Primer Congreso Internacional de Derecho Informático

y Tecnológico del Paraguay

Asunción, 24 y 25 de octubre de 2005

"LA AUTORÍA Y AUTENTICIDAD EN LA COMUNICACIÓN VÍA INTERNET"

Título de la ponencia:

Connotaciones jurídicas de la firma electrónica y digital

Ponente: María José Viega (Uruguay)

Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UR). Profesora de Derecho Telemático. Cursos del Posgrado de Derechos Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Miembro de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay. Miembro del Instituto de Derecho Informático (UR). Autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

Abstract:

Partiendo de los nuevos paradigmas en cuanto al tiempo, espacio y acceso como consecuencia del proceso de desmaterialización, se realiza un análisis del documento tradicional y el documento electrónico, planteando sus similitudes y diferencias. A los efectos de la validez de los mismos y de la seguridad en las transacciones electrónicas, se conceptualiza la firma ológrafa o tradicional, para llegar a su equivalente funcional que es la firma electrónica y la firma digital.

“Connotaciones jurídicas de la firma electrónica y digital”(*)

Dra. Esc. María José Viega

1. Introducción

La historia del Derecho, manifiesta el Profesor Losano, ”está condicionada por las tres revoluciones de la escritura, de la imprenta y de la ordenación electrónica de datos. En las tres revoluciones el Derecho es afectado a través del Lenguaje. En la primera se pasa de la expresión oral a la escrita; en la segunda, de la escritura manual a la impresa y en la tercera de la escritura tipológica, impresa o mecánica al lenguaje tratado electrónicamente”[1].

Y este lenguaje electrónico, que constituye la forma de comunicación en el ciberespacio, está signado por el cambio de tres elementos que son: el tiempo, el espacio y el acceso. El tiempo, debido a la inmediatez de las comunicaciones, a los diferentes usos horarios, el “ahora” es el tiempo presente en todas partes. El espacio telemático está signado por la inexistencia de fronteras geográficas y por la internacionalidad de los fenómenos. Y el acceso se convierte en la herramienta más poderosa en este proceso de cambios, donde pierde importancia la propiedad y se torna relevante “tener acceso a”[2].

La importancia del acceso se debe al fenómeno de la desmaterialización y éste “responde a la necesidad de cambio y adaptación que va a implicar para el desarrollo de la telemática a un concepto filosófico –antes que jurídico-. En efecto, es físicamente palpable por nuestros sentidos una gradual y ineludible desmaterialización de la realidad. Se observa con nostalgia, o satisfacción para algunos, el derrumbe de lo físico (el alto grado de la absolencia de lo material, la poca permanencia y duración de los objetos y la pérdida de su individualidad) y de lo ético o valorativo lo cual hace recordar la frase del pensador decimonónico: “todo lo sólido se desvanece en el aire”. El fenómeno evolutivo de la desmaterialización al decir de ILLESCAS ORTIZ resulta equiparable a una alteración contractual de similar importancia a la que se produjo

---

Primer Congreso Internacional de Derecho Informático y Tecnológico del Paraguay. Asunción, 24 y 25 de octubre de 2005.

[1] CARRASCOSA LOPEZ Valentín. “Valor Probatorio del Documento electrónico”. Revista Informática y Derecho. Volumen 8. UNED Centro Regional de Extremadura, 1995. Página 133.

[2] VIEGA RODRÍGUEZ María José y RODRÍGUEZ ACOSTA Beatriz. “Documento electrónico y firma digital. Cuestiones de seguridad en las nuevas formas documentales”. E-book editado por Viega & Asociados. Montevideo, Mayo 2005.

con la sustitución de la tabla o tablilla de piedra o barro por el papiro y la del pergamino por el papel"[3].

Este fenómeno podemos observarlo en la despersonalización de las relaciones comerciales, en los medios de pago electrónico, en la transferencia electrónica de fondos, en el documento electrónico, en la desmaterialización de los títulos valores, en el auge del comercio electrónico o desnudez del papel, lo que ha llevado a que se hable de la crisis de la sociedad del papel y se proponga un nuevo modelo social o cultural donde el papel será reemplazado por medios informáticos con soportes digitales y transferencia electrónica[4].

Este es el marco donde toma cuerpo la firma electrónica y digital, tema que hoy nos convoca, pudiendo ser analizada desde diferentes enfoques. Si bien, como se refiere el título de la ponencia, nos vamos a referir a las connotaciones jurídicas de la misma, será necesario realizar conceptualizaciones y precisiones técnicas.

