reglas de la sana crítica para aquellos medios de prueba no excluidos en forma expresa en la ley, en este sentido, el juzgador le deberá atribuir los efectos y fuerza probatoria después de una adecuada valoración y comprobación de autenticidad.

Se hace inevitable que las instituciones, especialmente las gubernamentales, tomen conciencia del retraso que pueden estar sufriendo las sociedades a las que sirven e inciden las acciones que estén dentro de sus posibilidades para que se implemente de forma ágil y diligente un nuevo marco de actuación que permita la utilización cotidiana de medios tecnológicos, especialmente, del documento electrónico.

En tal sentido, los foros de discusión, centros de investigación, entidades públicas y privadas de los países, y especialmente los legisladores, tienen la obligación de generar un debate en todos los ámbitos de la sociedad y especialmente en los que se ven más afectados, esto es, las empresas y el sector público. Este impulso es ineludible para colocar a cualquier país que pretenda un desarrollo sostenido en una situación de igualdad frente a otras naciones o regiones que ya tienen medio camino recorrido.

En este contexto el presente trabajo monográfico propone un estudio de los delitos de falsedad documental a partir de los documentos electrónicos, establecer que en nuestro país, Bolivia, la legislación es mínima, de manera que mediante este trabajo pretendemos contemplar aspectos teóricos, jurídicos y prácticos de la temática planteada y así permitir un mejor manejo judicial de este tipo de delitos.

En este sentido la monografía esta constituida por seis capítulos que para una mejor y mayor comprensión de su contenido, desarrollaremos detalladamente, así tenemos:

1. El primer capítulo, esta compuesto por el diseño de la monografía que contiene siete puntos, referidos a la elección del tema, la justificación del mismo, sus delimitaciones, los marcos de referencias, el planteamiento del problema, los objetivos, la estrategia metodológica y las técnicas de investigación monográfica donde se describen las técnicas que se utilizaron en la presente monografía.

2. El segundo capítulo, trata sobre los documentos electrónicos, aspectos acerca de la teoría desarrollado en dos puntos, referidos al concepto y a su definición, conceptualización legal en diferentes países, donde se pretende tener un conocimiento más exacto del documento electrónico.

3. El tercer capítulo, sobre la firma electrónica y digital y los certificados electrónicos y digitales contiene siete puntos, referidos a la firma convencional, aspectos teóricos de la firma digital, para que sirve, en que se basa, aspectos teóricos de la firma electrónica,

sus características y regulación en diversos lugares, sus aplicaciones; en relación a los certificados analizamos los certificados digitales y electrónicos, sus diferencias, características y aplicaciones.

4. El cuarto capítulo, está compuesto por los delitos de falsedad documental, sus conceptualizaciones, clasificación, su doctrina, tipificación, eficacia probatoria y relevancia jurídica, todo lo anteriormente citado esta detallado en seis puntos que componen este capitulo.

5. El quinto capítulo, que trata sobre el bien jurídicamente protegido esta desarrollado en tres puntos, que contienen las conceptualizaciones y definiciones, la posición dogmática y la doctrina y dogmática comparada.

6. El sexto capítulo trata de la falsedad en el documento electrónico, esta desarrollado en tres puntos que establecen los antecedentes, la noción de documento y tecnología y por ultimo la función de garantía de los documentos electrónicos,

Finalmente se establecen las conclusiones y por ultimo las sugerencias y recomendaciones propias del tema.

Este es el lineamiento integral y general de la presente monografía, de la cual tengo la firme convicción de que sea objeto de un estudio más profundo y que pronto se mejore la legislación en relación a esta temática dentro de nuestra legislación vigente, aspecto que es necesario y vital para la población y en especial para las personas naturales y jurídicas que trabajan y se desempeñan con base en este tipo de documentos y que necesitan respuestas inmediatas a sus inquietudes. Espero que esta monografía les sea agradable y útil.

Gracias.

CAPITULO I
DISEÑO DE LA MONOGRAFÍA

4. ELECCIÓN DEL TEMA DEL ENUNCIADO

El presente trabajo tiene como objeto de investigación LOS DOCUMENTOS ELECTRÓNICOS Y DELITOS DE FALSEDAD DOCUMENTAL, el mismo que se estudiará desde los puntos de vista sociológico y jurídico, debido a que tales hechos delictivos cometidos consecutivamente, se traducen en que no se estarían cumpliendo las normas de manera correcta y eficiente.

5. JUSTIFICACIÓN DEL TEMA

La revolución tecnológica ha redimensionado las relaciones entre los hombres. Estamos en una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a la expresión "sociedad de la información".

Asimismo, detrás de todo este desarrollo tecnológico descansa la información como objeto de dicha revolución. La información fue valiosa en el pasado, la misma que significaba encontrarse en una situación ventajosa respecto a quienes no la tenían; pero en el presente su valor acrecienta, ya que antes no existía la posibilidad de convertir informaciones parciales y dispersas en informaciones en masa y organizadas, de interrelacionar esa información y de procesarla con rapidez, como ocurre hoy en la sociedad de la información. En definitiva, lo que ocurre es que esa información cada vez aporta más conocimiento, y quien dispone de conocimiento tiene poder.

Peter F. Drucker señala: "El recurso económico básico, el medio de producción, para utilizar el término de los economistas, ya no es el capital ni los recursos naturales (el suelo de los economistas) ni la mano de obra. Es y será el saber".

Frente a las mayores repercusiones de la informática en el Derecho, muchos de los problemas que se suscitan no se satisfacen con las soluciones jurídicas tradicionales, muchas de ellas son insuficientes y obsoletas hoy en día, debido a que los conceptos y categorías básicos de la ciencia jurídica que surgieron en la edad moderna y en la codificación actual, han variado.

Ello obliga a tener una actitud reflexiva, crítica y responsable ante los nuevos problemas que trae consigo la tecnología de la información, aunque sea imprescindible que los estudiosos del Derecho adopten una conciencia tecnológica y se familiaricen con aspectos científicos e informáticos. De esta forma se presenta el acercamiento de dos disciplinas inmutables e irreconciliables entre sí como lo son el Derecho y la Informática, las cuales, si bien diferentes en su naturaleza, no lo son tanto en sus propósitos de prestar servicio al hombre y propender a una sociedad más justa y eficiente.

Por esta razón, se deben diseñar nuevos instrumentos de análisis y marcos conceptuales para adaptarse a las exigencias de una sociedad en transformación, hay que construir una ciencia del Derecho abierta y comprometida con las respuestas a las nuevas necesidades de quienes vivimos en la era de la Informática.

Esta nueva ciencia debe tomar muy en cuenta el valor probatorio de los documentos informáticos, pues desde hace mucho tiempo y más aun de aquí en adelante los mismos se convertirán en un grave problema, por la dudosa procedencia y la falta de garantías de los mismos.

Por esta razón y más aun por el retrazo tecnológico que vive nuestro país, que considero necesario presentar este trabajo de investigación para poder dar a los documentos un valor que garantice y de la seguridad necesaria a cualquier persona para defender sus derechos, asimismo orientarlos con los pasos que se podrían seguir en este complicado mundo informático.

La aparición de la firma electrónica en el tráfico jurídico representa una nueva etapa en la vida dogmática de los delitos de falsedad documental .Los avances tecnológicos han ido generando diferentes problemas jurídicos en relación al concepto de documento y, por extensión al de firma. En primer lugar se planteó la cuestión de si era posible considerar documento los que realmente no constituyeran escrituras, como, por ejemplo la expresión de la palabra grabada.

Más tarde se generaron dificultades con las fotocopias y finalmente con el fax; de alguna manera, los problemas de la influencia de la tecnología superan el ámbito de la estricta falsedad documental. En la práctica se ha planteado recientemente la cuestión de si la falsificación de los datos contenidos en la banda magnética de una tarjeta de crédito debe ser considerada equivalente a la falsedad de moneda. No podemos ignorar que el problema proviene de la gravedad de la pena que tal equivalencia genera, pero no deja de ser significativo que para resolver la supuesta desproporción penal se haya pensado que la utilización fraudulenta de datos electrónicos en la banda magnética de una tarjeta de crédito no debería ser considerada como falsificación de la tarjeta. La tesis, pone de manifiesto la posible tendencia, sobre todo intuitiva, de negar –a priori el carácter de documento a la utilización de datos electrónicos, es decir, una solución difícilmente sostenible.

Cada vez que la realidad social presenta a los juristas nuevas situaciones, la primera aproximación a la solución del problema suele ser llevada a cabo mediante un análisis de problemas análogos del pasado, que hoy pueden estar ya olvidados como tales. Un ejemplo que resulta instructivo es el del contagio del SIDA. Cuando apareció esta nueva

enfermedad, los juristas recordaron de inmediato que en las décadas de los 20 y los 30 el contagio venéreo de determinadas enfermedades había dado lugar a una serie de cuestiones que mutatis mutandis, fueron orientando las nuevas soluciones dogmáticas.

En el plazo aproximado de tres décadas en materia de documentos la dogmática de los delitos de falsedad documental se ha visto confrontada con diversas innovaciones tecnológicas que han obligado a reflexionar sobre la trascendencia que ellas podían tener en la aplicación de los delitos correspondientes a este ámbito.

También la legislación ha experimentado transformaciones que provienen de la evolución de la tecnología en el tráfico jurídico. Lamentablemente, la reforma penal de 1995 no ha tenido en cuenta la evolución que en la materia se observa en el derecho europeo.

Si se comparan los tipos penales de la falsedad documental del Código vigente con los del Código Penal Alemán, se podrá percibir de inmediato que este último ha introducido en el parágrafo 268 un tipo específico para la falsificación de los soportes documentales de comprobaciones y mediciones expedidas por medios técnicos (technische Aufzeichnungen), en el que en el lugar de la declaración de voluntad o de pensamiento, característica del documento tradicional, entra el registro de datos, medidas, o valores aritméticos realizados por un aparato automático. Se trata de casos en los que se protege la confianza no en la emisión de una declaración documentada por una persona, sino en los datos automáticamente emitidos por una máquina o aparato especialmente programado para tales fines.

En el Código alemán se introdujo también el parágrafo 269, referido a la falsificación de datos relevantes desde el punto de vista probatorio, cuya principal finalidad es la prevención de la criminalidad informática. Ambas disposiciones anticipan una serie de problemas que sin lugar a duda son de especial importancia en los documentos electrónicos.

Los antecedentes histórico-dogmáticos a los que cabe referirse ahora son los de las fotocopias y el telefax.

Las fotocopias, lo mismo que las copias, de documentos no se consideran tales en la doctrina y en alguna jurisprudencia del Tribunal Supremo, dado que no permiten conocer la identidad del emisor, un elemento esencial del documento, como hemos visto.

Por el contrario, cuando la fotocopia (en su caso la copia) ha sido certificada o autenticada como copia fiel de un documento (por ejemplo mediante una intervención notarial), el conocimiento del emisor está asegurado y el carácter documental no ha generado problemas. El BGH (Tribunal Supremo Federal alemán) ha formulado esta tesis de manera precisa: “La fotocopia (…) únicamente reproduce (como imagen) una declaración corporizada en un escrito (…) [pero] no certifica su emisor. Por lo tanto, no es posible reconocerle [a la fotocopia], sin más, la función de garantía de la corrección del contenido, que básicamente es propia de todo documento”.

Como es claro, ello no significa que la fotocopia de un documento, aunque no sea objeto de la acción idóneo de una falsedad documental, no sea un instrumento idóneo para engañar y, de esta manera, cometer un delito de estafa. No se debe olvidar que el delito de falsedad documental constituye, como tipo penal autónomo, un desprendimiento de la estafa.

Lo que aquí se quiere decir es, simplemente que alterar una fotocopia no es alterar un documento, aunque sea la creación de un medio para la comisión de una estafa.

6. DELIMITACIONES DEL TEMA

7.1. Delimitación Temática

Los DOCUMENTOS ELECTRÓNICOS Y DELITOS DE FALSEDAD DOCUMENTAL, están destinados a estudiar una etapa y tarea de cada ser humano como sus problemas, carencias, deficiencias en si, las necesidades que lo llevan a delinquir y a ser rectificado por la sociedad. En este sentido el presente trabajo se encuentra delimitado temáticamente dentro del Derecho Informático.

7.2. Delimitación Espacial

El tema de la Monografía será estudiado en la Ciudad de La Paz, por ser en esta ciudad donde se realizaron las pasantitas, más precisamente en las oficinas de la Fiscalía de Distrito.

7.3. Delimitación Temporal

Este fenómeno de nuestro interés será estudiado desde el mes de julio 2009 a mayo de 2010 fechas en la que realicé la pasantía en la Fiscalía de Distrito de la ciudad de La Paz.

8. MARCO DE REFERENCIA

F) MARCO INSTITUCIONAL

MINISTERIO PÚBLICO O FISCALÍA GENERAL DEL ESTADO

El Ministerio Público o Fiscalía del Estado es un organismo constitucional con independencia funcional de los poderes del Estado, con autonomía presupuestaría y

actúa en estricta sujeción al ordenamiento jurídico, ejerce de oficio las acciones inherentes a sus funciones cuando sean procedentes, o se opone a las indebidamente intentadas, en la medida y forma que la Constitución Política del Estado y las leyes lo establecen.

Finalidad

El Ministerio Público tiene por finalidad promover la acción de la justicia, defender la legalidad, los intereses del Estado y la Sociedad, establecidos en la Constitución Política del Estado y las leyes de la República.

Funciones

Para el cumplimiento de sus fines. El Ministerio Público tiene las siguientes funciones:

- El Ministerio Público defenderá la legalidad y los intereses generales de la sociedad, y ejercerá la acción penal pública. El Ministerio Público tiene autonomía funcional, administrativa y financiera.

- El Ministerio Público ejercerá sus funciones de acuerdo con los principios de legalidad, oportunidad, objetividad, responsabilidad, autonomía, unidad y jerarquía.

La Fiscal o el Fiscal General del Estado es la autoridad jerárquica superior del Ministerio Público y ejerce la representación de la institución.

El Ministerio Público contará con fiscales departamentales, fiscales de materia y demás fiscales establecidos por la ley. La Fiscal o el Fiscal General del Estado se designará por mayoría absoluta de la Asamblea Legislativa Plurinacional.

La designación requerirá de convocatoria pública previa, y calificación de capacidad profesional y méritos, a través de concurso público. La Fiscal o el Fiscal General del Estado

reunirá los requisitos generales de los servidores públicos, así como los específicos establecidos para la Magistratura del Tribunal Supremo de Justicia. La Fiscal o el Fiscal General del Estado ejercerá sus funciones por seis años, sin posibilidad de nueva designación.

En la nueva CPE, el Ministerio Público representado por la Fiscalía General de la República pasa a convertirse en la Fiscalía General del Estado, según establece la Constitución Política vigente.

Se le ha quitado al Ministerio Público anterior, en la nueva Constitución una función, que es el ser el representante de los intereses del Estado, esta función ha de ser desarrollada y ejercida por la Procuraduría General del Estado, que tiene facultades específicas que representa los intereses del Estado, velar por ejemplo la recuperación de los recursos económicos, etc.

De ahora en adelante la Fiscalía General del Estado es defensora del Estado y la sociedad pero en el marco del ejercicio de la acción penal pública.

Obligaciones

El Ministerio Público tiene las siguientes obligaciones:

a) Velar porque los tribunales de justicia respeten los derechos y las garantías constitucionales de la persona.
b) Velar por el respeto a la independencia funcional de los magistrados, jueces y fiscales.
c) Apersonarse a los juzgados e instancias administrativas, para proponer las diligencias necesarias a fin de regularizar procedimientos y subsanar vicios.
d) Vigilar la observancia estricta de los plazos procesales tomando las medidas pertinentes en los casos de negligencia u omisión.

e) Verificar, asegurar y presentar las pruebas necesarias en los procedimientos en que participe.
f) Cuidar por el estricto cumplimiento de las resoluciones judiciales.
g) Visitar periódicamente los establecimientos penitenciarios de detención para verificar y exigir el respeto a los derechos de los detenidos.
h) Ordenar la libertad de las personas arrestadas, aprehendidas o detenidas sin mandamiento emanado de autoridad competente, salvo los casos previstos por Ley.

Fiscal General

El Fiscal General del Estado, es el máximo representante del Ministerio Público. Ejerce autoridad en todo el territorio nacional y sobre todos los funcionarios del Ministerio Público, cualquiera sea el Distrito al que pertenezcan. Ejerce la acción penal pública y las atribuciones que la Constitución Política del Estado y las leyes le otorgan al Ministerio Público, por sí mismo o por medio de los órganos de la institución.

Fiscales de Distrito

Los Fiscales de Distrito son los representantes de mayor jerarquía del Ministerio Público en su distrito. Ejercerán la acción penal pública y las atribuciones que la Constitución Política del Estado y las Leyes le otorgan al Ministerio Público, por sí mismos o por intermedio de los fiscales a su cargo, salvo cuando el Fiscal General asuma directamente esa función o la encomiende a otro funcionario, mediante instrucción expresa, conjunta o separadamente.

Fiscales de Recursos

Los Fiscales de Recursos tendrán su sede en la ciudad de Sucre y serán designados de conformidad a las normas que regulan la carrera fiscal. Su especialización e

incremento en el número, será determinado anualmente por el Fiscal General, previo dictamen del Consejo Nacional y según las necesidades del servicio.

Fiscales de Materia

Los Fiscales de Materia ejercerán la acción penal pública, con todas las atribuciones que la Constitución Política del Estado y las Leyes le otorgan al Ministerio Público, asegurando su intervención en las diferentes etapas del proceso penal y aún ante el tribunal de casación, cuando así lo disponga el fiscal de su distrito o el Fiscal General de la República.

Su especialización e incremento en el número, será determinado anualmente por el Fiscal General, previo dictamen del Consejo Nacional del Ministerio Público y según las necesidades del servicio. Sin perjuicio de la facultad prevista, el ejercicio de la acción penal pública en delitos vinculados al tráfico de sustancias controladas, estará a cargo de los Fiscales de Materia de sustancias controladas.

Fiscales Asistentes

Los Fiscales Asistentes son funcionarios del Ministerio Público asignados por el Fiscal de Distrito para asistir a los Fiscales de Materia en el cumplimiento de sus funciones. Actuarán siempre bajo la supervisión y responsabilidad del superior jerárquico a quien asisten. No podrán intervenir autónomamente en las audiencias ni en el juicio.

G) MARCO TEÓRICO

Ante los elementos legales que plantea el problema, nuestra legislación a futuro debe optar por:

- La adaptación de conceptos y principios mediante la interpretación jurisprudencial en relación con la doctrina tradicional;

- o, por el contrario, el establecimiento de un marco jurídico propio que, sin apartarse de las bases histórico-jurídicas, desarrolle un sistema que tenga como fin último la seguridad jurídica de los sujetos, bienes y negocios jurídicos.

Siendo partidarios de la segunda posibilidad podemos concluir que:

La imperiosa necesidad de publicitar y perpetuar los actos jurídicos transcendentes de los hombres, ha constituido la razón primordial para que estos actos sean conservados en soportes que garanticen la integridad, autenticidad y autoría de su contenido en el transcurso del tiempo; encontrándose que el documento escrito ha sido al soporte más idóneo para garantizar el cumplimiento de dichos fines. Esta preferencia por el documento escrito y la expresa obligatoriedad de conservarlos, clasificarlos, ordenarlos e incluso signarlos, para su recuperación con el propósito de satisfacer la demanda de información contenida en éste es ahora posible de ser complemento con el documento electrónico.

La incorporación de las nuevas tecnologías de la información hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades. El avance de su implantación en todas las actividades ha provocado cambios de tal magnitud que puede afirmarse que la sociedad actual está inmersa en la era de la revolución informática. Este avance no es sólo cuantitativo, sino de algo más importante, que puede acceder a todo tipo de información y obtener con ello el beneficio correspondiente.