La invitación de hoy a reflexionar sobre la firma digital, debemos enmarcarla en un ámbito más amplio, que es la contratación informática. La problemática que se plantea es compleja, tiene relación directa con el consentimiento, ya que necesitamos tener la convicción de que esa persona que no está físicamente presente, es quien dice ser y que es capaz de obligarse contractualmente.

Definimos al contrato telemático como aquel contrato cuyo objeto es cualquier bien o servicio que se encuentre en el comercio y cuya negociación y perfeccionamiento se celebran a través de la utilización del instrumental telemático.

El tema los vamos a desarrollar entonces, dando un panorama teórico general del documento y la firma electrónica. Cuando decimos firma electrónica, nos estamos refiriendo al género, siendo la firma digital una especie de firma electrónica.

Esta es una apreciación de relevancia en la medida que el análisis de la vulnerabilidades tecnológicas y las diferentes medidas que apuntan a lograr su seguridad, nos interesa desde el punto de vista de la protección de la información, de la integridad de la misma, ya sea a la hora de trasmitir documentos electrónicos, de celebrar contratos o de ejecutar los mismos.

[3] HERNÁNDEZ AGUILAR Alvaro. "Comercio y contratación electrónica". IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.
[4] HERNÁNDEZ AGUILAR Alvaro. "Comercio y contratación electrónica". IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.

La seguridad informática tiene como objetivo la protección del dato, lo que implica que el mismo mantenga la siguientes cualidades[5]:

a) La integridad: implica que el contenido, ya sea que se encuentre en un computador o que circule a través de una red, permanezca inalterado. En caso de sufrir modificaciones que sea por persona autorizada y que exista en el sistema la constancia de esta modificación, que hará viable su control al realizarse auditorías.

b) La disponibilidad: u operatividad de la información es su capacidad de estar disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware o el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria[6].

c) La confidencialidad o privacidad: implica el conocimiento de la misma exclusivamente por las personas autorizadas. Esto se logra a través de control de acceso, sistemas criptográficos y métodos apropiados de conducción de las personas, los documentos y los medios de almacenamiento de datos.

Los niveles de protección son cuatro[7]:

1º. Legal o ético: consiste en la protección provista por la legislación y la obligación moral que nuestra condición humana nos impone.

2º. Auditoria y controles del sistema informático: es la protección provista por las políticas, la organización y la metodología de contralor de las personas, los procedimientos operativos y los programas de aplicación.

3º. Seguridad física y ambiental: medios de protección contra incendios, robos, estado de las instalaciones.

4º. Seguridad lógica: protección prevista por dispositivos de hardware y software.

Es esta última clase de seguridad la que nos interesa abordar a los efectos del análisis del documento electrónico.

---

[5] VIEGA María José. "Seguridad Informática". Boletín Electrónico de Viega & Asociados Nº 8 Mayo de 2004 www.viegasociados.com

[6] A.S.S. BORGHELLO, Cristian Fabián. Director de Tesis: Ing. GOTTLIEB Bernardo. Asesor científico: MINGO Graciela. "Tesis Licenciatura en Sistemas: Seguridad Informática sus implicancias e implementación". Universidad Tecnológica Nacional. Setiembre, 2001. www.cfbsoft.com.ar

[7] DE LA FUENTE Reynaldo. "Aportes a la Seguridad y Privacidad en Informática y Comunicación de Datos". Polo Ltda. 2da. Edición Actualizada. Montevideo, 1995.

Los elementos relevantes en la contratación electrónica están dado por que la transferencia de información sea a través de un sistema seguro, para lo cual es importante tener en cuenta los siguientes elementos: confidencialidad, integridad de la transacción, identificación de las partes y seguridad de la transacción.

2. Documento tradicional y electrónico

Desde un punto de vista funcional, dice Carnelutti que el documento es "una cosa que sirve para representar a otra"[8]. Se hace énfasis entonces en el aspecto probatorio del documento.

Otra posición, sustentada por Siegel, y aceptada por Núñez Lagos, define al documento como "una exteriorización del pensamiento, perceptible por la vista", y así, éste último consigna como requisito de la grafía, entre otros, la visibilidad, esto es que el documentum sea apreciable por la vista. El disco fonográfico y la escritura Braille quedan excluidos. Si bien se trata de medios de comunicación, lo cierto es que en ellos es muy difícil el reconocimiento de su autor y agrega un concepto, sobre el cual desde ya, queremos llamar la atención, y relativo a que aún no se ha encontrado un equivalente funcional de la firma[9].

Podemos decir que un documento tiene las siguientes características:

a) ocupa un lugar en el espacio,

b) se ubica en un tiempo específico,

c) tiene relación entre el autor y lo querido y expresado por éste y

d) un valor probatorio (propio del documento jurídico).

El Derecho, ha tomado las pruebas a partir de esta materialidad (instrumentos, informes periciales) o bien, a partir de la expresión hablada (deposiciones, sean personales, como la confesión, o de terceros, como los testigos). Pero naturalmente las expresiones habladas no son perdurables, y para que lo sean deberán transformarse en escritas (trascripción al papel de lo dicho, lo cual luego será firmado), de lo contrario, se corre el riesgo de que se pierda en el tiempo (se por olvido, sea por fallecimiento de quien depone)[10].

[8] CARNELUTTI, Francesco, "Sistema de derecho procesal civil". Buenos Aires (1944), tomo II, página 414.
[9] GAETE GONZALEZ Eugenio Alberto. "Instrumento público electrónico". Editorial Bosch. España, abril de 2000. Página 71.
[10] GAETE GONZALEZ Eugenio Alberto. "Instrumento público electrónico. Ob. cit., página 35.

Según la opinión del Dr. Guibourg la escritura sobre papel, tiene varias cualidades que la han tornado irremplazable: durabilidad, inalterabilidad, legibilidad y debidamente individualizada y firmada posee, además confiabilidad[11].

Giannantonio define el documento electrónico, distinguiendo:

En sentido estricto: el que queda almacenado en la memoria del computador y no puede llegar a conocimiento del hombre sino mediante el empleo de tecnología informática.

En sentido amplio: el que es procesado por el computador por medio de periféricos de salida y se torna así susceptible de conocimiento por el hombre.

Pero el punto crucial es el origen del documento. Tenemos que tener en cuenta si el mismo ha sido generado por el hombre y almacenado posteriormente o se reproduce por intermedio del ordenador o si se admite que el propio computador genere el contenido del documento a partir de alguna combinación de la información disponible con ciertas instrucciones que operan en sus sistema.

Las características del documento electrónico son:

a) es generado o emitido a través de un computador.

b) Sólo puede hacerse público mediante tecnología informática.

c) Es inmaterial.

d) Para que tenga valor deberá estar sujeto a medidas técnicas de seguridad.

Los diferentes autores se encuentran divididos en sus opiniones referente a los mismos. Algunos entienden que los registros informáticos no constituyen un documento escrito basándose en las diferencias entre uno y otro.

Pero existen aquellos que les encuentran muchas similitudes y opinan que el documento electrónico es otra forma de escribir, se habla de una nueva forma de alfabetización. Sin lugar a dudas ambos tienen razón, existen diferencias, pero también existen aspectos en que ambos se parecen.

Las **diferencias** entre ambos podemos decir que son las siguientes:

a) Un documento escrito no puede concebirse sin el soporte material que es el papel. Sin embargo esto no siempre fue así. Existen a lo largo de la historia muchísimos tipos de documentos que nos demuestran la existencia de un hecho y que no necesariamente fueron realizados en soporte papel. Por otra parte, el papel, tan

[11] GUIBOURG Ricardo y otros. "Manual de Informática Jurídica. Editorial Astrea. Buenos Aires, 1996. Páginas 235 y siguientes.

importante en nuestra época no lo ha sido en el pasado, y no veo razones de peso por lo que deba serlo en el futuro. Y aquí no podemos obviar el problema de la seguridad, que, para quienes escribían en las cavernas, sobre la piedra, el papel no les resultaría seguro en absoluto, al igual que como hoy, muchos dudan de la seguridad de los soportes informáticos[12].

Al respecto nos dice Bill Gates: "Durante más de 500 años, todo el volumen del conocimiento y de la información humanos se ha almacenado en forma de documentos de papel. (...) el papel estará siempre con nosotros, pero su importancia como medio de buscar, preservar y distribuir información está disminuyendo ya"[13].

El documento electrónico se diferencia básicamente de aquel *per cartam*, desde el punto de vista estructural. Se transforma su corporalidad, sus elementos materiales cambian, de tal manera, que su soporte será un sistema de conformación electrónica, expresado a través de un lenguaje binario. Tocante a su aspecto funcional, continuará siendo el mismo, *una cosa que docuit*, que enseña, designa algo[14].

b) Otra diferencia que se enuncia es que el registro informático puede ser fácilmente modificado, mientras que el documento escrito puede resultar más difícil de modificar sin dejar huellas en él. Creo que el gran avance de la técnica, no sólo en materia informática, desmiente esta afirmación. Las fotocopiadoras láser color, por ejemplo, permiten realizar copias de una calidad tal que nos resultaría muy difícil distinguir el original de la copia a simple vista.

c) Otro punto importante es la firma. La firma ológrafa no es la única forma de identificar a una persona, ésta también es falsificable y sólo un perito calígrafo nos dirá que grado de originalidad tiene. La firma electrónica ya es una realidad entre nosotros, también la firma digital, así como las empresas certificadoras de las mismas. Esto ha planteado un gran desafío para los notarios, que hasta el momento eran los únicos investidos para realizar certificación de firmas.

d) Una diferencia importante es que en el documento informático desaparece la diferencia entre la copia y el original. Esta es quizá una de las apreciaciones más valederas, porque no es posible distinguir entre un documento informático original y su copia.