La información ha sido calificada como un auténtico poder de las sociedades avanzadas, ya tenía su importancia en la antigüedad, pero con el desarrollo de la

telemática su valor ha crecido de forma tal que se dirige a un futuro prometedor para unos e incierto para otros.

La revolución tecnológica ha determinado el surgimiento de la informática y de la telemática, produciendo cambios profundos en distintas actividades que acceden al uso de las nuevas tecnologías que estas ciencias ponen a disposición de la población mundial. Uno de ellos será la reducción drástica de la circulación de papel, lo que acarreará, con el creciente uso de la telemática, importantes consecuencias en la actividad inter-empresarial, en la banca, en los seguros y en el comercio exterior. En especial se requiere una adaptación normativa en relación con los medios de prueba admisibles, tanto respecto del contenido de los actos como de la identidad del emisor.

Innumerables transacciones económicas se vienen realizando a través de los medios electrónicos, sin más soporte legal que el pacto entre las partes.

La contratación electrónica en su más puro sentido, poco a poco se viene abriendo paso y crece de forma espectacular.

Una vez más los hechos caminan delante del Derecho, entendiendo éste como Derecho positivo.

Muchas veces sucede que cuando se trata de reconducir estos nuevos hechos a las figuras jurídicas existentes se encuentra con dificultades. Las viejas instituciones jurídicas que, a través de los siglos han ido incorporando nuevas realidades sociales, cuando tienen que hacerlo respecto a estas nuevas tecnologías, en cierto modo dudan y las admiten con reservas. Así ocurre cuando se trata de adaptar el concepto de documento y firma, tal como antiguamente se concebía, al nuevo campo de las transferencias electrónicas.

La "Firma electrónica" es -por su parte- el conjunto de datos, en forma electrónica, asociados a otros datos electrónicos o adjuntos funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

H) MARCO HISTÓRICO

Desde los tiempos del Derecho Romano el acta escriturada se ha tenido como el instrumento más respetable para probar hechos y guardar memoria de un tiempo. El derecho dominicano, por su parte, tradicionalmente ha considerado la firma como el trazo gráfico duradero, que de su mano y puño realiza una persona natural ante un soporte físico, usualmente de papel, validando con ello el contenido de lo expresado en el documento, y si ella es estampada ante Notario Público adquiere además el carácter de autenticidad.

Sin embargo, con el vertiginoso avance de las Tecnologías de la Información y la Comunicación (TIC) se han producido en la sociedad contemporánea nuevas herramientas de comunicación y de intercambio entre los sujetos de derecho, que permiten instrumentar declaraciones de voluntad mediante el uso de otro tipo de soporte distinto al papel: surge entonces el formato digital.

A fin de dotar de validez jurídica las transacciones que cada día en mayor cantidad se realizan en soporte alternativo al papel, es decir en soporte digital y por medios electrónicos, en el año 1996 la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) elabora la “Ley Modelo sobre Comercio Electrónico”. Dicha ley recomienda que las disposiciones contenidas en su texto sean incorporadas a los ordenamientos jurídicos de los Estados partes, por considerarlas instrumento útil para agilizar las relaciones entre particulares.

En respuesta a esa recomendación, una gran parte de las naciones latinoamericanas y de todo el mundo comenzaron la adaptación de sus sistemas legales.

Las sociedades humanas se caracterizan por el constante cambio, el que cada día nos sorprende más por su rapidez y profunda incidencia en el desarrollo de patrones de conducta social, creando entre las personas nuevos modos de interacción. Sin embargo, no estamos en presencia únicamente de progreso científico o tecnológico, sino que el cambio involucra las creencias, las actitudes psicológicas, el ámbito económico y político; en suma, la forma de convivir en el mundo. Es decir, estamos viviendo un verdadero cambio social que modifica irreversiblemente los modos de conducta en sociedad.

Sin lugar a dudas, estos cambios sociales profundos se tienen que reflejar a través de modificaciones serias en el ordenamiento jurídico, como sucede por ejemplo, con el surgimiento de la legislación medioambiental o las normas que rigen a las tecnologías de la información. Ante ello, el Derecho no puede negarse a progresar, entendiendo que éste progresa cuando es capaz de interpretar mejor las necesidades humanas y de adaptarse en forma más perfecta a lo que de él se requiere para el bien común, la paz, la justicia y el progreso.

Por tal motivo, en un cambio que consiste en la modernización del sistema social, sin sustituir los valores y las estructuras fundamentales existentes en la comunidad, el Derecho debe permitir o facilitar el uso oportuno de recursos humanos, naturales, financieros, científicos y otros, existentes en la comunidad.

Este cambio no es producto de un acaso, sino del afán conciente de las personas por buscar soluciones satisfactorias a sus problemas y necesidades. Es así como nadie podría desconocer que el desarrollo de la ciencia y la tecnología es una de sus importantes causas directas e inmediatas.

I) MARCO CONCEPTUAL

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Consiste en la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras le dieron lugar al concepto.

Pero, sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas, ya sean jurídicas o naturales.

El fin, de la firma digital, es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado; y es por eso que a través de la legislación, se intenta acercarla, exigiéndose ciertos requisitos de validez.

El papel es el medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito, etc.). Esta cualidad física le da entidad al documento, contiene sus términos, conceptos y sentidos de una manera perdurable, y al ser un elemento físico cualquier alteración dejará " señales" identificables.

Pero, los papeles ocupan lugar y pesan demasiado, resulta complejo y molesto buscar información en ellos (requiriendo de la acción humana ya sea al archivarlos y/o al

rescatarlos), y el compartir los documentos también resulta inconveniente, lo que se podría evitar con un sistema de computación.

El documento digital es simplemente una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información. Esta representación de la información en base a dígitos implica en el ámbito informático una representación binaria, es decir por medio de unos y ceros.-

Todo tipo de información representada digitalmente constituye un documento digital y es susceptible de ser firmada digitalmente. Es por ello que la firma digital puede utilizarse para otorgar validez jurídica o eficacia probatoria a toda declaración de voluntad o de conocimiento, con independencia de su extensión o de su medio de almacenamiento, sin limitación alguna.

J) MARCO JURÍDICO

- **Marco Jurídico Nacional**

a) Antecedentes

Desde el año 2004, se retomó de manera oficial el concepto e importancia del "comercio electrónico", recogiendo una serie de trabajos previos, que en la última década habían pretendido impulsar una política gubernamental que permita un marco legal en esta importante temática, la base de esta discusión se había iniciado con la entrega por parte de la Cámara de Comercio en el año 1994 al Congreso Nacional del Proyecto de Ley denominado Código Ordenador de Mercado, que contenía 5 normas fundamentales referidas no solo ala comercio electrónico sino también a las temáticas transversales, de propiedad intelectual, promoción y defensa del consumidor, ley de competencia y la reforma al Código de Comercio, este esfuerzo del sector privado se

quedó en una buena iniciativa que posteriormente derivó en diversos anteproyectos por cada uno de los temas.

Se retoma con fuerza inusitada la temática de la tecnología y de la Sociedad de la Información en el marco del comercio electrónico gracias a la iniciativa de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), bajo el financiamiento de la línea del programa BID ATN SF 7692 BO, que logró resumir en un solo documento varias propuestas de ley que esta temática tenía, presentando un Anteproyecto de Ley de Comunicación Electrónica de Datos, Firmas Electrónicas y Comercio Electrónico, Proyecto de Ley, que tuvo la virtud de reunir a varias instituciones del sector público y privado, encabezando este proceso el ADSIB contó con la valiosa participación de el Viceministerio de Justicia, el Banco Central, CEPROBOL, Ministerio de Hacienda, Superintendencia de Empresas, Superintendencia de Bancos, Superintendencia de Telecomunicaciones, Impuestos Nacionales, Aduana Nacional, así como las Comisiones de Comercio Industria Ciencia y Tecnología por parte de la Cámara de Senadores y la Comisión de Constitución y Policía Judicial de la Cámara de Diputados, e itinerantemente con la participación de otros ministerios e instituciones del Estado. Por parte del sector privado se contó con la valiosa participación de la Cámara Nacional de Comercio que aglutina a sus nueve Cámaras Departamentales, y gentilmente se dio sus espacios para las reuniones de coordinación y discusión de este importante proyecto, ASOBAN representando al Sistema Financiero, la Cámara Nacional de Industrias, El Colegio de Abogados de La Paz, Colegio Nacional y Departamental de Notarios, La Cámara Boliviana de Tecnologías de la Información, la valiosa participación de los diversos actores y de los expertos y profesionales delegados coadyuvó, ni duda cabe, a la consolidación de una norma marco muy clara que pretende consolidar un marco legal eficiente para lograr una mayor seguridad jurídica de los usuarios de las tecnologías de la información.

Este Proyecto, antes de ser remitido al Congreso Nacional sufrió una serie de modificaciones (56 versiones), y fue posteriormente remitido para su estudio y

aprobación a la Comisión en la Legislatura precedente, en ese entonces a la cabeza del ex Senador Huáscar Aguilar, quien luego de convocar a los sectores involucrados en el Proyecto de Ley, (Enero 6 del 2006), sugirió una nueva revisión global al documento y se hizo la recomendación colectiva de que le den consistencia, pues a causa de las múltiples modificaciones se encontraron algunas incongruencias contenidas en el propio documento final, puesto que el sector público llevó adelante en forma conjunta una última versión para su presentación ante el Congreso sin la participación del sector privado.

El Proyecto de Ley presentado a consideración del Pleno Camaral, fue la versión modificada y última por parte del sector público, presentada en noviembre de 2005 “Anteproyecto de Ley de Comunicación Electrónica de Datos y Comercio Electrónico” -consensuada solamente por el sector público-, y el Proyecto de Ley “Documentos, firmas Electrónicas y Entidades Certificadoras”, presentado por el Senador Oscar Ortiz. Por definición de los sectores público y privado convocados por el senador Huascar Aguilar, se definió trabajar sobre la versión consensuada por el sector público y privado, puesto que, el trabajo de más de dos años no se podía desechar y el documento de Anteproyecto de Ley de Comunicación Electrónica de Datos y Comercio Electrónico era un documento mucho más completo y adecuado.

Este Proyecto de Ley cambia de título por otro más adecuado al contenido del mismo, denominándose: “Documentos, Firmas y Comercio Electrónico”, tiene como aporte la inclusión de un Título específico para el Comercio electrónico, considerando a los proveedores de servicios y la protección al consumidor en el ámbito del comercio electrónico.

b) Normatividad nacional en relación al tema

En Bolivia se cuenta actualmente con las siguientes normativas legales:

Anteproyecto de Ley: Documentos, Firmas y Comercio Electrónico

Propone el reconocimiento del valor jurídico y probatorio de:

a) Los actos jurídicos celebrados mediante medios electrónicos u otros de mayor avance tecnológico.
b) El uso de firmas electrónicas debidamente certificadas.
c) Los actos civiles y comerciales que utilicen directa o indirectamente medios electrónicos para realizar actividades de comercio electrónico.

Guía de estandarización de sitios Web gubernamentales del Estado boliviano

El cual tiene el objetivo de cumplir ciertas pautas en los sitios Web gubernamentales bolivianos que permitan asegurar que estos sitios contengan la información requerida por la normativa actual, sean accesibles, se encuentren fácilmente en la Web, cumplan con preceptos en cuanto a su diseño e interfaz para cumplir de manera eficiente y eficaz con su objetivo y cumplan preceptos mínimos sobre su seguridad.

Anteproyecto de Ley de Protección de datos

El Anteproyecto de Ley de Protección de Datos tiene por objetivo garantizar y proteger los datos personales de personas físicas y naturales asentados en base de datos sean estos privadas o publicas, tomando en cuenta que el Derecho a la Privacidad e Intimidad como derechos fundamentales que complementan el Recurso de Hábeas Data establecido en la Constitución Política del Estado.

c) Ley sobre “Documentos, Firmas y Comercio Electrónico”

En Bolivia, en el años 2009 se aprobó el proyecto de **ley sobre “Documentos, Firmas y Comercio Electrónico”,** con el objetivo de facilitar el trámite en los diferentes

ámbitos de la administración. Esta ley entró en vigencia desde 18 meses después de su aprobación y no cambia la estructura del derecho existente.

El proyecto de ley que fuera aprobado en grande el 21 de agosto de 2007 tiene como objeto reconocer el valor jurídico y probatorio de los mensajes de datos, documento electrónico, firma electrónica, contratación electrónica, así como el comercio electrónico, incluyendo modificaciones al Código Penal sobre la utilización de los medios electrónicos y a los delitos informáticos.

Según los entendidos este proyecto de ley no cambia la estructura del Derecho existente, simplemente reconoce el valor jurídico y probatorio de un nuevo soporte el "soporte electrónico", es así que se respetan los Códigos Civil y Comercial y sólo se incluyen modificaciones al Código Penal, incluyendo al correo electrónico, documento electrónico, medios electrónicos y nuevos delitos informáticos.

Al igual que como se hacia con la información contenida en soporte papel, es importante conocer los nuevos términos que se empezarán a manejar, es así que el documento escrito pasa a ser el documento electrónico, la firma manuscrita (firma electrónica), la Cédula de Identidad o Pasaporte para identificarse (Certificado Electrónico), algunos contratos en presencia física del Notario de Fe Pública (documento público electrónico), la contratación entre personas presentes (contratación electrónica) y el comercio tradicional (comercio electrónico).

Este nuevo soporte conocido de forma genérica como "medios electrónicos" (computadora, Internet, celular, fax, televisión, entre otros) van a permitir agilizar y hacer más eficientes nuestros trámites en los ámbitos de la Administración Pública (diversos trámites en línea), Administración de Justicia (notificaciones electrónicas a un correo electrónico si se fija como domicilio), ámbito financiero (banca electrónica o telebanca, desmaterialización de documentos), ámbito tributario (presentación de

impuestos por Internet, factura electrónica), ámbito comercial (contratación electrónica, vender a cualquier parte del mundo), entre otros.

Hoy en día se está realizando contratación electrónica y utilizando documentos electrónicos al retirar dinero de cualquier cajero automático con nuestra tarjeta de débito o crédito, o al pagar con las mismas en un supermercado o negocio que aceptan el pago con tarjeta.

Con este sistema se puede tener presencia a nivel mundial al contar con un sitio web a través del cual se podrá vender productos, ya sean bienes o servicios, ahorrando en costos de pagar el alquiler de una oficina, luz, agua, secretaria, etc.

La nueva ley de Documentos, Firmas y Comercio Electrónico provee de seguridad en el marco de las transacciones que se realizan a través de medios electrónicos en cualquier ámbito. Se tiene previsto que una vez aprobada la ley, se contará con un plazo de hasta dieciocho meses para la difusión de la misma al sector público (Administración Central, Departamental y Local y al Poder Judicial), sector privado y sociedad civil (Colegios de Abogados, Notarios, Ingenieros, entre otros).

La Ley de Documentos, Firmas y Comercio Electrónico se ha aprobado por unanimidad en el Congreso Boliviano en el mes de agosto de 2007, pero no se han encontrado referencias sobre su publicación en la Gaceta Oficial.

La presente Ley tiene por objeto reconocer el valor jurídico y probatorio de:

- Los actos jurídicos celebrados mediante medios electrónicos u otros de mayor avance tecnológico realizados por personas naturales, jurídicas, empresas colectivas o unipersonales, comunidades de bienes y otras entidades que constituyan una unidad económica sujeta a derechos y obligaciones.

- El uso de firmas electrónicas debidamente certificadas por una Entidad de Certificación acreditada bajo lo estipulado en la presente ley.
- Los actos civiles y comerciales que utilicen directa o indirectamente medios electrónicos u otros de mayor avance tecnológico para realizar actividades del comercio electrónico.

Los principios y normas establecidas en esta Ley se aplican a los actos jurídicos otorgados o celebrados a través de mensajes de datos y documentos electrónicos que den origen a contratos, operaciones o servicios. Igualmente, será aplicable a todo tipo de información que tenga relación con la naturaleza de los servicios de la sociedad de la información utilizada en el contexto de actividades del comercio electrónico. Las disposiciones contenidas en esta Ley no alteran, sino complementan las normas relativas a la celebración, formalización, validez, eficacia y extinción de los contratos y cualquier otro acto jurídico efectuado por medios electrónicos u otro de mayor avance tecnológico. Tampoco altera las normas relativas al tipo de instrumento en que deba constar un acto jurídico.

Las disposiciones de esta Ley se aplican en materia tributaria siempre y cuando no contravengan su normativa especial y respondan a los principios, naturaleza y fines de la misma. Quedan excluidas del ámbito de aplicación de esta Ley las actividades realizadas en el marco del sistema de pagos, a través de medios electrónicos u otros de mayor avance tecnológico, correspondiendo al Banco Central de Bolivia establecer el marco normativo que brinde seguridad y operatividad al mismo.

d) La ADSIB (Agencia para el Desarrollo de la Sociedad de la Información en Bolivia)

Es la encargada de proponer políticas, implementar estrategias y coordinar acciones orientadas a reducir la brecha digital en el país, a través del impulso de las Tecnologías de la Información y Comunicación en todos sus ámbitos, teniendo como principal misión

favorecer relaciones del Gobierno con la Sociedad, mediante el uso de tecnologías adecuadas.

El 19 de marzo de 2002, mediante el Decreto Supremo 26553 se crea la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia - ADSIB, entidad descentralizada bajo tuición de la Vicepresidencia de la República de Bolivia. A partir de este Decreto las funciones de la Red Boliviana de Comunicación de Datos - BOLNET son transferidas a la estructura de la ADSIB. El 14 de mayo de 2002, por medio del Decreto Supremo 26624 se reglamenta y ordena el registro de nombres de dominio en Internet en el país, bajo la responsabilidad de BOLNET. En septiembre 21 del 2004 se da un nuevo Decreto Supremo 27739 mediante el cual, la Presidencia del Congreso Nacional asume tuición sobre la ADSIB con lo que es una Agencia TRANSVERSAL entre dos poderes (Legislativo y Ejecutivo).

Lamentablemente, en Bolivia no existen muchas leyes ni artículos que defiendan la informática, comercio electrónico, TIC's, etc.; porque no existen personas que realmente luchen por esto. En Bolivia deberían existir más leyes para este ámbito, ya que es muy necesario.

- **Marco Jurídico Comparado**

ALEMANIA

- Ley y decreto promulgados en materia de firma digital, estableciendo las condiciones para considerar segura una firma digital; acreditación voluntaria de proveedores de servicios de certificación;
- Elaboración de un catálogo de medidas de seguridad adecuadas;
- Consulta pública en cursos sobre los aspectos jurídicos de la firma digital y de los documentos firmados digitalmente.

AUSTRALIA

- Estrategia para la creación de una infraestructura de firma digital que asegure la integridad y autenticidad de las transacciones efectuadas en el ámbito gubernamental y en su relación con el sector privado.
- Prevé la creación de una autoridad pública que administre dicha infraestructura y acredite a los certificadores de clave pública (Proyecto Gatekeeper).

BRASIL

- Proyecto de ley sobre creación, archivo y utilización de documentos electrónicos.-

CHILE

- Proyecto de ley sobre documento electrónico que regula la utilización de la firma y el funcionamiento de los certificadores de clave pública.

ESPAÑA

- Circulares de la dirección de Aduanas sobre utilización de la firma digital;
- Resolución en el ámbito de la seguridad social que regula la utilización de medios digitales;
- Leyes y circulares en materia de hipotecas, fiscalidad, servicios financieros y registros de empresas que autorizan el uso de procedimientos digitales;
- Ley de presupuestos de 1998, por la que la Casa de la Moneda actuará como certificador de clave pública.

EE.UU.

INICIATIVAS DEL GOBIERNO FEDERAL

- Iniciativa sobre la creación de una infraestructura de clave pública para el comercio electrónico.
- Ley que autoriza la utilización de documentación electrónica en la comunicación entre las agencias gubernamentales y los ciudadanos, otorgando a la firma digital igual validez que la firma manuscrita
- Ley que promueve la utilización de documentación electrónica para la remisión de declaraciones del impuesto a las ganancias.
- Proyecto piloto para promover la utilización de la firma digital en las declaraciones impositivas.
- Proyecto de ley de Firma Digital y Autenticación Electrónica para facilitar el uso de las tecnologías de autenticación electrónica por instituciones financieras.
- Proyecto de ley que promueve el reconocimiento de técnicas de autenticación electrónica como alternativa válida en toda comunicación electrónica en el ámbito público o privado.
- Resolución de la Reserva Federal regulando las transferencias electrónicas de fondos.
- Iniciativa del Departamento de Salud proponiendo la utilización de la firma digital en la transmisión electrónica de datos de su jurisdicción.
- Iniciativa del Departamento del Tesoro aceptando la recepción de solicitudes de compra de bonos del gobierno firmados digitalmente.

EE.UU. INICIATIVAS DE LOS GOBIERNOS ESTATALES

- Se destaca la Ley de Firma Digital del Estado de Utah, que fue primer estado en legislar el uso comercial de la firma digital. Regula la

utilización de la criptografía asimétrica y fue diseñada para ser compatible con varios estándares internacionales. Prevé la creación de certificadores de clave pública licenciados por el Departamento de Comercio de Estado. Además protege la propiedad exclusiva de la clave privada del suscriptor del certificado, por lo que su uso no autorizado queda sujeto a responsabilidades civiles y criminales

Ley de firma digital

Tanto Argentina como Brasil están trabajando en aprobar leyes que regulen la firma digital. El presidente de la Comisión de Informática de la Cámara baja argentina, señaló que no hay puntos conflictivos y que la ley podría ser aprobada en breve.

Perú y México aprobaron las leyes de firma digital el 2000, seguidos por Venezuela, quien lo hizo el 2001. Estas leyes se basaron en las directrices presentadas por la Comisión de las Naciones Unidas de Leyes Internacionales de Comercio (Uncitral). Según la firma estadounidense de abogados Morrison & Foerster, especializada en regulaciones de Internet, Uncitral se reunirá para presentar un esbozo de leyes uniformes sobre firmas digitales; esto "acelerará la aprobación de leyes en todo el mundo y las hará más compatibles". EEUU aprobó la ley federal el año 2006; sin embargo, hasta ese entonces alrededor de 40 estados ya tenían su propia legislación sobre el tema. En Europa, la Unión Europea ya aprobó regulaciones de firma digital así como de comercio electrónico.

9. PLANTEAMIENTO DEL PROBLEMA DE LA MONOGRAFÍA

Nuestro escaso desarrollo legislativo respecto de la normativización de los nuevos instrumentos informáticos actualmente empleados para la vinculación comercial y civil, nos presentan la ineludible obligación de elaborar planteamientos tendientes a subsanar la inexistencia de una adecuada reglamentación de los mismos.

A este fin y con el objetivo de integrar nuestra cultura jurídica y judicial al mundo emergente de la informática jurídica y con el ánimo de reavivar la solución a una postergada necesidad, se presenta un resumen sintético de un trabajo elaborado por mi persona.

La investigación a la que se hace referencia aborda la actual problemática que nace del constante desarrollo tecnológico y de las nuevas formas de relacionamiento legal que no han sido adecuadamente sistematizadas, organizadas ni correctamente normadas en la administración nacional.

La ausencia de una normativa expresa relacionada al tema que nos ocupa nos lleva a considerar el manejo alternativo de datos en soportes “no tradicionales”; considerando la definición legal y la formulación de las bases jurídicas del DOCUMENTO ELECTRONICO, su alcance como tal, su validez, eficacia y autenticidad por medio de otro concepto nuevo pero inseparable del primero cual es la FIRMA DIGITAL.

5.1. Problema científico

La formulación del problema científico de la investigación parte de la identificación de un conjunto de caracteres criminológicos con una probabilidad elevada de constituir elementos comunes en los sujetos de interés de la investigación, por la que se define como:

¿Cuáles son las características criminológicas comunes de la firma digital, la figura del delito y el proceso seguido contra estos en el período comprendido entre el año 2009 al 2011 en la Fiscalía de Distrito de la ciudad de La Paz?

La formulación de esta interrogante nos conduce a su vez a plantearnos las siguientes preguntas científicas para dar cumplimiento a los objetivos que nos proponemos para el desarrollo de la investigación:

- ¿Cuál es el fundamento teórico de la caracterización criminológica del delito de falsedad documental, atendiendo a la doctrina y legislación vigente?
- ¿Cuáles son las características criminológicas comunes en la Falsedad documental en los documentos electrónicos en la Fiscalía en el período 2009 al 2010?
- ¿Cuáles son las características criminológicas comunes en cuanto a la figura del delito?
- ¿Cuáles son las características criminológicas comunes en los procesos penales seguidos en la Fiscalía en el período 2009 al 2010?
- ¿Qué fundamentos se tendrán en cuenta para la elaboración de un Plan de Acción para potenciar el enfrentamiento al delito de falsedad documental en los documentos electrónicos?

10. DEFINICIÓN DE LOS OBJETIVOS

10.1. Objetivo General

Llegar a caracterizar criminológicamente los documentos electrónicos y la falsedad documental, la figura de delito y el proceso seguido contra estos en el período comprendido entre el año 2009 al 2011 que contribuyan a contar con un Plan de Acción para su enfrentamiento.

10.2. Objetivos Específicos

- Determinar los lineamientos del marco jurídico referente a la definición legal del Documento Electrónico.

- Establecer su viabilidad como medio probatorio.
- Definir el concepto legal de la Firma Digital.
- Regular el uso y administración de la Firma Digital
- Especificar la importancia mundial como elementos de autentificación y validación.
- Detallar la deficiente regulación del tema en Bolivia.
- Precisar los elementos que imponen su uso general
- Establecer el papel del documento Electrónico frente al Derecho Civil
- Determinar los elementos nuevos que lo componen.
- Especificar el documento electrónico y los elementos que lo enfrentan al documento tradicional.
- Precisar la necesidad de incorporarlo como elemento de uso general y la necesidad de revestirlo de un carácter de autenticidad.
- Puntualizar las características esenciales de la firma digital.
- Precisar la valoración de la firma digital como elemento fundamental para la validación y autentificación de los documentos electrónicos.

11. ESTRATEGIA METODOLÓGICA Y TÉCNICAS DE INVESTIGACIÓN MONOGRÁFICA

El Campo de acción de la investigación lo ocupa las características criminológicas comunes.

En materia de características criminológicas se agrupó en este criterio todos los caracteres socio-jurídicos que permitiesen identificar a los infractores como sujetos de interés, valorando la concordancia entre la muestra seleccionada con relación a la población determinada a través del diagnóstico inicial.

La investigación realizada es un estudio exploratorio ya que gira en torno a determinar cuáles son las características criminológicas comunes. Al mismo tiempo es un estudio

productivo porque facilita una futura definición de lo que puede ser un perfil de los actores del crimen relacionados con este delito teniendo en cuenta lo prescrito normativamente y un plan de acciones para su atención.

7.1. Métodos del nivel teórico

- **Histórico-Lógico**: Este método posibilitó el análisis de los antecedentes históricos del delito a través del análisis documental y legislativo, hasta llegar al estado actual del mismo.

- **Sistémico-Estructural**: Permitió estructurar el sistema de plan de acciones para potenciar el enfrentamiento al delito partiendo de la caracterización.

- **Inductivo-Deductivo**: Permitió llegar a conclusiones acerca de la efectividad del conocimiento de las características criminológicas comunes.

- **Estudio Documental**: Por este método se pudo analizar los diferentes materiales y legislaciones que antecedieron a esta investigación, para detectar los cambios que pudieron producirse antes de la investigación realizada; así como la revisión de expedientes lo cual permitió un análisis detallado con respecto a los datos, pudiendo determinar así las características criminológicas.

7.2. Métodos del nivel empírico

Encuesta: Su aplicación fue dirigida a Jueces Instructores en la materia Penal e investigadores de la Fuerza Especial de Lucha contra el Crimen FELC-C, las mismas están dirigidas a monitorear el criterio de los sujetos vinculados directa y especialmente al enfrentamiento, prevención, investigación y administración de justicia en relación al delito.

Métodos técnicos:

Teórico-Jurídico:

Permitió un análisis detallado de los conceptos que expresan los expertos permitiendo que la autora se auxiliara de las diversas definiciones para su investigación.

Población:

La población objeto de la investigación, es no determinada y compartimentada según las reglas generales de compartimentación, orientadas por la Fiscalía, para las investigaciones de corte criminológico y el procesamiento estadístico de la información sobre las causas penales.

Muestra:

La muestra la componen 20 cuadernos de investigación de la Etapa de la Fiscalía de Distrito de la ciudad de La Paz, 20 denuncias realizadas en la Fuerza Especial de Lucha Contra el Crimen (FELC-C).No se exponen los criterios de selección de la muestra a partir de las reglas generales de compartimentación, orientadas por la Corte Superior de Justicia para las investigaciones de corte criminológico y el procesamiento estadístico de la información sobre las causas penales.

CAPITULO II
LOS DOCUMENTOS ELECTRÓNICOS

Hemos escuchado miles de definiciones y conceptos sobre este tipo de documentos y se ha debatido sobre su valor probatorio en la nueva era tecnológica.

Es por eso que se me ha ocurrido explicar un poco sobre este tema y mostrar las diferentes concepciones que adoptan distintos países. Los documentos soportados en medios magnéticos no responden al concepto tradicional o restringido de documento manuscrito en soporte papel, sino al amplio. Por exclusión, entendemos que constituye un documento no electrónico aquel que es elaborado por las formas tradicionales, sean éstas manuales, mecanográficas, micrograbadas, microcopiadas o fotográficas.

1. DEFINICIÓN

El documento electrónico debe entenderse como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

2. CONCEPTO EN LA LEGISLACIÓN DE ALGUNOS PAÍSES

México: El documento electrónico o informático, se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática.

España: "Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios gozarán de la validez y eficacia de documento original siempre que quede garantizada

su autenticidad, integridad, conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de la garantías y requisitos exigidos por leyes."

Francia: "Los documentos emitidos, cualquiera sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que estas emitan como copias de originales almacenados por estos mismos medios, gozarán de validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación".

Francia es uno de los países pioneros en este campo. La ley 80/525 del 12 de julio de 1980 introdujo un trascendente cambio en el artículo 1348 de su Código Civil. En efecto, desde ese momento se estableció que el documento electrónico tendría el mismo valor probatorio que el documento en soporte papel escrito y firmado, cuando cumpliera determinados requisitos que son la inalterabilidad y la durabilidad. Son legislaciones que, con algunas fallas, se muestran avanzadas en cuanto al reconocimiento de la realidad que es palpable hoy y que lo era menos hace pocos años.

Chile: El concepto de "Documento Electrónico" es toda representación informática que da testimonio de un hecho. También sostienen que la "Firma digital" es el código informático que permite determinar la autenticidad de un documento electrónico y su integridad, impidiendo a su transmisor desconocer la autoría del mensaje en forma posterior. En este orden de cosas no está de agregar el concepto de "Firma Digital" que es una especie de firma electrónica que resulta de un proceso informático validado, implementado a través de un sistema criptográfico de claves públicas y privadas.

O.N.U: Finalmente es de destacar la actitud adoptada por las Naciones Unidas (a través de la UNCITRAL) quien, reconociendo las dificultades de que se llegue mediante la negociación a un acuerdo internacional sobre la materia, se ha decantado a favor de una rápida adecuación de las legislaciones de cada país como medida de carácter más pragmático. Es de señalar que este organismo ha emitido un valioso documento,

titulado Legal Value of Computer Records, en el que se expresa que las normas o reglas concernientes a las pruebas relativas a documentos electrónicos (si bien dice registros de computadora) no deben suponer un obstáculo para el uso de las tecnologías emergentes tanto a nivel doméstico como internacional. Y señala que las normas redactadas por algunos países deben superar los problemas que genera el lenguaje empleado pues incorpora referencias culturales que todavía suponen un freno al desarrollo. Igualmente el esfuerzo de los diferentes países no es suficiente ni tiene la velocidad con la que se está desarrollando este fenómeno en la práctica. Este término, velocidad, ha adquirido una importancia fundamental por cuanto implica, en temas tecnológicos la adaptación al medio con ventaja sobre el resto, lo que trae aparejado, a escala mundial, una atracción de recursos, inversiones, capitales y sobre todo de actividad (Activación de la economía).

CAPITULO III
FIRMA ELECTRONICA, FIRMA DIGITAL, CERTIFICADOS ELECTRONICOS Y DIGITALES

1. LA FIRMA CONVENCIONAL

La firma es una palabra, o pequeño mensaje o dibujo, que tiene como fin identificar y asegurar o autentificar la identidad de un autor o remitente, o como una prueba del consentimiento y/o de verificación de la integridad y aprobación de la información contenida en un documento o similar.

La firma tradicionalmente se ha realizado de forma manuscrita y es la forma más habitual de certificar el consentimiento de forma escrita. Mediante este sistema, el firmante escribe una palabra y una serie de trazas personales que lo identifican como tal. En caso de duda un Perito Calígrafo podría determinar si una firma pertenece a una determinada persona o si se trata de una falsificación, una automodificación, etc. A través de este tipo de firma, un grafólogo además postula que puede analizar determinados rasgos de la personalidad de un individuo.

2. LA FIRMA DIGITAL

Firma digital es una tecnología que produce los mismos efectos jurídicos que la "firma autógrafa" de un documento físico, siendo también admisible como prueba en juicio, en función de la legislación de cada país. Esta tecnología se basa en la criptografía. Mediante unos mecanismos criptográficos, se lleva a cabo la firma y la posterior confirmación y validación de dicha firma y que es en nombre y apellido de la persona

Se dice firma digital a un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Una firma digital da al destinatario

seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión.

Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación. Consiste en un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

Los términos de firma digital y firma electrónica se utilizan con frecuencia como sinónimos, pero este uso en realidad es incorrecto.

Mientras que firma digital hace referencia a una serie de métodos criptográficos, firma electrónica es un término de naturaleza fundamentalmente legal y más amplia desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos.

Un ejemplo claro de la importancia de esta distinción es el uso por la Comisión europea. En el desarrollo de la Directiva europea 1999/93/CE que establece un marco europeo común para la firma electrónica empezó utilizando el término de firma digital en el primer borrador, pero finalmente acabó utilizando el término de firma electrónica para desacoplar la regulación legal de este tipo de firma de la tecnología utilizada en su implementación.

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

- Vigencia del certificado digital del firmante,
- Revocación del certificado digital del firmante (puede ser por OCSP o CRL),
- Inclusión de sello de tiempo.

¿Qué es y para qué sirve la firma digital?

La firma digital puede ser definida como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo (fórmula matemática) de cifrado asimétrico o de clave pública, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje. Desde un punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

La aparición y desarrollo de las redes telemáticas, de las que internet es el ejemplo más notorio, ha supuesto la posibilidad de intercambiar entre personas distantes geográficamente mensajes de todo tipo, incluidos los mensajes de contenido contractual. Estos mensajes plantean el problema de acreditar tanto la autenticidad como la autoría de los mismos.

Concretamente, para que dos personas (ya sean dos empresarios o un empresario y un consumidor) puedan intercambiar entre ellos mensajes electrónicos de carácter comercial que sean mínimamente fiables y puedan, en consecuencia, dar a las partes contratantes la confianza y la seguridad que necesita el tráfico comercial, esos mensajes deben cumplir los siguientes requisitos:

1º.- **Identidad**, que implica poder atribuir de forma indubitada el mensaje electrónico recibido a una determinada persona como autora del mensaje.

2º.- **Integridad**, que implica la certeza de que el mensaje recibido por B (receptor) es exactamente el mismo mensaje emitido por A (emisor), sin que haya sufrido alteración alguna durante el proceso de transmisión de A hacia B.
3º.- **No repudiación** o no rechazo en origen, que implica que el emisor del mensaje (A) no pueda negar en ningún caso que el mensaje ha sido enviado por él.

Pues bien, la firma digital es un procedimiento técnico que basándose en técnicas criptográficas trata de dar respuesta a esa triple necesidad apuntada anteriormente, a fin de posibilitar el tráfico comercial electrónico.

Por otra parte, a los tres requisitos anteriores, se une un cuarto elemento, que es la confidencialidad, que no es un requisito esencial de la firma digital sino accesorio de la misma. La confidencialidad implica que el mensaje no haya podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión del mismo.

¿En qué se basa la firma digital?

La criptografía como base de la firma digital.

La firma digital se basa en la utilización combinada de dos técnicas distintas, que son la criptografía asimétrica o de clave pública para cifrar mensajes y el uso de las llamadas funciones hash o funciones resumen.

El diccionario de la Real Academia Española de la Lengua define la criptografía como "el arte de escribir con clave secreta o de forma enigmática". La criptografía es un conjunto de técnicas que mediante la utilización de algoritmos y métodos matemáticos sirven para cifrar y descifrar mensajes. La criptografía ha venido siendo utilizada desde antiguo, fundamentalmente con fines militares. Tradicionalmente se ha hablado de dos

tipos de sistemas criptográficos: los simétricos o de clave privada y los asimétricos o de clave pública.

Los llamados sistemas criptográficos simétricos son aquellos en los que dos personas (A y B), que van a intercambiarse mensajes entre sí, utilizan ambos la misma clave para cifrar y descifrar el mensaje. Así, el emisor del mensaje (A), lo cifra utilizando una determinada clave, y una vez cifrado, lo envía a B. Recibido el mensaje, B lo descifra utilizando la misma clave que usó A para cifrarlo. Los sistemas criptográficos simétricos más utilizados son los conocidos con los nombres de DES, TDES y AES.

Los principales inconvenientes del sistema simétrico son los siguientes:

- La necesidad de que A (emisor) y B (receptor) se intercambien previamente por un medio seguro la clave que ambos van a utilizar para cifrar y descifrar los mensajes.
- La necesidad de que exista una clave para cada par de personas que vayan a intercambiarse mensajes cifrados entre sí.

Las dos dificultades apuntadas determinan que los sistemas de cifrado simétricos no sean aptos para ser utilizados en redes abiertas como internet, en las que confluye una pluralidad indeterminada de personas que se desconocen entre sí y que en la mayoría de los casos no podrán intercambiarse previamente claves de cifrado por ningún medio seguro.

Los sistemas criptográficos asimétricos o de clave pública se basan en el cifrado de mensajes mediante la utilización de un par de claves diferentes (privada y pública), de ahí el nombre de asimétricos, que se atribuyen a una persona determinada y que tienen las siguientes características:

- Una de las claves, la privada, permanece secreta y es conocida únicamente por la persona a quien se ha atribuido el par de claves y que la va a utilizar para cifrar mensajes. La segunda clave, la pública, es o puede ser conocida por cualquiera.
- Ambas claves, privada y pública, sirven tanto para cifrar como para descifrar mensajes.
- A partir de la clave pública, que es conocida o puede ser conocida por cualquiera, no se puede deducir ni obtener matemáticamente la clave privada, ya que si partiendo de la clave pública, que es puede o ser conocida por cualquier persona, se pudiese obtener la clave privada, el sistema carecería de seguridad dado que cualquier podría utilizar la clave privada atribuida a otra persona pero obtenida ilícitamente por un tercero partiendo de la clave pública.

Este dato se basa en una característica de los números primos y en el llamado problema de la factorización. El problema de la factorización es la obtención a partir de un determinado producto de los factores cuya multiplicación ha dado como resultado ese producto. Los números primos (números enteros que no admiten otro divisor que no sea el 1 o ellos mismos), incluidos los números primos grandes, se caracterizan porque si se multiplica un número primo por otro número primo, da como resultado un tercer número primo a partir del cual es imposible averiguar y deducir los factores.