En las comunicaciones telemáticas la pregunta que se plantea es cual es el documento original, es el que posee el que lo envía o el documento que se recibe. Sin

[12] VIEGA, María José. "La influencia de la informática en la actividad probatoria y su regulación en Uruguay". Ponencia presentada al VII Congreso Iberoamericano de Derecho e Informático. Lima, abril de 2000.
[13] GATES, Bill. "Camino al futuro", Ed. Mac Graw-Hill, España, 1996, Segunda Edición.
[14] GAETE GONZALEZ Eugenio Alberto. "Instrumento público electrónico. Ob. cit., página 177.

lugar a dudas habrá que crear una forma de distinguir un original electrónico de su copia, lo que es importante a nivel notarial, debiendo crearse estándares a tales efectos, diferenciándolos por ejemplo con una determinada secuencia de código u otro mecanismo informático.

Con relación a quines hacen hincapié en las **similitudes** y entendiendo como documento al electrónico, como nueva forma de documental, podemos decir que:

a) Una de las hipótesis posibles, es que constituye una forma nueva de documento en consideración a que desde los albores de la humanidad éste se ha caracterizado por tener una realidad, que comenzó revelándose a través de materiales consistentes, como las tablillas de arcilla mesopotámica, los pairos egipcios, las tablillas de madera chinas o egipcias, para pasar luego al pergamino, a la seda y finalmente al papel de pulpa, como se lo conoce en la actualidad[15].

b) Se considera en nuestra época a la informática como un nuevo lenguaje, hablamos de que en este siglo que se ha iniciado, quienes no conozcan el manejo informático serán considerados analfabetos, ya que podemos considerar el lenguaje binario como un alfabeto. El nivel de educación en esta área crece a pasos agigantados.

c) El lenguaje binario es criticado porque no puede ser leído directamente. La música también se escribe en forma diferente, y es leída sólo por aquellos que saben solfeo, sin embargo las partituras musicales no han planteado problemas. Tengamos presente que la ley no establece con que signos debe manifestarse la escritura[16].

d) El carácter de indestructibilidad del soporte no constituye una exigencia legal, también el papel se destruye, por el fuego o la humedad. Con respecto a la posibilidad de modificación del documento informático frente a lo irreversible que puede ser el documento escrito, quizá podría ser cierto cuando pensamos en los Protocolos de los escribanos realizados en tinta negra de buena calidad, pero no lo será si pensamos en un documento enviado por fax, que al ser recibido en un papel estándar de transferencia térmica tiende a ser borrado. Y la realidad nos demuestra que hoy, a nivel mundial, un alto porcentaje de contratos se realizan por fax, a través de redes privadas, por correo electrónico o a través de Interne[17]t.

e) Interactividad de los textos informáticos. La posibilidad de añadir comentarios, nuevos datos a un documento, lo distingue del documento en papel. Esto ha dado

[15] GAETE GONZALEZ Eugenio Alberto "Instrumento Público electrónico. Editorial Bosch. España, abril, 2000. Página 181.
[16] VIEGA, María José. “La influencia de la informática en la actividad probatoria y su regulación en Uruguay”. Ponencia presentada al VII Congreso Iberoamericano de Derecho e Informático. Lima, abril de 2000
[17] VIEGA, María José. “El documento electrónico y la firma digital”. Trabajo final del Posgrado en Contratación electrónica. Universidad de Buenos Aires, 2001.

origen al hipertexto, lo que da dinamismo al documento, el mismo deja de ser lineal, perdiendo importancia el principio y el final.

3. La firma: concepto y clasificación

En Roma el concepto de firma era diferente, se realizaba a través de una ceremonia llamada manufirmatio, por la cual, luego de la lectura del documento por su autor o el notarius, era desplegado sobre una mesa y se pasaba la mano por el pergamino en signo de aceptación. Solamente después de cumplir esta ceremonia se estampa el nombre del autor[18].