El criptosistema de clave pública más utilizado en la actualidad es el llamado RSA, creado en 1978 y que debe su nombre a sus tres creadores (Rivest, Shamir y Adleman).

La utilización del par de claves (privada y pública) implica que A (emisor) cifra un mensaje utilizando para ello su clave privada y, una vez cifrado, lo envía a B (receptor). B descifra el mensaje recibido utilizando la clave pública de A. Si el mensaje descifrado es legible e inteligible significa necesariamente que ese mensaje ha sido cifrado con la

clave privada de A (es decir, que proviene de A) y que no ha sufrido ninguna alteración durante la transmisión de A hacia B, porque si hubiera sido alterado por un tercero, el mensaje descifrado por B con la clave pública de A no sería legible ni inteligible. Así se cumplen dos de los requisitos anteriormente apuntados, que son la integridad (certeza de que el mensaje no ha sido alterado) y no repudiación en origen (imposibilidad de que A niegue que el mensaje recibido por B ha sido cifrado por A con la clave privada de éste). El tercer requisito (identidad del emisor del mensaje) se obtiene mediante la utilización de los certificados digitales, que se analizan en otro apartado de esta guía.
Las funciones Hash.

Junto a la criptografía asimétrica se utilizan en la firma digital las llamadas funciones hash o funciones resumen. Los mensajes que se intercambian pueden tener un gran tamaño, hecho éste que dificulta el proceso de cifrado. Por ello, no se cifra el mensaje entero sino un resumen del mismo obtenido aplicando al mensaje una función hash. Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función hash en un mensaje con una dimensión fija (generalmente de 160 bits). Para ello, el mensaje originario se divide en varias partes cada una de las cuales tendrá ese tamaño de 160 bits, y una vez dividido se combinan elementos tomados de cada una de las partes resultantes de la división para formar el mensaje-resumen o hash, que también tendrá una dimensión fija y constante de 160 bits.Este resumen de dimensión fija es el que se cifrará utilizando la clave privada del emisor del mensaje.

Los sellos temporales

Finalmente, en el proceso de intercambio de mensajes electrónicos es importante que, además de los elementos o requisitos anteriormente analizados, pueda saberse y establecerse con certeza la fecha exacta en la que los mensajes han sido enviados. Esta característica se consigue mediante los llamados sellos temporales o "time stamping", que es aquella función atribuida generalmente a los Prestadores de

Servicios de Certificación mediante la cual se fija la fecha de los mensajes electrónicos firmados digitalmente.

La confidencialidad de los mensajes

En ocasiones, además de garantizar la procedencia de los mensajes electrónicos que se intercambian por medio de internet y la autenticidad o integridad de los mismos, puede ser conveniente garantizar también su confidencialidad. Ello implica tener la certeza de que el mensaje enviado por A (emisor) únicamente será leído por B (receptor) y no por terceras personas ajenas a la relación que mantienen A y B.

En tales casos, también se acude al cifrado del mensaje con el par de claves, pero de manera diferente al mecanismo propio y característico de la firma digital. Para garantizar la confidencialidad del mensaje, el cuerpo del mismo (no el hash o resumen) se cifra utilizando la clave pública de B (receptor), quien al recibir el mensaje lo descifrará utilizando para ello su clave privada (la clave privada de B). De esta manera se garantiza que únicamente B pueda descifrar el cuerpo del mensaje y conocer su contenido.

3. LA FIRMA ELECTRÓNICA

La firma electrónica es un concepto directamente relacionado con la firma digital, sin embargo no son lo mismo, a pesar del extendido uso indistinto y de una utilización léxica y práctica muy similar de estos dos conceptos. A pesar del uso indistinto que se le suele dar a los dos términos, cada vez más, entre los profesionales y expertos del tema se hace una clara diferenciación entre estos.

La firma electrónica, como la firma hológrafa (autógrafa, manuscrita), puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído y, en su defecto mostrar el tipo de firma y

garantizar que no se pueda modificar su contenido. La firma electrónica surge de la necesidad de las empresas y administraciones de reducir los costes y aumentar la seguridad de sus procesos internos. Uno de los métodos de firma electrónica es la firma electrónica escrita que consiste en la captación de la firma física mediante un dispositivo de firmas, llamado pad de firmas.

Para realizar la firma electrónica escrita son necesarios el hardware y software apropiados.

Definición

La firma electrónica de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, al contenido. Esta función hash asocia un valor dentro de un conjunto finito (generalmente los números naturales) a su entrada. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi unívocamente al texto en concreto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar el resultado con el que ha recibido. No obstante esto presenta algunas dificultades.

Una firma electrónica es una firma digital que se ha almacenado en un soporte de hardware; mientras que la firma digital se puede almacenar tanto en soportes de hardware como de software. La firma electrónica reconocida tiene el mismo valor legal que la firma manuscrita.

De hecho se podría decir que una firma electrónica es una firma digital contenida o almacenada en un contenedor electrónico, normalmente un chip de ROM. Su principal característica diferenciadora con la firma digital es su cualidad de ser inmodificable (que no inviolable). No se debe confundir el almacenamiento en hardware, como por ejemplo, en un chip, con el almacenamiento de la firma digital en soportes físicos; es posible almacenar una firma digital en una memoria flash, pero al ser esta del tipo RAM

y no ROM, no se consideraría una firma electrónica si no una firma digital contenida en un soporte físico.

Ejemplos de Firma Electrónica

La firma digital contenida en soportes de tipo ROM tiene ya hoy en día un uso muy extendido y se utiliza en gran cantidad de tarjetas de acceso, tarjetas de telefonía, RFID o cualquier otra actividad en la que es preciso identificar inequívocamente una persona u objeto. Una de las aplicaciones mas destacadas a nivel mundial es El DNI electrónico español, también conocido como DNIE que, al ser de uso obligado, ya dispone de varios millones de usuarios.

Características y usos especiales de la firma electrónica

Las características y usos de la Firma electrónica son exactamente los mismos que los de la Firma digital con la única diferenciación del tipo de soporte en el que se almacenan. Su condición de inmodificable aporta un grado superior de seguridad, si bien la ausencia habitual de contraseñas de seguridad que protejan su uso permitiría que un portador ilegítimo pudiese suplantar al propietario con facilidad.

Las posibilidades de red en la firma electrónica

Para que sea de utilidad, la función hash debe satisfacer dos importantes requisitos. Primero, debe ser difícil encontrar dos documentos cuyo valor para la función "hash" sea igual. Segundo, dado uno de estos valores, debería ser difícil recuperar el documento que lo ha producido.

Algunos sistemas de codificación de clave pública se pueden usar para firmar documentos. El firmante cifra o codifica el documento con su clave privada y cualquiera

que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrarla.

Existen funciones "hash" especialmente designadas para satisfacer estas dos importantes propiedades. SHA y MD5 son ejemplos de este tipo de algoritmos. Para usarlos un documento se firma con una función "hash", cuyo resultado es la firma. Otra persona puede comprobar la firma mediante la misma función a su copia del documento y comparando el resultado con el del documento original. Si concuerdan, es prácticamente seguro que los documentos sean idénticos.

El problema radica en usar una función "hash" para firmas digitales que no permita que un "atacante" interfiera en la comprobación de la firma. Si el documento y la firma se enviaran sin cifrar este individuo podría modificar el documento y generar una firma correspondiente sin que lo supiera el destinatario. En caso de que sólo se cifrara el documento, un atacante podría manipular la firma y hacer que la comprobación de ésta fallara. Una tercera opción es usar un sistema de codificación híbrido para cifrar tanto la firma como el documento. El firmante usará su clave privada, y cualquiera puede usar su clave pública para comprobar la firma y el documento. Esto quizás suene bien, pero en realidad no tiene sentido. Si este algoritmo hiciera el documento seguro también lo aseguraría de manipulaciones, y no habría necesidad de firmarlo. El problema más grave es que esto no protege de manipulaciones ni a la firma, ni al documento. Con este método, tan sólo la clave de sesión del sistema de cifrado simétrico se cifra usando la clave privada del firmante. Cualquiera puede usar la clave pública y recuperar la clave de la sesión. Por tanto, resulta obvio usarla para cifrar documentos substitutos y firmas para enviarlas a terceros en nombre del remitente.

La solución

Un algoritmo efectivo tendrá que hacer uso de un sistema de clave pública para cifrar solo la firma. En particular, el valor "hash" se cifrará mediante el uso de la clave privada

del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se podrá enviar usando cualquier otro algoritmo de cifrado, o incluso ninguno si es un documento público. En caso de que el documento se modifique, la comprobación de la firma fallará, pero esto es precisamente lo que la verificación se supone que debe descubrir. El Digital Signature Algorithm es un algoritmo de firma de clave pública que funciona como hemos descrito. DSA es el algoritmo principal para la firma que se usa en GnuPG.

La firma electrónica escrita

Una de las formas de firma electrónica escrita es mediante pads, dispositivos para la captación de la firma escrita. Estos dispositivos pueden aplicarse para digitalizar gran parte de los procesos internos de la empresa e incluso algunos externos.

- Así por ejemplo, gran parte de los procesos internos en los que sea necesaria la firma (autorizaciones, recibos, pedidos, contratos, etc.) podrán hacerse
1º sin imprimir el documento en papel y
2º sin tener, a continuación, que organizar y almacenar físicamente el documento.
Y claro está, el día que se quiera encontrar uno de estos documentos, no habrá más que introducir el nombre del documento en el ordenador, en lugar de bajar al sótano o almacén a buscar el archivo. Así, la firma electrónica escrita, de momento, ya tiene dos claras ventajas: ahorro (tiempo y materiales) y cuidado del medioambiente.

En cuanto a los procesos externos, el dispositivo para la firma electrónica entra en juego en la firma de contratos y documentos por el cliente. El cliente firmará como siempre sobre el papel, que estará sobre nuestro pad o "tablero" de firmas. De esta forma el cliente tendrá su copia firmada sobre el papel y la empresa la suya firmada electrónicamente. Aquí, podemos incluir a las dos anteriores una ventaja más, la imagen. Una imagen de empresa moderna y concienciada con el medioambiente.

Ventajas de la firma electrónica escrita

- Mediante la firma electrónica escrita se suprime el choque de medios, es decir se evita la impresión en papel para la firma.
- Como la firma escrita es intransferible, la firma electrónica escrita es una forma de identificación que al contrario que las contraseñas y llaves no se puede robar ni olvidar.
- La firma es sin duda un acto voluntario.
- La firma es un proceso reconocido y aceptado por todos que da constancia de un acuerdo voluntario.
- El sujeto firmante no tiene que ser socio de ninguna compañía certificadora para poder utilizar la firma electrónica escrita.
- La firma capturada mediante la firma electrónica escrita puede ser examinada por expertos grafólogos (comparando, por ejemplo, la firma electrónica contra otra realizada sobre papel).

Para la firma electrónica escrita necesitará:

Un pad o dispositivo de firma electrónica que sea capaz de capturar o registrar la firma escrita y todos sus aspectos, tales como tiempo, presión y trazado. También necesitará un programa capaz de codificar la firma electrónica de modo seguro y asimétrico en un documento electrónico con poder probatorio. El sistema que utilice habrá de ser capaz de captar y guardar la firma escrita de modo que, en caso de juicio, y a pesar de tratarse de una firma electrónica, un grafólogo pueda verificar su autenticidad.

Firma Electrónica Móvil

Un usuario de Internet que haya obtenido el certificado electrónico denominado Firma Electrónica Móvil, puede realizar todo tipo de trámites de forma que queda garantizada

su verdadera identidad. Además permite firmar electrónicamente formularios y documentos electrónicos con la misma validez jurídica que si firmara con su "puño y letra" el mismo documento en papel. Para la obtención del mismo tan sólo deberá disponer de un certificado electrónico FNMT, una tarjeta SIM habilitada para Firma Electrónica Móvil que deberá proporcionar el operador de telefonía móvil y un teléfono móvil que soporta la firma electrónica (como ocurre con los más modernos).

4. REGULACIÓN DE LA FIRMA DIGITAL EN DIFERENTES PAÍSES

El marco común de firma electrónica de la Unión Europea

El mercado interior de la Unión Europea implica un espacio sin fronteras interiores en el que está garantizada la libre circulación de mercancías. Deben satisfacerse los requisitos esenciales específicos de los productos de firma electrónica a fin de garantizar la libre circulación en el mercado interior y fomentar la confianza en la firma electrónica. En ese sentido la Directiva 1999/93/CE sienta un marco común para la firma electrónica que se concretó con la transposición de la Directiva a las diferentes legislaciones nacionales de los países miembros.

Ley sobre firma electrónica en México

Esta ley fue publicada el 15 de septiembre del año 2003 por el Ministerio Secretaría General de la Presidencia, la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, reconoce que los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica simple. Igualmente señala que estos actos, contratos y documentos, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos en soporte de papel.

Firma Digital en Costa Rica

En Costa Rica, la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley 8454) es firmada el 22 de agosto del 2005. Esta Ley faculta la posibilidad de vincular jurídicamente a los actores que participan en transacciones electrónicas, lo que permite llevar al mundo virtual transacciones o procesos que anteriormente requerían el uso de documentos físicos para tener validez jurídica, bajo el precepto de presunción de autoría y responsabilidad, además lo anterior sin demérito del cumplimiento de los requisitos de las formalidades legales según negocio jurídico.

La ley de firma electrónica en España

En España existe la Ley 59/2003, de Firma electrónica, que define tres tipos de firma:
Simple. Datos que puedan ser usados para identificar al firmante (autenticidad)
Avanzada. Además de identificar al firmante permite garantizar la integridad del documento y la integridad de la clave usada, utilizando para ello un DSCF (dispositivo seguro de creación de firma, el DNI electrónico). Se emplean técnicas de PKI.

Reconocida. Es la firma avanzada y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante). En ocasiones, esta firma se denomina cualificada por traducción del término inglés qualified que aparece en la Directiva Europea de Firma Electrónica.

Firma Electrónica en Guatemala

En Guatemala, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas (Decreto 47-2008), fue publicada en el diario oficial el 23 de septiembre de 2008.

El Ministerio de Economía de ese país tiene bajo su responsabilidad el regular este tema, y abrió en el mes de Junio de 2009 el Registro de Prestadores de Servicios de Certificación, publicando su sitio web con copia de la ley e información importante sobre el tema.

Firma Digital en Nicaragua

El 2 de julio de 2010 se aprobó en Nicaragua la Ley de Firma Electrónica, siendo la Dirección General de Tecnología, adscrita al Ministerio de Hacienda y Crédito Público, la entidad acreditadora de la firma electrónica. Sin embargo, la implementación de dicha Ley, será dentro de un año calendario, contado a partir del 30 de agosto de 2010.

La Ley de firma digital en Perú

En el Perú se ha dictado la Ley de Firmas y Certificados Digitales (Ley 27269), la cual regula la utilización de la firma electrónica, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Firma Electrónica en la República Dominicana

En la República Dominicana, la Ley 126-02 de Comercio Electrónico, Documentos y Firmas Digitales, de fecha 29 de septiembre de 2002, regula toda relación comercial, estructurada a partir de la utilización de uno o más documentos digitales o mensajes de datos o de cualquier otro medio similar. Y se designa al Instituto Dominicano de las Telecomunicaciones (INDOTEL) como el Órgano Regulador.

5. APLICACIONES DE LA FIRMA DIGITAL

La firma digital se puede aplicar en las siguientes situaciones:

- E-mail
- Contratos electrónicos
- Procesos de aplicaciones electrónicos
- Formas de procesamiento automatizado
- Transacciones realizadas desde financieras alejadas
- Transferencia en sistemas electrónicos, por ejemplo si se quiere enviar un mensaje para transferir $100,000 de una cuenta a otra. Si el mensaje se quiere pasar sobre una red no protegida, es muy posible que algún adversario quiera alterar el mensaje tratando de cambiar los $100,000 por 1000,000,con esta información adicional no se podrá verificar la firma lo cual indicará que ha sido alterada y por lo tanto se denegará la transacción
- En aplicaciones de negocios, un ejemplo es el Electronic Data Interchange (EDI) intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios

En sistemas legislativos, es a menudo necesario poner un grupo fecha / hora a un documento para indicar la fecha y la hora en las cuales el documento fue ejecutado o llegó a ser eficaz. Un grupo fecha / hora electrónico se podría poner a los documentos en forma electrónica y entonces firmado usando al DSA o al RSA. Aplicando cualquiera de los dos algoritmos al documento protegería y verificaría la integridad del documento y de su grupo fecha / hora.

La firma digital se aplica además de lo anterior en:

- Mensajes con autenticidad asegurada
- Mensajes sin posibilidad de repudio
- Contratos comerciales electrónicos
- Factura Electrónica
- Desmaterialización de documentos

- Transacciones comerciales electrónicas
- Invitación electrónica
- Dinero electrónico
- Notificaciones judiciales electrónicas
- Voto electrónico
- Decretos ejecutivos (gobierno)
- Créditos de seguridad social
- Contratación pública
- Sellado de tiempo

6. LOS CERTIFICADOS DIGITALES

La utilización del par de claves (privada y pública) para cifrar y descifrar los mensajes permite tener la certeza de que el mensaje que B recibe de A y que descifra con la clave pública de A, no ha sido alterado y proviene necesariamente de A. Pero ¿quién es A?. Para responder de la identidad de A (emisor) es necesario la intervención de un tercero, que son los llamados Prestadores de Servicios de Certificación, cuya misión es la de emitir los llamados certificados digitales o certificados de clave pública.

Un certificado digital es un archivo electrónico que tiene un tamaño máximo de 2 Kilobytes y que contiene los datos de identificación personal de A (emisor de los mensajes), la clave pública de A y la firma privada del propio Prestador de Servicios de Certificación. Ese archivo electrónico es cifrado por la entidad Prestadora de Servicios de Certificación con la clave privada de ésta. Los certificados digitales tienen una duración determinada, transcurrida la cual deben ser renovados, y pueden ser revocados anticipadamente en ciertos supuestos (por ejemplo, en el caso de que la clave privada, que debe permanecer secreta, haya pasado a ser conocida por terceras personas no autorizadas para usarla).

Gracias al certificado digital, el par de claves obtenido por una persona estará siempre vinculado a una determinada identidad personal, y si sabemos que el mensaje ha sido cifrado con la clave privada de esa persona, sabremos también quién es la persona titular de esa clave privada.

Un certificado digital (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad (por ejemplo: nombre, dirección y otros aspectos de identificación) y una clave pública.

Este tipo de certificados se emplea para comprobar que una clave pública pertenece a un individuo o entidad. La existencia de firmas en los certificados aseguran por parte del firmante del certificado (una autoridad de certificación, por ejemplo) que la información de identidad y la clave pública perteneciente al usuario o entidad referida en el certificado digital están vinculadas.

Un aspecto fundamental que hay que entender es que el certificado para cumplir la función de identificación y autenticación necesita del uso de la clave privada (que sólo el titular conoce). El certificado y la clave pública se consideran información no sensible que puede distribuirse perfectamente a terceros. Por tanto el certificado sin más no puede ser utilizado como medio de identificación, cumple esa función cuando se usa para comprobar que una determinada clave privada pertenece a un sujeto.

El ejemplo por excelencia es la firma electrónica: aquí el titular tiene que utilizar su clave privada para crear una firma electrónica. A esta firma se le adjuntará el certificado. El receptor del documento que quiera comprobar la autenticidad de la identidad del firmante necesitará la clave pública que acompaña al certificado para que a través de una serie de operaciones criptográfica se compruebe que es la pareja de la clave

privada utilizada en la firma. Es esta operación de asociación al dato secreto del firmante lo que hará la función de comprobar su identidad.

Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El certificado contiene usualmente lo siguiente:

- el nombre de la entidad certificada,
- número de serie,
- fecha de expiración del certificado,
- una copia de la clave pública del titular del certificado (esta clave es utilizada para la verificación de su firma digital)

Esta información se firma de forma digital por la autoridad emisora del certificado. De esa forma, el receptor puede verificar que esta última ha establecido realmente la asociación.

Formato de certificado digital

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.

- Fecha de emisión y expiración del certificado.

Emisores de certificados

Cualquier individuo o institución puede generar un certificado digital, pero si éste emisor no es reconocido por quienes interactúen con el propietario del certificado, el valor del mismo es prácticamente nulo. Por ello los emisores deben acreditarse: así se denomina al proceso por el cuál entidades reconocidas, generalmente públicas, otorgan validez a la institución certificadora, de forma que su firma pueda ser reconocida como fiable, transmitiendo esa fiabilidad a los certificados emitidos por la citada institución.

La gran mayoría de los emisores tiene fines comerciales, y otros, gracias al sistema de anillo de confianza pueden otorgar gratuitamente certificados en todo el mundo, como: CAcert.org, emisor administrado por la comunidad con base legal en Australia.

Pero para que un certificado digital tenga validez legal, el prestador de Servicios de Certificación debe acreditarse en cada país de acuerdo a la normativa que cada uno defina.

Encargados de autorizar la creación de una autoridad de certificación o prestador de servicios de certificación de algunos países hispanos son:

- En Chile, el Ministerio de Economía.
- En Colombia, la Sociedad Camaral de Certificación Digital Certicámara y GSE Gestión de Seguridad Electrónica.
- En Costa Rica, el Ministerio de Ciencia y Tecnología, bajo el Sistema Nacional de Certificación Digital.
- En Ecuador, el Banco Central del Ecuador.

- En España, la Fábrica Nacional de Moneda y Timbre, el Ministerio de Industria, Turismo y Comercio, la Agència Catalana de Certificació, la Autoritat de Certificació de la Comunitat Valenciana, etc.
- En Guatemala, el Ministerio de Economía.
- En México, la Secretaría de Economía.
- En Perú, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
- En la República Dominicana, el Instituto Dominicano de las Telecomunicaciones.
- En Uruguay, la Administración Nacional de Correos (ANC - Correo Uruguayo).
- En Venezuela, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

7. EL CERTIFICADO ELECTRÓNICO

Un Certificado Electrónico es un conjunto de datos que permiten la identificación del titular del Certificado, intercambiar información con otras personas y entidades, de manera segura, y firmar electrónicamente los datos que se envían de tal forma que se pueda comprobar su integridad y procedencia.

El Certificado Electrónico garantiza:

- La autenticidad de las personas y entidades que intervienen en el intercambio de información.
- Confidencialidad: que solo el emisor y el receptor vean la información.
- La integridad de la información intercambiada, asegurando que no se produce ninguna manipulación.

- El no repudio, que garantiza al titular del certificado que nadie más que él puede generar una firma vinculada a su certificado y le imposibilita a negar su titularidad en los mensajes que haya firmado.

Un Certificado Electrónico sirve para:

- Autentificar la identidad del usuario, de forma electrónica, ante terceros.
- Firmar electrónicamente de forma que se garantice la integridad de los datos trasmitidos y su procedencia. Un documento firmado no puede ser manipulado, ya que la firma está asociada matemáticamente tanto al documento como al firmante
- Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.

CAPITULO IV
DELITOS DE FALSEDAD DOCUMENTAL

1. CONCEPTUALIZACIONES

No toda manipulación, genera falsedad, ni toda falsedad es constitutiva de delito, un escrito puede haber sido lavado, adicionado o mutilado y a pesas de ello ser perfectamente autentico. Generalmente tampoco hay falsedad en ninguna de las modalidades de coautoría grafica, ni en la desfiguración o disfraz de l propia firma ¿en que consiste, entonces, la falsedad documental? ¿Qué es lo que convierte en falso un documento determinado?

Falso, del latin Falsus, participio pasado de fallere, engañar, es lo "engañoso, fingido, simulado; falto de ley, de realidad o veracidad", según el diccionario. Los tratadistas del derecho penal distinguen el documento falso del apócrifo y del falsificado. De la misma manera se diferencia el documento autentico del genuino y aun del legitimo. A nuestro juicio, sin embargo, estas distinciones pueden tener sentido en el campo del derecho, pero no corresponden siempre a conceptos operantes en el terreno pericial.

2. EN TORNO AL CONCEPTO DE FALSEDAD MATERIAL E IDEOLÓGICA

El concepto "falsedad ideológica" se aplica al delito de "falsedad documental".

La regulación es la siguiente (a los fines de entender los conceptos es igual en la mayoría de los países): 3 tipos básicos de falsedad: la material, la ideológica y la impropia. La 1era y la última son posibles tanto en documentos públicos como privados. La 2da, como forma general, sólo es punible en los públicos.

A) La falsedad material. Recae en la escritura misma, y puede consistir en hacerla íntegramente, o en agregar o en reemplazar parte de ella. La falsedad material se

refiere esencialmente a la autenticidad del documento, a la condición de emanado de su autor, o si se quiere, de quien aparece como tal. La pura alteración de la verdad no es apta para configurar una falsedad material.

B) La falsedad ideológica. Esta forma prescinde de la mutación material que caracteriza a la modalidad explicada. Es aquella que existe en un acto incluso exteriormente verdadero, cuando contiene declaraciones mendaces. Se llama ideológica porque el documento no es falso en sus condiciones de existencia, sino que son falsas las ideas que en él se quieren afirmar como verdaderas. Ella puede consistir en hacer aparecer en el documento como ocurrido algo que en la realidad no ocurrió o acaeció de manera distinta. Por eso se la denomina, también, falsedad histórica.

C) La falsedad impropia. La falsedad resulta del hecho de destruir o suprimir el documento. Ambos supuestos están previstos en el art. 294. Es presupuesto de este delito la existencia de un documento auténtico.

Para un sector doctrinal que parte de la idea previa de que sólo la falsedad material es punible, la distinción es fundamental a la hora de interpretar los tipos penales. Ocurre, sin embargo, que nuestro Código no menciona estas categorías, sino que describe las conductas que deben ser objeto de sanción penal, considerando que hay una conducta que es merecedora de reproche penal en función de quien la lleve a cabo o en qué documentos, y otras que deben ser objeto de sanción cualquiera que sea el sujeto activo. A mi entender, este es el punto de partida fundamental, sin que las ideas previas nos puedan servir de ayuda interpretativa. Es decir, una determinada ausencia de verdad en un particular, no será impune por tratarse de una falsedad ideológica, sino por no estar integrada en uno de los tipos penales; de la misma forma, la que esté castigada no lo será por su cualidad de falsedad material, sino por estar integrada en el ordenamiento penal.

En una primera aproximación se distinguiría cuando la falsedad se refiera al continente de cuando lo sea al contenido, a lo que es documental o a lo que es documentado; la falsedad material afectaría al continente, a la estructura física del documento y las ideológicas se referirían al contenido, a la verdad de lo declarado.

La falsedad ideológica sería la manifestación destinada a constatar en un documento algo que quien la hace es consciente de que no se corresponde ni con la verdad absoluta ni con su conocimiento o percepción del hecho pero el documento reuniría todos los requisitos necesarios para su validez. En atención al objeto sobre el que recae, la material afectaría a la autoría o genuidad del documento y la ideológica a su veracidad. Por el momento en que se realiza, la ideológica necesariamente ha de serlo en el momento de la redacción del documento, mientras que la otra puede serlo después.

También se ha intentado acudir a la naturaleza del deber que se vulnera, si es de veracidad como ocurre con los funcionarios públicos encargados de la documentación, sería ideológica, mientras que si se refiere al deber de los particulares de no modificar una realidad ya constatada, sería material.

En la dogmática italiana, por la distinción efectuada en su propio código, estas categorías han sido objeto de amplio estudio, destacando Villacampa , que la opinión mayoritaria se decanta por entender que la distinción se basa en la diferencia que hay entre la alteración de la materialidad o forma del documento que coincide con la genuidad o legitimidad y la que lo es de su contenido o sustancia. Al concepto de genuidad se ha asociado la idea de la coincidencia del autor aparente con el autor real y la ausencia de alteraciones tras su creación, extremo éste que no es pacífico puesto que si se parte de la idea de que un documento se identifica por el autor, tiempo y lugar de emisión, la alteración posterior por su mismo autor lo convertiría en no genuino. Si la identificación de un documento se extendiera a todos sus extremos la distinción

carecería de sentido, con lo que entiendo que el criterio distintivo sólo es claro si lo único que identificase al documento fuese el autor.

Partiendo del momento en que se lleva a cabo la falsedad sería material toda la realizada con posterioridad a la emisión del documento, aunque lo fuese por su autor en cuanto que ya ha perdido la facultad de introducir modificaciones. También en base al criterio de temporalidad, se ha tratado de distinguir entre el diverso grado de veracidad a que está obligada una determinada persona en el momento de la redacción del documento que es distinto según de quien se trate y el deber de dejar inalterados los documentos existentes que corresponde a todos por igual.

En nuestro país la posición dominante es la que entiende que las falsedades materiales atentan contra la autenticidad del documento, mientras que las ideológicas atentan contra la veracidad en cuanto que documentan una declaración que no se ajusta a la realidad que debe reflejar. Sin embargo la distinción no es tan sencilla, siendo buena prueba de ello la diversa consideración que tanto en el ámbito doctrinal como jurisprudencial. Si bien el origen de la distinción obedece a un intento de sistematización que evitase el casuismo, la distinción no puede elevarse a una categoría general que permita encuadrar todas y cada una de las modalidades posibles de falsedad y buena prueba de ello son las dificultades de la doctrina para ponerse de acuerdo acerca de cómo se acogen falsedades ideológicas, materiales o mixtas. Las dificultades apuntadas han llevado a buena parte de la doctrina a tratar de solucionar la cuestión al margen de la distinción entre uno y otro tipo de falsedad

3. CLASIFICACIÓN

Dos grandes clases de falsedad han distinguido tradicionalmente los juristas: la ideológica, que afecta de manera inmediata y exclusiva el animus de la pieza, y surge cuando hay pugna entre sus contenidos debido y atestado, y la material que muda el animus a través del corpus, de los ingredientes materiales o perceptibles del escrito.

Un documento materialmente autentico es el que pertenece al que se imputa y no ha sido alterado. Hay falsedad material cuando el escrito aparenta un origen diferente del real, o cuando se altera su contenido informativo, de manera que deje de ser el que era, el original o primitivo. Es falso pues, el documento que en su condición actual no corresponde a su autor expreso o declarado.

Una firma es autentica cuando ha sido trazado por su creador aparente o manifiesto. Cuando alguien confecciona un documento y lo suscribe con una identidad supuesta o fingida, diferente de la propia incurre en falsedad material. Siempre que se suscriben con el nombre y o firma de otro para suplantarlo, para hacer creer que fue el su autor, se da esta especifica modalidad. Son falsedades materiales, en consecuencia, la confección cabal de una pieza apócrifa (creación) y una modificación sustancial (alteración) del documento genuino.

Para un mayoritario sector de la doctrina el concepto de falsedad documental es inseparable de la idea de mutación. Los estudiosos del derecho penal discuten si esta -la immutatio veritatis, de los clásicos- se puede o no catalogar como elemento estructural del tiempo. Hoy en día, sin embargo, casi todo el mundo ve en la mutación un ingrediente esencial de la acción falsaria. Para que exista falsedad hay que transponer o cambiar algo. Otro aspecto muy discutido también es el de la imitación como ingrediente o elemento de este tipo penal. El concepto jurídico de imitación, sin embargo, es más amplio que el término pericial y que el grafotécnico específicamente. En derecho penal, imitación es en general, la apariencia que presentan algunas cosas de ser lo que no es.

4. DOCTRINA

La doctrina jurídico-penal habla de falsedades por creación o elaboración, por alteración y por uso. En las primeras -en las falsedades ex novo o por elaboración integral- se

engendra en forma cabal un documento espurio. El escrito se saca de la nada, se muda su inexistencia en existencia. El no ser, en ser. Si la pieza no imita un modelo determinado, como acontece cuando se falsifica la credencial de empleado de una empresa inexistente, esa confección global constituye una creación libre. Si en cambio, se reproducen o copian las características del paradigma genuino -como en las falsificaciones de billetes de banco y de documentos de identidad, por ej. - la falsedad ex novo resultante será una creación simulativa.

En las falsedades materiales por alteración, la mutación recae sobre un documento ya elaborado. Se introduce cambios a este por agregación, supresión, o sustitución, transformando en falso lo genuino. No toda mutación del corpus documental, sin embargo, es esencial, "es decir", extraña necesariamente una mutación del animus o contenido ideo - moral del escrito, e indica falsedad. Hay también mutación en las denominadas falsedades impropias por ocultación, supresión, y destrucción, que de alguna manera suponen una modificación del documento preexistente. En este caso de su condición o situación y de sus posibilidades de utilización o aprovechamiento.

Falsear o falsificar es crear, a través de una intervención conciente, un contraste entre dos realidades: una preexistente (la inexistencia del documento, o su genuidad) y otra posterior (la existencia del escrito o su falsificación). En toda falsedad hay trastrocación de una realidad anterior, o de un documento ya elaborado. En la falsedad ex novo o por elaboración integral, repetimos, se cambia un statu quo o realidad trascendente (inexistencia del documento) en una falsedad (existencia, o apariencia de existencia del mismo). En las demás especies se transforma o altera un escrito legítimo, íntegramente formado o acabado.

Enfocando las cosas desde un ángulo estrictamente fenomenológico - haciendo abstracción de toda connotación jurídica - se puede decir que un documento es falso cuando no corresponde al autor a quien se atribuye o cuando su contenido expreso o

atestado no guarda conformidad con el ideal o debido, situación esta ultima que surge en principio, en dos momentos diferentes:

al crear el documento, consignando en el un mensaje diverso del que se debía expresar (falsedad Material o ideológica) o elaborando íntegramente un documento falso (Falsedad Material ex novo, por creación o elaboración integral) con posterioridad a la elaboración del documento, mudando en cualquier forma su contenido manifiesto o atestado (falsedades materiales por alteración).

Seguidamente analizaremos someramente estas modalidades.

a) Autenticidad Intrínseca y Falsedad Ideológica: en todo documento escrito lo hemos explicado ya, ha que distinguir un contenido ideal, o debido, y un contenido real, expreso o atestado. El primero es el mensaje que el documento esta llamado a registrar o expresar, aquello que su creador debe consignar en el. El segundo, el mensaje manifiesto o efectivamente inscripto. La conformidad entre texto expreso o real y el ideal o debido constituye a la verdad o autenticidad intrínseca del documento. La falta de correspondencia entre esos contenidos -se consigna en el escrito algo diferente de lo que se debería manifestar- típica la denominada falsedad ideológica.

Por su propia naturaleza el documento esta llamado a registrar la verdad. Lo normal, pues, es que recoja la realidad ontológica que la asegure y que garantice su fiel transmisión al destinatario. De ello depende precisamente, la tan cacareada vocación probatoria del documento.

Es perfectamente posible, sin embargo, que el contenido documental debido envuelva una declaración reñida con la realidad y que el documento, pese a ello, sea intrinsecamente autentico o veraz. La única condición para que un documento sea verídico, en efecto, es que su texto o mensaje escrito se adecue fielmente al mensaje ideal, que lo que expresa sea exactamente lo que debía proclamar. Ahora bien, el

debido documentar no es siempre, necesariamente, una declaración materialmente veraz, ya que el documento, en cierta forma no es mas que una fiel fotografía de la realidad. Su función no es otra que la de captar la verdad objetiva sin distorsiones de ningún tipo. Un documento autentico puede tener por objeto, pues, la prueba de una afirmación o declaración contraria a la verdad.

Francesco Carrara explicaba todos estos aspectos con un elocuente ejemplo, que se ha vuelto clásico en la literatura jurídico-penal:"supongamos -decía-que una de las partes le declara al notario que en el terreno que vende hay cien cultivos, aunque no hay sin o cincuenta, esos cincuenta cultivos no existen como materialidad ante el notario, pues ante el solo existe como materialidad la palabra de la parte, el no ve esos cultivos con los ojos corporales, y por lo tanto no los percibe sino como una idea por esto si escribe que son ciento, el escrito es verdadero porque reproduce fielmente la materialidad que esta destinado a certificar, o sea, lo dicho por la parte ante el notario; mas el escrito no será verídico, pues los cultivos no son sino cincuenta; pero esta es una mutación de la verdad ideológica, y el documento no puede llamarse falso. En cambio, si el notario, mejor informado de la verdad real, escribe que los cultivos son cincuenta, aunque la parte haya declarado que son cientos, el escrito es verídico porque reproduce una idea verdadera, pero el documento es falso, pues no reproduce la materialidad que debía reproducir, y así podría ser falso en la materialidad y al mismo tiempo verídico en la idea; he aquí la falsedad perpetrada con el fin de probar un hecho verdadero".

El ejemplo anterior nos viene bien para mejor precisar nuestros planteamientos. Las manifestaciones hechas por la parte ante el notario - la afirmación de que en el predio vendido hay cien cultivos- es el contenido ideal o debido del contrato en este caso. El debido documentar. El funcionario esta en la obligación de dar fe de lo declarado ante el por el compareciente. Debe certificar, en otros términos, que, según lo manifestado por el vendedor, en el predio objeto de la venta hay cien plantaciones. No es potra su

función, ya que la certificación notarial no esta destinada a probar cuantos cultivos hay en el fundo vendido, sino cuantos afirmo la parte que había en el.

Ahora bien, la manifestación del contratante del ejemplo es falsa porque los sembrados reales no eran cien, sino cincuenta. ¿Es falso entonces, por esta razón, el documento? Evidentemente, no. El contenido ideal de ese escrito no es verídico, desde luego, pero el documento llamado a registrarlo y que efectivamente lo recoge, es autentico. Es intrínsecamente autentico, pues expresa la única verdad que estaba llamada a registrar - las declaraciones de la parte ante el funcionario notarial- así su contenido no sea verídico.

En la transcripción que comentamos se plantean otras hipótesis. ¿ que ocurre, se pregunta el maestro Carrara, si el notario, mejor informado de la verdad real, escribe que los cultivos son cincuenta, aunque la parte haya declarado que son cientos? La respuesta no ofrece ninguna dificultad. El documento es falso, sin duda alguna, porque atribuye al compareciente declaraciones que no ha hecho. Es falso, en otros términos, porque su contenido es real o atestado no se conforma al contenido ideal, al que debía expresar. Lo que se debía declarar o documentar en este caso no era, pues - perdónese la reiteración - el numero de cultivos existentes en el fondo, sino el que afirmo la parte que haba en el. Estamos en este evento, como untaba muy bien el ilustre catedrático de Pisa, ante una falsedad en documentos perpetradas para probar el hecho verdadero. Ante una falsedad que merecía, quizás, un tratamiento punitivo mas benigno, pero en todo caso ante una inequívoca forma de falsedad documental.

b) Falsedades materiales: se conoce con este nombre en la literatura jurídico-penal aquellas mutaciones que afectan el contenido ideo - moral del documento a través del compromiso de sus ingredientes palpables u ostensibles. Inciden, pues, sobre el corpus del escrito. La falsedad material según montenegro, "consiste en la modificación de la realidad por creación de un instrumento totalmente apartado de la verdad, o por modificación o alteración de uno verdadero mediante actitudes perceptibles a los

sentidos y de relevancia. Supresión de ideas, cambio de términos mediante el borrado químico o mecánico agregación de conceptos, cifras, signos o símbolos. La verdad puede ser atacada creando un documento que la modifica o alterando uno verdadero con intercalación o cambios o mutación. La alteración o adulteración puede recaer en esos eventos sobre el contexto o la firma".

Creus sintetiza sus modalidades diciendo que la falsedad material del documento recae "sobre sus signos de autenticidad, incluidos los que forman su contenido, ya sea que los imite, creándolos, o que se los modifique, alterando los verdaderos. Ataca, pues, la verdad con el menoscabo de la autenticidad del documento".

En el primer caso el falsario saca de la nada un documento dándole apariencia de autenticidad. Ejemplos típicos de esta variedad son las falsificaciones de papel moneda y de sellos de correos. En la creación integral o falsedad ex novo se produce siempre, como anota con razón Arenas Salazar, una forma de mutación de la inexistencia a la existencia: " cuando no preexiste un documento, como es el caso de la falsedad integral o total, preexiste una verdad, una realidad que transciende al mundo del derecho, y es que no hay documento. Una vez producida la acción falsaria, una vez creado el documento falso, integro, tenemos un resultado espurio, esto es, una apariencia de verdad, o lo que es igual: un documento falso. El contraste entre la verdad, no existencia del documento, y una falacia: existencia de un documento. Falso, claro esta, pero existe y da la apariencia de genuinidad".

c) Alteración sustancial: en ella siempre existe -insistimos- un documento preexistente, al que se le agregan, suprimen o sustituyen elementos o signos gráficos, con el objeto de variar su contenido ideativo original.

d) Fecha y lugar de expedición: el documento escrito es inconcebible sin su entorno o marco espacio-temporal. El lugar y la fecha de producción son algo así como el recuadro dentro el cual se inscribe el documento. No siempre, sin embargo, se registran

estos datos en e texto. La atribución del escrito a un sitio y a un momento determinados, con todo, es bastante frecuente. La mención expresa del lugar y/o fecha de elaboración en el documento convierte esas referencias en parte integrante de su contenido inscrito, de su mensaje atestado, como antes anotamos. Si los datos no corresponden a la realidad, al debido documentar, habrá falsedad ideológica. Si se muda un documento ya elaborado, alterándole la fecha o el lugar de creación indicados en el, o adicionándole esta información, la falsedad será material.

e) Mutación del contenido atestado: materialmente constituye falsedad toda creación o elaboración integral de documentos atribuidos a un autor diferente del real y la mutación del contenido expreso o atestado de uno preexistente. La mutación del mensaje documentado, sin embargo, así sea para adecuarlo a la verdad que no expresaba el primitivo afecta la función representativa de la pieza y entraña siempre, desde el punto de vista fenomenológico, una falsedad material (inautenticidad), aunque el cambio solo busque dar veracidad al escrito. Puede haber alteración sustancial sin falsedad (para corregir un yerro involuntario del escrito, por ejemplo). La alteración del contenido documentado, sin embargo, entraña siempre la falsedad material, así sea para probar un hecho verdadero.

f) Manipulaciones del elemento autoría: desde el punto de vista estrictamente técnico hay una falsedad documental en la denominada ficción de autor (cuando se hace figurar como creador del documento a una persona imaginaria) y en la suplantación (cuando se presenta como autor a una persona determinada diferente de la real). Y ello, a pesar de esas conductas pueden no ser constitutivas de delitos.

En síntesis se puede decir que un documento es falso cuando no corresponde al autor a quien se atribuye, o cuando su contenido textuado - incluyendo en el por supuesto el lugar y la fecha declarada- no guarda conformidad con el ideal o debido. Las alteraciones no son más que mecanismos modificadores del mensaje documentado o contenido manifiesto del escrito.

5. TIPIFICACIÓN

La limitación de la tipificación del delito de falsedad cometido por particulares, llevó a numerosos estudiosos a sostener que en el CP la falsedad ideológica sólo está castigada cuando se comete por autoridad o funcionario público en el ejercicio de sus funciones, equiparando así la falsedad intelectual o ideológica al hecho de faltar a la verdad en la narración de los hechos. Otro grupo de autores, entendieron que el Código recogía la falsedad ideológica suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho, por lo que estando castigada esta conducta tanto cuando se comete por autoridades o funcionarios públicos como por particulares, para estos autores, el CP no supuso la despenalización de esta modalidad de falsedad cuando fuera cometida por particulares.

Bacigalupo señala que se ha eliminado la posibilidad de sancionar las falsedades ideológicas cometidas por particular al entender que se carece de virtualidad para éstos. Quintero Olivares indica que esta modalidad reúne aparentemente ingredientes de la falsedad ideológica y de la falsedad material, pero su naturaleza es más próxima a la falsedad ideológica si por ella se entiende una alteración consciente del hecho jurídico que se quiere probar plasmada en un documento formalmente correcto.

De forma gráfica se ha dicho que no toda mutación de la verdad constituye una falsedad con relevancia penal, pero toda falsedad implica alguna modificación de la verdad. Por otro lado la falsedad no suele ser un fin en si misma sino un medio para la obtención de determinados fines. Se distingue así los supuestos en que el hecho falsario se castiga con independencia de los fines perseguidos de cuando lo es si lleva aparejada una determinada finalidad, así respecto de los documentos privados está excluido el delito cuando la mutación de la verdad no tiene como finalidad el perjuicio de otro. Todavía se podría distinguir de nuevo los supuestos en que la falsedad es mero

instrumento para la comisión de otro delito existiendo unidad de acción, concurso ideal, de cuando hay dos o más acciones constitutivas cada una de un delito pero en que una es el instrumento para la comisión del otro, en que habrá un concurso medial o real. Singular importancia ofrecen las llamadas estafas documentales.

Como falsedades documentales impropias que forman parte del tipo de otros delitos, se encuentran en el CP diversas modalidades de estafa, la presentación de datos falsos relativos al estado contable para lograr indebidamente la declaración de quiebra, concurso de acreedores o suspensión de pagos, las que se llaman instrumentales en el delito fiscal y que declara exentas de responsabilidad cuando se produzca la regularización de la deuda tributaria, el falseamiento de información en los delitos contra los recursos naturales y el medio ambiente, el documento que incorpora la tasación de bienes o cosas, la presentación de documentos falsos en juicio, el falseamiento de correspondencia o documentación legalmente calificada como reservada o secreta en el delito relativo a la defensa nacional.

Dentro de las falsedades documentales que no están castigadas, resulta relevante, en relación con el punto que nos ocupa, la modalidad de falsedad ideológica, incluida dentro de los delitos societarios, de la que sólo pueden ser sujeto activo los administradores de hecho o de derecho de una sociedad y que puede recaer en las cuentas anuales u otros documentos, siendo necesario la existencia de un dolo específico, cual es el de causar un perjuicio económico a la misma, a alguno de sus socios, o a un tercero.

Ante todo hay que tener en cuenta que el carácter de cada documento le otorga un grado distinto de tutela, distinguiéndose por un lado los que emanan de una autoridad o funcionario público de los demás y dentro de éstos los mercantiles - si bien no están definidos- y los privados. Estos últimos sólo son objeto de protección penal en el caso de que la falsedad se cometa con la finalidad de perjudicar a otro.

6. EFICACIA PROBATORIA Y RELEVANCIA JURÍDICA

El CP condiciona el concepto de documento a que tenga eficacia probatoria o cualquier otro tipo de relevancia jurídica. Algunos autores han entendido que la única relevancia jurídica que puede tener un documento es la de prueba, trasponiendo al concepto de documento su eficacia probatoria en cuanto que los públicos prueban frente a terceros la fecha, el hecho de su otorgamiento y la realidad de las manifestaciones que en ellos hubiesen hecho los otorgantes - no la veracidad de dichas manifestaciones-, mientras que los privados sólo hacen prueba de las relaciones entre los otorgantes.

Sin embargo el concepto de relevancia jurídica a mi juicio es mucho más amplio puesto que de prueba sólo se puede hablar en el marco del proceso mientras que al margen de éste pueden crearse situaciones jurídicamente relevantes en base a un documento. Así mediante su presentación ante la administración. Todavía cabe, ciñéndonos al marco del proceso, que un documento sea suficiente para dictar una resolución que modifique las situaciones jurídicas existentes entre quienes en él aparecen como otorgantes y no constituya prueba; esto ocurre en los casos de acreditamiento documental previo o prueba prima facie.

Así, la justificación documental para la adopción de una medida cautelar en el orden jurisdiccional civil que crea una apariencia de buen derecho destinada a asegurar su efectividad para el caso de que la apariencia se transmute en certeza por la sentencia firme , la reclamación de una deuda que se acredite inicialmente por uno de los documentos señalados, que incluye facturas, documentos comerciales que acrediten una relación anterior duradera y otros aún unilateralmente creados por el acreedor es suficiente para crear en quien la petición atribuye la condición de deudor, la carga de oponerse o el despacho de ejecución; la letra de cambio, cheque o pagaré que ha de acompañarse a la demanda del juicio cambiario que sean o no auténticos, si cumplen los requisitos formales, provocan la orden de requerimiento de pago y embargo

preventivo de los bienes del deudor. Estos documentos pueden carecer de eficacia probatoria pero no de relevancia jurídica, siendo por tanto este concepto distinto y más amplio que el primero. Todo documento con eficacia probatoria tiene relevancia jurídica pero no todo el que tiene relevancia jurídica tiene eficacia probatoria.

El recurso a las normas sobre la fuerza probatoria de los documentos ya no es un criterio que nos sirva para determinar cuando un documento debe de ser objeto de protección penal, puesto que un documento que se revele que no ha sido firmado por quien en él aparece como su autor, no probara el hecho que trata de documentar, pero antes habrá podido tener relevancia jurídica. Al que se le haya alterado algún dato no probará eso, pero antes ha podido ser relevante.

CAPITULO V
BIEN JURIDICAMENTE PROTEGIDO

1. DEFINICIONES Y CONCEPTUALIZACIÓN

El bien jurídico protegido por los delitos de falsedad documental ha sido caracterizado por la doctrina, por lo general, como la «seguridad en el tráfico jurídico» o la «fe pública». Las nociones de seguridad en el tráfico jurídico o de fe pública, sin embargo, requieren una cierta precisión, pues, de lo contrario, carecen de toda capacidad operativa. Una categoría de delitos contra la fe pública parece haber sido introducida por FILANGARI y fue criticada por BINDING ya en el siglo pasado por entender que no existe un derecho a la verdad de carácter general.

En el mismo sentido ya decía RODRÍGUEZ DEVESA que «parece evidente que nuestra ley no da a las falsedades tal extensión, ni sería deseable que lo hiciera, porque equivaldría a reconocer un derecho a la verdad que rebasa las posibilidades del legislador y excede de las metas jurídicas». Por ello, proponía concretar el bien jurídico protegido por las falsedades documentales como un grupo de delitos contra los medios de prueba y signos de autenticación.

Esta concreción del bien jurídico presupone, como es lógico, establecer cuál es el objeto en el que se deposita la fe pública y en qué consiste la seguridad del tráfico jurídico. Por un lado, es claro que el público puede depositar su fe en múltiples objetos, pero se trata de proteger sólo algunos objetos. Por lo pronto, no parece que el legislador haya querido proteger la fe en las declaraciones de otros de una manera general. De lo contrario toda mentira, documentada o no, debería ser punible. La documentación en sí misma, no agrega nada a la mentira de un particular desde el punto de vista de su criminalidad. Por tanto, el público no puede sentir defraudada su fe por la simple mentira de otro, pues en una sociedad democrática los límites del control social presuponen una distinción entre deberes éticos y deberes jurídicos, cuya

confusión sería la inevitable consecuencia de convertir a la verdad de las declaraciones de los particulares en objeto jurídico de protección de los delitos de falsedad documental. Por otro lado, también es claro que la veracidad de ciertas declaraciones tiene entidad suficiente para ser objeto de protección cuando se trata de declaraciones de un funcionario público que tienen acordado un determinado valor probatorio por la ley. La diferencia de esta situación con la anterior ha sido reconocida ya hace más de un siglo.

Este doble significado social y jurídico de la veracidad de la declaración documentada es lo que permitió a la dogmática moderna distinguir una doble dimensión en la protección jurídica de los documentos, según sean públicos o privados. En los primeros se protege la fe del público en las constataciones documentadas por el oficial público; en los segundos se protege la fe del público en la atribución de una declaración a una determinada persona.

Esta doble dimensión de protección de los documentos se basa en la amplitud del deber de veracidad que incumbe a los sujetos del delito, es decir, por una parte a los funcionarios y oficiales públicos y por otra a los ciudadanos en general. Mientras el funcionario está obligado a declarar verazmente, el particular tiene prohibido alterar el soporte material de la declaración atribuida auténticamente a otro o a sí mismo. Es decir: los distintos deberes generan también diversas normas.

2. POSICIONES DOGMÁTICAS

Tres son las posiciones dogmáticas fundamentales a la hora de determinar el bien jurídico protegido por el delito de falsedad.

La que considera que es la fe pública, entendida como confianza de las personas en la autenticidad y veracidad que deben tener algunos signos y documentos. Así en el CP italiano y en el francés se denominan delitos contra la fe pública.

La que entiende que es la seguridad del trafico jurídico en cuanto que sólo en la medida en que el documento entra o está destinado a él, la falsedad tiene relevancia penal, existiendo una corriente de esta formulación que liga el bien jurídico con la función probatoria del documento, en la medida en que éste además de estar destinado a entrar en el tráfico económico y jurídico también lo está a cumplir un importante papel en la prueba de las relaciones jurídicas, en las que es un medio privilegiado, para lo que ponen el acento en el valor probatorio del documento. Sin embargo desde el momento en que la prueba no es lo mismo que la relevancia jurídica habría que ponerlo en relación con este ultimo concepto y entender que los delitos de falsedad documental tutelan los documentos con relevancia jurídica.

La tercera formulación parte de las funciones del documento, que tradicionalmente se han sido tres: la de perpetuación que supone la perdurabilidad temporal, la de prueba en cuanto que está destinado a acreditar la existencia de relaciones jurídicas y la de garantía en cuanto que la autoría del documento se atribuye a una determinada persona, por lo que el ilícito penal habrá de atentar contra alguna de estas funciones que conformarían el bien jurídico protegido. Dentro de esta formulación señala García Cantizano que el bien jurídico protegido específicamente en el delito de falsedad documental sería la propia funcionalidad del documento en las diversas funciones que tiene que cumplir en el tráfico jurídico.

La falsedad documental sólo tiene trascendencia en la medida que el documento entra en el tráfico jurídico o está destinado a entrar en él. Así el Código Penal alemán castiga a quien elabore un documento no auténtico, falsifique un documento auténtico o utilice un documento no auténtico para engañar en el tráfico jurídico. Por otro lado no cabe desconocer que la existencia de distintos tipos de falsedad puede dar lugar a que en unos supuestos el bien jurídico tenga unos matices de los que otra modalidad carece. Así, si la falsedad en documento privado sólo está castigada cuando se comete para perjudicar a otro, parece que además de la seguridad del tráfico o la función probatoria

del documento hay otro bien jurídico protegido, generalmente de contenido patrimonial. Desde esta perspectiva también se ha hablado del carácter pluriofensivo del delito de falsedad. Se ha destacado la importancia de las tres funciones del documento, así se señala que toda falsedad supone una mutación de la verdad, y la falsedad documental se produce cuando resultan afectadas algunas de las funciones esenciales que cumple un documento, es decir la función perpetuadora - fijación material de las manifestaciones del pensamiento-, la probatoria - adecuación para producir pruebas-, o la garantizadora- posibilitar el conocimiento del autor de las manifestaciones.

La función de perpetuación se ve afectada básicamente cuando el documento es destruido o deteriorado. La función probatoria resultará afectada cuando la alteración del documento afecte a aquello que el documento puede y debe probar. Y la función de garantía, continua señalando esta sentencia, resultará afectada cuando la falsedad no permita identificar al autor de la declaración de voluntad. Numéricamente han sido más las sentencias que se han posicionado con las dos primeras teorías, incluso complementándolas, se señala que la incriminación de las conductas falsarias encuentra su razón de ser en la necesidad de proteger la fe y la seguridad en el tráfico jurídico, evitando que tengan acceso a la vida civil o mercantil elementos probatorios falsos que puedan alterar la realidad jurídica de forma perjudicial para las partes afectadas.

A mi entender la simulación afecta tanto a la función de garantía como a la relevancia que el ordenamiento jurídico da a determinados documentos.

3. DOCTRINA Y DOGMÁTICA COMPARADA

La doble orientación de la protección penal en los delitos de falsedad documental no es un descubrimiento dogmático reciente. En efecto, en la doctrina italiana, CARRARA la sostuvo de una manera clara hace más de un siglo. Desde su punto de vista la falsedad del documento privado pertenecía a la «familia» de los delitos contra la propiedad al

tiempo que los delitos de falsedad en documento público pertenecían a los delitos contra la fe pública. CARRARA criticaba a la doctrina que había sostenido que las dos formas de falsedad constituían una única especie y pertenecían a la misma familia de delitos afirmando categóricamente: «esto es un error; y de tal error se ha derivado que, queriendo reducir la teoría del delito de falsedad documental a ciertas reglas generales, comunes a las dos falsedades antedichas, se ha contrahecho la naturaleza jurídica de uno y otro delito; y de allí ha surgido confusión y discordia respecto de los criterios esenciales y de los criterios mensuradores de ambos delitos, los que, por sus condiciones intrínsecas debían considerarse como una especie distinta que nada tienen entre sí en común, fuera de la identidad del sujeto pasivo (el papel)».

Una evolución paralela siguió la dogmática alemana. BINDING partió de una crítica radical de la teoría de la publica lides que consideraba una «teoría insalubre» y desarrolló luego una prolija investigación para subrayar que los documentos debían ser sólo aquellos que estaban determinados para servir de prueba y para demostrar que «los delitos, cuyo objeto son [los documentos], más precisamente el medio probatorio que les corresponde», están indisolublemente conectados con los que se refieren a otras declaraciones que operan como medios probatorios. La falsedad en despachos telegráficos, por el contrario, era tratada por BINDING como un delito de funcionario. Sin embargo, fue von LISZT quien culminó el nuevo desarrollo dogmático en Alemania al distinguir con precisión entre la falsificación de documentos (en el sentido de alteración material del soporte material) y la documentación falsa de hechos.

Von LISZT afirmaba en este sentido: «La documentación falsa es diversa de la falsificación de documentos. La esencia de la segunda consiste en la imitación o alteración de la forma acreditada (Beglaubigunsform).

Conceptualmente es indiferente si el contenido del documento creado coincide o no con la verdad. A pesar de la coincidencia con la verdad puede darse un documento falso; p.

ej., cuando el deudor que ha satisfecho la deuda al acreedor, pero no ha obtenido de éste el correspondiente recibo, confecciona un recibo.

Asimismo, a pesar de la no coincidencia puede ser excluida la falsedad documental, p. ej., cuando el acreedor, cuyo crédito no ha sido satisfecho, es inducido mediante engaño por el deudor a extender el recibo correspondiente. Por el contrario, la esencia de la documentación falsa consiste en la mendacidad respecto del hecho documentado, mientras que el documento mismo es auténtico y no falsificado».

En suma: la fe pública o la seguridad del tráfico jurídico son conceptos muy vagos y generales que requieren una precisión. Un análisis profundo de ellos demuestra que la fe del público en el valor probatorio de los documentos adquiere formas diversas según la fuerza probatoria del documento.

Antes de concluir estas consideraciones sobre el bien jurídico protegido se debe señalar que sería erróneo suponer que el CP contiene una norma que define el bien jurídico de los delitos de falsedad documental.

Consiguientemente sería erróneo entender que las expresiones finales «cualquier otro tipo de relevancia jurídica» podrían significar que los delitos de falsedad documental protegen intereses diversos de los referentes a los documentos como medio de prueba.

En efecto, es evidente que tales conclusiones se apoyarían en la confusión de dos conceptos diferentes: el bien jurídico (u objeto jurídico de protección) y el objeto de la acción (el objeto material sobre el que se deben producir los efectos de la acción en el mundo exterior). El CP sólo define el objeto de la acción, es decir, el documento como soporte material sobre el que debe recaer la acción.

El bien jurídico protegido, por el contrario, se debe extraer teleológicamente de las disposiciones sobre las falsedades documentales. Dicho de otra manera: el CP contiene

una definición de documento que puede ser de mayor alcance que la correspondiente al objeto de la acción de los delitos de falsedad documental. No todas las funciones del documento deben ser objeto de protección de los delitos de falsedad documental.

Los otros tipos de relevancia jurídica a los que se refiere el CP —hasta ahora no precisados en la teoría ni en la práctica— son objeto de otros delitos diversos de los de falsedad documental.

En particular la calidad de instrumento de un engaño, por ejemplo, es objeto básicamente del delito de estafa (sobre todo en la estafa informática), pero también del delito fiscal, entre otros.

CAPITULO VI
FALSEDAD EN DOCUMENTO ELECTRÓNICO

1. ANTECEDENTES

El art. 7 de la Convención del Consejo de Europa sobre Cibernética, Budapest, 27.11.2001, establece la obligación de los Estados de adoptar todas las medidas, legislativas o de otra especie, “para erigir en infracción penal conforme a su derecho interno, la introducción, la alteración, la eliminación (effacement) y la supresión intencional y contraria a derecho de datos informáticos, la generación de datos no auténticos, con la intención de que ellos sean tenidos en cuenta o utilizados para fines legales como si fueran auténticos, sean o no directamente legibles o inteligibles. Las parte pueden exigir una intención fraudulenta o una intención delictiva similar como la requerida para la responsabilidad penal”. Una convención como ésta nos propone como tarea inmediata la de estudiar hasta qué punto nuestro derecho vigente satisface las obligaciones contraídas por el Estado Boliviano en ella.

La lectura del texto pone de manifiesto una notable debilidad técnica de los redactores, que no han tenido siquiera sensibilidad para comprender que la expresión “intencionnel” no sólo es oscura en francés, sino equívoca también en otras lenguas europeas. Sin duda queda claro que lo querido por la convención es la exclusión de comportamientos meramente imprudentes. Pero, tampoco ofrece dudas que lo problemático será, como ocurre cada vez que se usa la expresión “intencional”, si también deben ser punibles los hechos cometidos con dolo eventual, forma del dolo que, conceptualmente, no puede, en principio, ser identificada con la intención. Por lo pronto la doctrina considera que el dolo eventual es suficiente respecto de la calidad de documento del objeto de la acción en los delitos de falsedad documental.

Desde el punto de vista objetivo esta disposición se refiere fundamentalmente a la falsificación de documentos informáticos, tanto por la alteración de sus funciones, como por su destrucción.

Paralelamente, mediante la Directiva CEE 99/93, de 13 de diciembre de 1999, se han establecido las condiciones relativas a las firmas electrónicas y a los servicios de certificación de las mismas. Ello ha dado lugar a la sanción de leyes nacionales armonizadas en los Estados Miembros (EEMM) de la Unión Europea (UE), entre las que cabe destacar nuestro Real Decreto Ley 14/1999, referido a la Posición Común de la UE de 22 de abril de 1999, la Ley marco alemana [Signaturgesetz (SigG)], de 16 de mayo de 2001 y la Ley italiana nº 39 del 15 de febrero de 2002 (Attuazione della directiva 1999/93/CE relativa ad un quadro communitario per le firme elettroniche).

En este contexto normativo se deben plantear las cuestiones referentes a la repercusión que las nuevas regulaciones tienen en el ámbito propio de los delitos de falsedad documental. Ello no es sólo consecuencia del art. 7 de la Convención de Budapest, cuya finalidad es indudablemente la protección penal de los documentos electrónicos, sino también de las consecuencias que esta nueva especie de documentos generan respecto del concepto de documento, especialmente en el derecho privado.

En tal sentido es de señalar la reforma del BGB (Código Civil alemán) por la Ley de Adaptación de Disposiciones sobre la Forma y otros Preceptos al Moderno Tráfico de Negocios Jurídicos, de 13 de julio de 2001, mediante la que se incluyeron nuevos parágrafos en el Código Civil (también en otras leyes) que admiten el reemplazo de la tradicional forma escrita por “forma electrónica”, de tal manera que la forma escrita se ha convertido en forma “textual”. El parágrafo126 BGB ha sido completado con una disposición (que se incluye como nuevo párrafo 3) en la que se dice “la forma escrita puede ser reemplazada por la forma electrónica, cuando la ley no establezca otra cosa”. El nuevo parágrafo 126 a), a su vez, prevé que “si la forma escrita legalmente establecida se reemplaza por la electrónica, el emisor de la declaración debe agregar

su nombre y el documento electrónico debe ser completado por una firma electrónica cualificada según lo previsto por la ley de firmas". También es importante tener en cuenta que la ley alemana introdujo en el BGB un nuevo parágrafo 126 b) que establece que "si la ley prescribe forma textual [o de texto, en el original: Textform], la declaración debe ser realizada en un documento o de otro modo adecuado para la fijación duradera en caracteres escritos [dauerhafte Wiedergabe in Schriftzeichen], mencionada la persona que efectúa la declaración y el final de la misma se hará constar mediante la reproducción de la firma de su nombre o de otra manera".

Si bien se ve, la posibilidad de creación electrónica de documentos no ha variado el concepto de documento en sí mismo. Lo que ha cambiado son las maneras en las que se llevaban a cabo las funciones tradicionales del documento, básicamente el tipo de soporte en el cuál se perpetúa la declaración de la voluntad que se documenta, la forma de garantizar la imputación del contenido de la declaración a quien la realizó y la prueba de la autenticidad mediante una certificación de determinados signos, análoga a una certificación de carácter notarial, a través de un servicio de certificación electrónico.

Esta afirmación se ve confirmada por el ley española, que establece que "la firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales".

Las funciones de un documento electrónico, consiguientemente son las mismas que las reconocidas hasta ahora en la doctrina y en la jurisprudencia. El nuevo parágrafo 126 b) del Código Civil alemán, antes transcritos, parecen ser una confirmación irrefutable de esta afirmación.

La doctrina y la jurisprudencia españolas han reconocido, ya antes del art. 26 CP, que el documento tiene tres funciones: una función de perpetuación, referida al mantenimiento de la declaración de voluntad en un soporte capaz de fijarla en el tiempo y de hacerla cognoscible a otras personas distintas del emisor; una función probatoria, que permite demostrar procesalmente la existencia de la declaración de voluntad de su emisor y una función de garantía, por la que se garantiza la imputación de lo declarado al autor de la declaración.

La definición de documento introducida por el CP, no ha sido totalmente acertada. En él se hace referencia a la eficacia probatoria del documento, pero también a "cualquier otro tipo de relevancia jurídica". Esta amplitud del texto puede generar la idea errónea de que el CP contiene la definición del objeto de la acción de los delitos de falsedad documental. Sin embargo, debemos aclarar, no contiene únicamente una definición del objeto de la acción de los delitos de falsedad documental, sino una definición del documento en sentido más amplio, con la finalidad de que sea adecuada a cualquiera de los tipos penales que tienen alguna relación con documentos. Si el CP tuviera la función de definir exclusivamente el objeto de la acción de los delitos de falsedad documental, su posición sistemática sería evidentemente otra: estaría situado entre las disposiciones que estructuran esos tipos penales. Esta amplitud convierte al CP en una disposición carente de verdadera utilidad dogmática, dado que el concepto de documento se debe precisar luego, en cada delito en particular, es decir, casi de la misma manera que si esta definición no existiera. Dicho con otras palabras: el concepto de documento sigue padeciendo en nuestro derecho penal el déficit de seguridad que ya había señalado Binding cuando afirmaba que "todo respira una gran inseguridad".

2. NOCIÓN DE DOCUMENTO Y TECNOLOGÍA

La aparición de la firma electrónica en el tráfico jurídico representa una nueva etapa en la vida dogmática de los delitos de falsedad documental. Los avances tecnológicos han

ido generando diferentes problemas jurídicos en relación al concepto de documento y, por extensión al de firma.

En primer lugar se planteó la cuestión de si era posible considerar documento los que realmente no constituyeran escrituras, como, por ejemplo la expresión de la palabra grabada. Más tarde se generaron dificultades con las fotocopias y finalmente con el fax. De alguna manera, los problemas de la influencia de la tecnología supera el ámbito de la estricta falsedad documental.

Un ejemplo en este sentido surge de la equiparación de la falsificación de tarjetas de crédito con la falsificación de moneda. En la práctica se ha planteado recientemente la cuestión de si la falsificación de los datos contenidos en la banda magnética de una tarjeta de crédito debe ser considerada equivalente a la falsedad de moneda. No podemos ignorar que el problema proviene de la gravedad de la pena que tal equivalencia genera, pero no deja de ser significativo que para resolver la supuesta desproporción penal se haya pensado que la utilización fraudulenta de datos electrónicos en la banda magnética de una tarjeta de crédito no debería ser considerada como falsificación de la tarjeta. La tesis, pone de manifiesto la posible tendencia, sobre todo intuitiva, de negar –a priori el carácter de documento a la utilización de datos electrónicos, es decir, una solución difícilmente sostenible.

Cada vez que la realidad social presenta a los juristas nuevas situaciones, la primera aproximación a la solución del problema suele ser llevada a cabo mediante un análisis de problemas análogos del pasado, que hoy pueden estar ya olvidados como tales. Un ejemplo que resulta instructivo es el del contagio del SIDA. Cuando apareció esta nueva enfermedad, los juristas recordaron de inmediato que en las décadas de los 20 y los 30 el contagio venéreo de determinadas enfermedades había dado lugar a una serie de cuestiones que mutatis mutandis, fueron orientando las nuevas soluciones dogmáticas.

En el plazo aproximado de tres décadas en materia de documentos la dogmática de los delitos de falsedad documental se ha visto confrontada con diversas innovaciones tecnológicas que han obligado a reflexionar sobre la trascendencia que ellas podían tener en la aplicación de los delitos correspondientes a este ámbito. También la legislación ha experimentado transformaciones que provienen de la evolución de la tecnología en el tráfico jurídico. Lamentablemente, la reforma penal no ha tenido en cuenta la evolución que en la materia se observa en el derecho europeo.

Si se comparan los tipos penales de la falsedad documental del Código vigente con los del Código penal alemán, se podrá percibir de inmediato que este último ha introducido en el parágrafo 268 un tipo específico para la falsificación de los soportes documentales de comprobaciones y mediciones expedidas por medios técnicos (technische Aufzeichnungen), en el que en el lugar de la declaración de voluntad o de pensamiento, característica del documento tradicional, entra el registro de datos, medidas, o valores aritméticos realizados por un aparato automático. Se trata de casos en los que se protege la confianza no en la emisión de una declaración documentada por una persona, sino en los datos automáticamente emitidos por una máquina o aparato especialmente programado para tales fines. En el Código alemán se introdujo también el parágrafo 269, referido a la falsificación de datos relevantes desde el punto de vista probatorio, cuya principal finalidad es la prevención de la criminalidad informática. Ambas disposiciones anticipan una serie de problemas que sin lugar a duda son de especial importancia en los documentos electrónicos.

Los antecedentes histórico-dogmáticos a los que cabe referirse ahora son los de las fotocopias y el **telefax**.

Las **fotocopias**, lo mismo que las copias, de documentos no se consideran tales en la doctrina, dado que no permiten conocer la identidad del emisor, un elemento esencial del documento, como hemos visto. Por el contrario, cuando la **fotocopia** (en su caso la copia) ha sido certificada o autenticada como copia fiel de un documento (por ejemplo

mediante una intervención notarial), el conocimiento del emisor está asegurado y el carácter documental no ha generado problemas. El BGH (Tribunal Supremo Federal alemán) ha formulado esta tesis de manera precisa: “La fotocopia (…) únicamente reproduce (como imagen) una declaración corporizada en un escrito (…) [pero] no certifica su emisor. Por lo tanto, no es posible reconocerle [a la fotocopia], sin más, la función de garantía de la corrección del contenido, que básicamente es propia de todo documento”.

Como es claro, ello no significa que la fotocopia de un documento, aunque no sea objeto de la acción idóneo de una falsedad documental, no sea un instrumento idóneo para engañar y, de esta manera, cometer un delito de estafa. No se debe olvidar que el delito de falsedad documental constituye, como tipo penal autónomo, un desprendimiento de la estafa. Lo que aquí se quiere decir es, simplemente que alterar una fotocopia no es alterar un documento, aunque sea la creación de un medio para la comisión de una estafa. Desde el punto de vista procesal, de todos modos, la fotocopia de un documento constituye una prueba válida de la existencia del documento. Por lo tanto, la fotocopia de un documento falsificado hace prueba de la falsificación del mismo, es decir, de la existencia del documento falsificado.

También generó dudas, en su momento, el **valor documental del fax**. Los libros de hace veinte años todavía no trataban de los problemas que la transmisión de un documento por fax podía generar. La doctrina se ha planteado la cuestión llegando a una conclusión afirmativa.

En este sentido se dice que “la diferencia respecto de la fotocopia consiste en lo siguiente: mientras la fotocopia sólo reproduce la imagen del documento y de la declaración en él contenida, en el caso del telefax se trata de la corporización de una declaración del emisor, remitida al destinatario con su voluntad, es decir como original, técnicamente confeccionado, destinado al receptor”.

3. LA FUNCIÓN DE GARANTÍA EN LOS DOCUMENTOS ELECTRÓNICOS

Como hemos señalado anteriormente, y como lo pone de manifiesto otros problemas generados por innovaciones técnicas, la función de garantía del documento tiene una importancia sustancial, pues los delitos de falsedad documental protegen la fe pública básicamente a través de la protección de la confianza del público en la autenticidad de la declaración documentada, es decir en la creencia justificada de que la declaración contenida en el documento pertenece al sujeto que aparece en él como su emisor. Como lo dicen Arzt/Weber “normalmente se protege la confianza en la atribución [de la declaración a un sujeto] y no la confianza en el contenido correcto [de lo declarado]”.

La autenticidad de un documento depende, por lo tanto, de la certeza de la imputación de la declaración en él contenida al sujeto que verdaderamente la realizó. La veracidad de la declaración no afecta ni altera la autenticidad, que se refiere a la relación entre el sujeto emisor y lo declarado; no se trata de la correspondencia de lo declarado con la verdad. Este último es un problema de engaño que se puede cometer con el documento, que, por eso mismo, está más allá de la consumación del delito de falsedad documental, probablemente, se podría decir, aunque con todas las cautelas, en la fase del agotamiento.

Por regla general, la firma del documento es un elemento decisivo para determinar la pertenencia de la declaración a su autor. Sin embargo, la firma no constituye un elemento esencial del documento. Pero, cabe afirmar, que es uno, probablemente el más habitual, de los elementos que permite la imputación de la declaración contenida en documento a quien es su autor. Inclusive cuando la firma no ha sido puesta de puño y letra por el emisor de la declaración, la firma puede ser el elemento decisivo de la imputación y por lo tanto de la autenticidad del documento. Esta es la razón de ser de la frecuente afirmación jurisprudencial de que los delitos de falsedad documental no son delitos “de propia mano”, es decir, no se trata de delitos en los que el disvalor de la acción se deduzca de la realización corporal de la acción por parte del autor. Todo esto

es válido también para los documentos electrónicos y por ello se han dictado las normas que actualmente regulan la firma electrónica en la UE.

Es obvio, que la firma electrónica no necesita ser puesta por el titular de ella. Puede hacerlo cualquier persona que conozca los datos de la misma. Los problemas que esto puede generar existen también en relación a la firma manuscrita. En el caso en el que la firma haya sido puesta por otra persona la doctrina ha distinguido diversos casos en los que el reconocimiento de la declaración por el titular de la firma manuscrita no se altera y en los que, consecuentemente, no cabe apreciar una falsificación del documento. Básicamente se parte de que la firma de propia mano sólo es necesaria donde la ley la requiera, es decir, allí donde la ley excluya la posibilidad de representación en la firma, como actualmente ocurre en los testamentos ológrafos.

Pero, en los demás casos una tercera persona puede ser autorizada para la reproducción de la firma por quien realiza verdaderamente la declaración documentada. En tales supuestos, cuando una persona ha firmado con el nombre o con los signos de otra, la autenticidad puede no verse afectada. Tal es el caso cuando una persona imposibilitada de firmar se vale de otra para hacerlo, así como cuando exista un poder jurídico otorgado a tales fines. En estos supuestos el documento será auténtico, pues lo decisivo no es la ejecución de propia mano de la firma, sino su “autoría espiritual”.

Desde el punto de vista conceptual la firma electrónica no difiere de la noción genérica de firma. En general, la firma es el signo característico mediante el cual un sujeto expresa su reconocimiento de la declaración documentada. Por otra parte, el concepto jurídico de firma coincide, en lo sustancial, con el uso corriente de la palabra. El Diccionario de la Real Academia no es totalmente preciso cuando dice que firma “es el nombre y apellido, o título, de una persona, que ésta pone con rúbrica al pie de un documento escrito de propia mano o ajena, para darle autenticidad, para expresar que aprueba su contenido, o para obligarse a lo que en él se dice”. Por ello, la definición del diccionario requiere ser precisada, pues, inclusive en el lenguaje ordinario, la firma no

es la escritura del nombre y apellido o del título de una persona, sino un signo propio que permite su identificación, que jurídicamente puede ser realizada también por una persona autorizada por el titular para reproducirla en señal de reconocimiento del contenido de una declaración de algún modo documentada.

De esta manera se puede considerar demostrado que los datos electrónicos que permiten la identificación del que reconoce una declaración determinada y documentada, no se diferencian sustancialmente con la noción de firma del lenguaje ordinario. Tradicionalmente la firma ha sido ejecutada de propia mano y constituye un signo gráfico personal difícilmente repetible por otro, pero, como se ha visto, puede ser ejecutada por otra persona y puede ser igualmente irrepetible cuando es realizada mediante datos electrónicos que sólo están a disposición del interesado. Admitida la autoría espiritual de la firma y del documento, resulta claro que la introducción de la firma electrónica en el tráfico jurídico no requiere ninguna modificación conceptual en el marco de la autenticidad del documento: auténtico será el documento cuando el uso del conjunto de los datos informáticos que se utilizan como medio para identificar al autor de la declaración haya sido puesto por una persona autorizada y no provenga de un abuso del secreto de las claves que lo garantizan.

En este sentido adquiere especial significación el CP, cuya posición sistemática entre los delitos relativos al mercado y a los consumidores es, cuanto menos dudosa. Este tipo penal pone bajo amenaza de pena el apoderamiento, por cualquier medio, de “datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo”, cuando tenga la finalidad de descubrir un secreto. Se trata, por ejemplo del caso de quien utiliza sin autorización los datos de la firma electrónica de una empresa con sede en Bolivia y trasmite, a una filial de Singapur, una orden de comunicarle hechos o directivas comerciales de la empresa, cuya divulgación determinará perjuicios en la competitividad de la empresa en el mercado. La cuestión de la posición sistemática del CP podría ser, a nuestros fines, en principio, secundaria, si no tuviera un efecto claramente limitativo del ámbito de protección del tipo penal.

Evidentemente los datos de creación de firma, que se define como “datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica”, constituyen un “secreto de empresa” en el sentido del tipo penal del CP. Es decir que éste presupone que los datos de creación de firma pertenezcan a una empresa; de lo contrario quedarán fuera del ámbito de protección de dicho artículo. Si bien es cierto que puede haber una empresa individual, es decir constituida por un único titular, no es menos cierto que un particular que opera jurídicamente en su propio nombre no siempre constituye una empresa.

Cuando se trate de los datos de creación de firma de un particular la protección se debe dispensar a través del CP, que sanciona al que “sin estar autorizado se apodere, utilice o modifique, en perjuicio de tercero [debería decir de otro], datos reservados de carácter personal (…) que se hallen registrados en ficheros electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado”. La protección se extiende a los datos reservados de personas jurídicas por medio del CP.

Las únicas diferencias, por lo tanto, se refieren al bien jurídico protegido y a la pena, cuyo mínimo es superior en el caso de la protección de los secretos de empresa. Ninguna de estas diferencias tiene un fundamento evidente y el legislador ha omitido explicar qué razones determinaron su decisión, sobre todo, por qué razón el apoderamiento de los datos de una persona física que no opera como una empresa, puede ser menos punible que el que perjudique a una empresa.

CONCLUSIONES

La economía de los países desarrollados se mantiene gracias a la innovación de sus empresarios a través de mecanismos de la época, al principio fueron las herramientas manuales de trabajo, después las grandes maquinas operadas por el ser humano, en nuestros días la tecnología a través de computadoras donde el trabajo es reducido al control.

En un mundo donde la tecnología ha tenido un crecimiento exponencial, es de vital importancia hacer de la tecnología una herramienta útil para el individuo, lo que nos lleva a que debe haber control social sobre ella. La globalización fue posible gracias a la comunicación sin fronteras entre ciudadanos de todas partes del mundo haciendo del Internet el nuevo mercado mundial.

La rapidez del crecimiento dejo un vacío en muchas áreas que todavía intentan acomodarse a la nueva forma de hacer negocios, como el derecho. La regulación legal de transacciones, intercambio de servicios a través de la Web en Bolivia es nula, ahí es donde nace el tema de Contratos Electrónicos Seguros.

En cuanto a validez del documento electrónico es preciso concluir que existe una tendencia mundial a dotarlo de valor probatorio, y así, son varias las directrices recomendaciones, por ejemplo de la Comunidad Europea relativas a la regulación del tema, la leyes dictadas en diferentes países al respecto e incluso el tratamiento jurisprudencia) destinado a dotarlo de valor probatorio.

Podríamos decir en términos amplios que debe entenderse por documento a cualquier objeto que contiene una información que narra, hace conocer o representa un hecho, cualquiera sea su naturaleza su soporte o su continente, su proceso de elaboración o su tipo de firma.

Técnicamente el documento electrónico es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que sometidos a un adecuado proceso, permiten su traducción a lenguaje natural a través de una pantalla o de una impresora.

La firma digital es, a mi entender, un requerimiento de los tiempos que corren y un requerimiento, también, de esta globalización que se viene dando en el mundo, desde hace ya unos años, que acarrea consigo al comercio y el cual, a su vez, le exige al derecho que avance al ritmo de esta; y es por eso que considero, que era necesaria y fue oportuna la legislación sobre este tema.

Por suerte por tratarse de un tema de esta índole, es decir ser un requerimiento de los tiempos que corren, y como ya anticipara mi introducción, se podría decir que esta presento a nuestro derecho, casi, un único inconveniente que está relacionado con la concepción que el código civil tiene de la firma como manifestación de la voluntad, una concepción que se la podría considerar obsoleta para los tiempos que corren, aunque adecuada para los tiempos del código.

Se establece que la firma es condición esencial para la existencia de todo acto bajo forma privada. Y agrega además que la firma es el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad. Al parecer dentro de los términos de lo citado no cabría la concepción de firma digital y lo que ella significa, ya que esta firma es un conjunto de números y letras encriptadas, donde existe una clave pública y una privada.

Como se demostró en el desarrollo de este trabajo, la firma digital da la característica de ser manifestación de la voluntad, igualándola, así, a la firma ológrafa.

Como ya di a entender al inicio de esta conclusión, estoy totalmente de acuerdo con la implementación del sistema de la firma digital como una nueva forma de manifestación de la voluntad, ya que considero que este significa un gran avance, no solo por lo que

puede importar al derecho, que es en definitiva la materia de este trabajo, sino también por la influencia que esto tiene en el comercio para con Bolivia, como de ésta para con el mundo, ya que esta ley coloca nuestra legislación a la par de la legislación de otros países del mundo, como ser Alemania, EE.UU., entre otros, y se nos permite así mejorar nuestras relaciones comerciales con esos países y, en la medida de lo posible, acrecentarlas.

Según sondeos realizados en la facultad de derecho, el profesional en derecho es escéptico de los procesos informáticos y de su seguridad ya que hasta ahora se prefiere todavía en el campo legal la firma manuscrita y el papel sellado. Para el universo de profesionales del ámbito legal es difícil de creer en la seguridad de la firma digital y sus procesos es por eso que en el trabajo de investigación se analiza la seguridad de los documentos electrónicos para probar la seguridad de los contratos digitales autenticados bajo una firma digital de clave publica y clave privada.

Tocando aspectos técnicos y sociales de interés para la población en general La informática y el derecho, la tecnología y el control legal de ella tiene que tornarse en un pilar fundamental para el desarrollo de Bolivia, tanto en lo económico como en lo social. El desarrollo de la investigación en un ámbito netamente técnico le dan a la monografía una visión completa de lo que debe aplicarse en cuanto al derecho informático en Bolivia.

Lamentablemente, en Bolivia no existen muchas leyes ni artículos que defiendan la informática, comercio electrónico, TIC’s, etc.; porque no existen personas que realmente luchen por esto. En Bolivia deberían existir más leyes para este ámbito, ya que es muy necesario.

Del estudio realizado, se he evidenciado que en Bolivia los documentos electrónicos tecnicamente hablando, no están reconocidos como documentos con valor probatorio, porque no reúnen los requisitos de validez en el orden jurídico, ya que no siempre

tienen su origen en un entre real que pueda ser sujeto de verificación. Dado el enorme uso y reconocida aceptación de los documentos electrónicos en el comercio mundial, y en vista que no es un asunto que solo atañe a países con desarrollos tecnológicos elevados, las pruebas en medios electrónicos cobran vital importancia en las etapas probatorias de los procesos judiciales y administrativos.

Esperamos que este estudio haya proporcionado suficiente información para dar a conocer la situación actual de los Documentos Electrónicos y de los Delitos de Falsedad Documental y contribuido al intercambio de la misma en materias de mensajes de datos, de firmas electrónicas (y digitales), de certificados digitales y de entidades y/o proveedores de servicios de certificación y registro.

Para concluir quiero decir que, espero este trabajo monográfico haya cumplido con su objetivo de informar a todo lector acerca de un tema, que a lo mejor no ha tenido la difusión que merecería tener, y que a través de este trabajo pretendo, en cierta medida, dársela.

RECOMENDACIONES Y SUGERENCIAS

El impacto que esta teniendo el Comercio Electrónico en el funcionamiento de la sociedad hace indispensable el adecuado reconocimiento legal de los acuerdos y demás contratos celebrados electrónicamente, de manera que sea posible utilizar los documentos digitales, o aquellos que no constan en el "papel tradicional", como medio probatorio, perfectamente valido, en cualquier procedimiento judicial, determinando su legalidad y validez.

Sin embargo, en la realidad muchas veces esta regulación no será suficiente, ya que las personas que van a aplicar la ley necesariamente deben conocer los limites y capacidades de las tecnologías de la informática, para lograr una adecuada valorización de los documentos electrónicos.

Asimismo, es indispensable contar con la infraestructura física de herramientas, como computadores actualizados, que permitan recibir las pruebas que consten en documentos electrónicos y que puedan determinar su legalidad y detectar la falsedad documental de estos.

Que en el sano propósito de que Bolivia no se quede a la zaga de otros Países, con relación a este adelanto tecnológico, debe ya activar los mecanismos necesarios considerar el valor probatorio del documento electrónico, así como determinar su legalidad y establecer la falsedad de estos documentos electrónicos.

ANEXOS

GLOSARIO

Acreditación. Es el procedimiento en virtud del cual la Entidad de Certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en la ley

Autenticación. Es el medio o procedimiento a través del cual es posible verificar la identidad de un emisor o un destinatario de documentos electrónicos mediante su firma electrónica.

Certificado electrónico. Es un documento firmado electrónicamente por una Entidad de Certificación que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

Clave Privada. Conjunto de datos únicos e inalterables originados en un procedimiento informático contenido en un soporte físico o lógico (como un software, una tarjeta inteligente u otros análogos) que garantiza su irreproductibilidad y confidencialidad.

Clave Pública. Conjunto de datos únicos e inalterables generados en forma simultánea y que corresponden unívocamente a los datos contenidos en la clave privada mantenida en un registro electrónico.

Comercio electrónico. Es toda transacción civil o comercial de bienes y servicios, realizada por personas naturales o jurídicas efectuada en parte o en su totalidad a través de medios electrónicos.

Contratación electrónica. Es todo contrato en el que la oferta y la aceptación se expresa y se transmite por medios electrónicos.

Correo electrónico. Es todo mensaje sea que incluya o no, archivos, datos u otra información electrónica, que se transmite a una o más personas por medios electrónicos utilizando en su origen y destino una dirección de correo electrónico.

Dato. Unidad mínima de información, que adquiere significado en conjunción con otros datos del contexto en que se originaron.

Dirección de correo electrónico. Una serie dé caracteres utilizados para identificar el origen o el destino de un mensaje de correo electrónico, compuesto por una exclusiva combinación de dos elementos, un nombre o identificador de usuario y el nombre de servidor (de correo electrónico) o de dominio, siendo otorgada y administrada por un proveedor de correo electrónico.

Dispositivo de creación de firma. Es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

Dispositivo de verificación de firma. Es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

Documento electrónico. Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

Encriptar. Proteger archivos expresando su contenido en un lenguaje cifrado.

Emisor. Persona natural o jurídica a la cual se le atribuye la generación, comunicación o archivo de un mensaje de datos o documento electrónico.

Firma electrónica. Son los datos en forma electrónica consignados a un documento electrónico, adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al titular de la firma en forma unívoca con el documento electrónico, e indicar que aprueba y reconoce la información contenida en el mismo. La firma electrónica asegura la integridad, autenticidad y no repudio.

Medios Electrónicos. Soporte digital para el envío, recepción, modificación o almacenamiento de información.

Signatario. Es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Sitio web. Es un conjunto de archivos electrónicos y páginas Web referentes a un tema en particular, que incluye una página inicial de bienvenida, generalmente denominada página de inicio, con un nombre de dominio y dirección en Internet específicos. Empleados por las instituciones públicas y privadas, organizaciones e individuos para comunicarse con el mundo entero.

Sistema de información. Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Titular del certificado electrónico. Es la persona que contrata con una Entidad de Certificación la expedición de un certificado, para que sea nombrada o identificada en él. Esta persona mantiene bajo su estricto y exclusivo control el procedimiento para generar su firma electrónica.

BIBLIOGRAFÍA

- ALONSO PÉREZ, “El delito de falsedad documental cometido por autoridad o funcionario público”, LL 2010

- BACIGALUPO ZAPATER, “El delito de falsedad documental”, Madrid 2009

- BOLDOVA PASAMAR, Estudio del bien jurídico protegido en las falsedades documentales, Granada 2010

- BOLIVIA. Ley del Ministerio Público. Nro. 1469. Titulo Preliminar. Principios Generales.

- BOLIVIA. Honorable Congreso Nacional. "Ley de Documentos, Firmas y Comercio Electrónico". 2010.

- CABANELAS GUILLERMO, Diccionario Enciclopédico Usual, Editorial Heliasta, Buenos Aires-Argentina. 2009

- CALLE RODRÍGUEZ, “Teoría general sobre la falsedad documental y selección de la jurisprudencia sobre falsedad documental, con especial referencia al documento mercantil”, CPC 2008

- CASTILLO ALVA José Luís “LA FALSEDAD DOCUMENTAL”. Edición Agosto de 2009, Editorial San Marcos, Juristas Editores, pp.243

- COBO DEL ROSAL, “Esquema de una teoría general de los delitos de falsedad, CPC (56) 2007

- CÓRDOBA RODA, “Las falsedades documentales. Perspectiva jurisprudencial”, Problemas específicos de la aplicación del Código Penal, Madrid 2009

- GACETA OFICIAL DE BOLIVIA. Constitución Política del Estado de Bolivia. Gaceta Oficial. 30-06-10. Primera Edición, La Paz, Bolivia, 2010.

- GACETA OFICIAL DE BOLIVIA. Código Penal de Bolivia. Edición Oficial. 2004.

- GACETA OFICIAL DE BOLIVIA. Ley Nº 2175. Ley de 6 de Febrero de 2001. Ley Orgánica del Ministerio Público

- HERNANDEZ SAMPIERI Roberto, FERNANDEZ COLLADO Carlos, BAPTISTA LUCIO Pilar, Metodología de la Investigación, Editorial McGraw Hill, México,2003

- LLORIA GARCÍA, “El documento como objeto material de los delitos de falsedad. Su concepto y naturaleza”, LH-Casabó, 2007

- LUZÓN CUESTA José María “COMPENDIO DE DERECHO PENAL. PARTE ESPECIAL”. 12º Edición, Tercera Conforme al Código Penal de 1995, 2010, DYKINSON, Madrid - España, pp. 421

- MARTÍNEZ-PEREDA RODRÍGUEZ, “La falsedad documental en el ámbito de la función pública”, CDJ 2008

- MOSTAJO MACHICADO MAX, los 12 Temas del Seminario Taller de Grado y la Asignatura CJR-000 Técnicas de Estudio, Primera Edición, La Paz-Bolivia, 2005.

- MUÑOZ CONDE Francisco “DERECHO PENAL. PARTE ESPECIAL”. Decimoséptima edición, 2009, tirant lo blanch, Valencia – España, pp. 932

- OSORIO. Diccionario Jurídico. 8va. Edición actualizada y ampliada. Editorial Interamericana. México DF – México. 2009.

- RODRÍGUEZ RAMOS, “Falsedades documentales: interpretación actualizada”, LH-Torío López, Granada 2009

- RUÍZ VADILLO, “Falsedad y defraudación por abuso informático”, CDJ 2010

PROPUESTA DE LEY EN MATERIA DE DOCUMENTOS Y FIRMAS ELECTRÓNICAS Y EL ORDEN PÚBLICO ECONÓMICO BOLIVIANO

1. El Título I del Proyecto, sobre disposiciones generales, resume el objeto y ámbito de aplicación de la ley, que alude a los documentos electrónicos, a su posibilidad de ser firmados de la misma manera, al valor legal que tendrán, a la forma legal de almacenarse y a los requisitos de las empresas que, celebrando contratos de prestación de servicios de certificación electrónica con los signatarios y previamente acreditadas, habilitan técnicamente para la firma de documentos electrónicos.

Junto con consignarse como principios generales inspiradores y de interpretación los de neutralidad tecnológica, asimilación jurídica, equivalencia funcional y homologación de soportes, acreditación obligatoria, compatibilidad internacional, objetividad, transparencia y proporcionalidad, se definen conceptos claves tales como documento electrónico, firma electrónica, certificado electrónico, Entidades Certificadoras y signatarios o suscriptores.

2. En el Título II se regula y se valida de manera general el uso de cualquier documento electrónico, de cualquier naturaleza (pública o privada, comercial, registral, notarial, etcétera), siempre que sea firmado electrónicamente, con el respaldo de un software o certificado emitido o generado por una Entidad Certificadora previamente autorizada o acreditada. Se regula, homologa con el soporte papel y se valida “el continente” de cualquier documento ahora soportado digital o electrónicamente, cualquiera sea la naturaleza de los datos o su “contenido” (mercantil, comercial, registral, bancario, judicial, público, etcétera). En otros países se ha llegado a normar específicamente los documentos nacionales de identificación, pero el proyecto que se presenta opta por no regular casos específicos sino por habilitar la generalidad posible de documentos electrónicos.

Se define además que debe entenderse por documentos electrónicos "originales" y cuáles son los requisitos al efecto, se valida su impresión en soporte papel, se permite la desmaterialización de documentos y su conversión en electrónicos, se regulan los requisitos generales de los repositorios de almacenamiento de documentos, se habilita el caso particular de los registros y archivos judiciales o notariales para salvar cualquiera duda de interpretación, se contemplan las notificaciones electrónicas y, por último, se regula el valor o mérito probatorio de los documentos electrónicos que sena firmados electrónicamente.

Al contemplarse la existencia legal de documentos "públicos" electrónicos, se establecen -ampliamente- los lineamientos básicos de todo proceso de "Gobierno Electrónico" que requiera la sustitución de los documentos soportados en papel y que en el futuro se desarrolle en Bolivia.

3. El Título III, a continuación, norma la validez de las firmas o claves electrónicas generadas para ser aplicadas sobre un documento electrónico en base a un software o "certificado electrónico" que previamente emite una Entidad Certificadora.

Siguiendo un principio fundamental, se declara la homologación legal entre firmas manuscritas y electrónicas, se establecen requisitos legales esenciales y algunas presunciones, se consignan

obligaciones mínimas que deben cumplir los signatarios o suscriptores y las causales de caducidad de una firma electrónica.

Luego de permitirse expresamente el uso de firmas electrónicas por parte de todos los órganos públicos del Estado boliviano, se definen los requisitos esenciales y legales de todo certificado electrónico, la emisión de ellos para los representantes de las personas jurídicas, su vigencia, caducidad, posible suspensión temporal y eventual revocación (es el llamado "ciclo de vida" de un certificado).

4. En el Título IV se establece, en cuanto a la naturaleza jurídica de la Entidades Certificadoras de identidad electrónica -no se certifica cada firma generada sino la persona del signatario que la genera, y esto es un error conceptual recurrente-, que sólo podrán serlo personas jurídicas de derecho privado o público.

Al permitirse expresamente que los servicios públicos se consideren acreditados por la ley y puedan desempeñar funciones de Entidades Certificadoras sólo en el contexto de su competencia, creemos que se establecen nuevamente los lineamientos básicos de todo proceso de "Gobierno Electrónico" que en el futuro se desarrolle en Bolivia.

Conforme al proyecto, todas las Entidades Certificadoras que operen en Bolivia deberán ser previamente acreditadas, sea por el órgano competente o por la ley en el caso de los servicios públicos. Así, siempre existirán procedimientos de comprobación de la identidad de los firmantes y mayores garantías en los procesos de certificación electrónica de identidades y de firma de documentos.

Se trata de funciones de asignación de fe pública, lo que debe ser resguardado principalmente en el contexto del orden público económico. Consecuencialmente, sólo existirán dos especies de certificados electrónicos o programas de respaldo para la generación de firmas electrónicas, a saber, (i) los adquiridos a empresas que -por asignar fe pública y respaldar en Internet “la identidad” de los firmantes o signatarios- siempre serán acreditadas por el ente fiscalizador; y, (ii) los emitidos por los órganos públicos exclusivamente para operar dentro de su competencia y sólo respaldar la identidad electrónica de sus funcionarios. Y se definen requisitos generales para operar, mismos que deberán ser evaluados al acreditarse o autorizarse tal operación, y las obligaciones esenciales de toda Entidad Certificadora. Consecuencialmente, se regulan sus responsabilidades y la forma del posible cese de sus funciones.

5. Por último, el Título V regula la existencia de una Entidad Acreditadora y fiscalizadora de Entidades Certificadoras, función que se le asigna al Ministerio de Economía. A este se le califica como órgano competente, quien administrará un registro formal ad hoc que también se crea, aplicará un arancel de acreditación que se contempla, eventualmente cancelará la autorización otorgada e incluso podrá aplicar sanciones.

Es, por cierto, una diferencia esencial con diversas normas del Derecho Comparado el carácter obligatorio del procedimiento de acreditación, de manera tal que en Bolivia no podrán operar libremente empresas no autorizadas o extranjeras, con lo cual, se logra resguardar idóneamente

una función de asignación de Fe Pública en el contexto de los documentos y transacciones electrónicas.