En el sistema jurídico visigótico existía la confirmación del documento por los testigos que lo tocaban (chartam tangere), signaban o suscribían (firmatio, roboratio, stipulatio). (...) La "suscriptio", representaba la indicación del nombre del signante y la fecha, y el "signum", un rasgo que la sustituye si no sabe o no puede escribir. La suscriptio daba pleno valor probatorio al documento y el signum debía ser completado con el juramento de la veracidad por parte de uno de los testigos. Si falta la firma y el signo del autor del documento, este es inoperante y debe completarse con el juramento de los testigos sobre la veracidad del contenido[19].

En la Edad Media se implantaba el sello real, el cual pasó posteriormente a las clases nobles y privilegiadas.

3.1 Firma ológrafa o tradicional

Según el Dr. Eduardo Couture en su "Vocabulario Jurídico", firma es: " el trazado gráfico, conteniendo habitualmente el nombre, apellido y rúbrica de una persona, con el cual se suscriben los documentos para darle autoría y obligarse con lo que en ellos se dice"[20]. Cuando una persona "firma" un documento en papel está manifestando su voluntad y lo que hace es dibujar sobre él una serie de símbolos que lo identifican.

[18] CARRASCOSA LOPEZ Valentín. "Valor Probatorio del Documento electrónico". Revista Informática y Derecho. Volumen 8. UNED Centro Regional de Extremadura, 1995. Página 140.
[19] LOPEZ Fernando Ernesto. "De la caligrafía a la criptografía". Ponencia presentada al IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.
[20] COUTURE, Eduardo J.. "Vocabulario Jurídico". Ediciones Depalma, Buenos Aires, 1983.

Pablo Palazzi[21] define la firma como "*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*".

La firma en este caso cumple diversas funciones, lo cual dependerá de la naturaleza del documento:

- Establecer la autoría del propio texto.
- Aceptar las obligaciones que surgen de un texto.
- Adherir a lo expresado por otro.
- Determinar la presencia del mismo

Cuando un Escribano certifica una firma lo que está asegurando es que la persona que firma es quien dice ser, que lo hizo libre y conscientemente, que firmó dicho documento en un lugar y día determinado.

Dice Palazzi[22] que: "Si se encuentra un medio que reemplace a la firma ológrafa en ambientes digitales, éste nuevo medio deberá cumplir con las funciones tradicionales de la firma. Estas son: (i) indicativa: informa acerca de la identidad de un autor; (ii) declarativa: se refiere al acuerdo respecto al contenido del acto; (iii) probatoria: permite vincular al autor con el signatario".

3.2 La firma electrónica

La firma electrónica en sentido amplio es "cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones de la firma manuscrita"[23].

Así es que el artículo 7 de la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI o UNCITRAL) establece que: "Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos;

[21] PALAZZI, Pablo Andrés. "Firma digital y comercio electrónico en Internet". VI Congreso Iberoamericano de Derecho e Informática. Libro de Ponencias. Montevideo – Uruguay, l998.
[22] PALAZZI, Pablo. "Firma digital y comercio electrónico en Internet". Ob. Cit.
[23] MARTINEZ NADAL Apol-lonia. "Comercio electrónico, firma digital y autoridades de certificación". Civitas, Madrid 1998.

b) si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje incluido, cualquier acuerdo pertinente".

Consagrándose aquí el criterio de la "equivalencia funcional".

La firma electrónica a su vez puede tener diferentes técnicas para firmar un documento, así tenemos las siguientes:

a) Código secreto o de ingreso: es la necesidad de una combinación determinada de números o letras, que son sólo conocidas por el dueño del documento, o lo que todos usamos, por ejemplo en los cajeros automáticos, es el famoso PIN o Personal Identification Number;

b) Métodos basados en la Biometría: se realiza el acceso al documento mediante mecanismos de identificación física o biológica del usuario o dueño del documento.

La Biometría es la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. La biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz)[24].

Con relación a las diferentes técnicas utilizadas para firmar electrónicamente un documento, podemos distinguir:

a) Una técnica disponible es el uso de una tableta sensible y un lápiz magnético conectados a un PC donde se registra la presión, velocidad y coordenadas donde el operador apoya el lápiz. Esos datos se combinan matemáticamente para formar la "firma electrónica" de la persona. Posteriormente, se puede comparar esa firma almacenada con otra para verificar si pertenecen a la misma persona[25].

b) Emisión de calor: se mide la emisión de calor de un cuerpo (termograma) realizando un mapa de valores sobre la forma de cada persona.

[24] BORGHELLO Cristian Fabian. "Seguridad Informática. Sus implicancias e implementación". Tesis Licenciatura en Sistemas. Universidad Tecnológica Nacional. Setiembre de 2001. Capítulo 2, página 11. www.cfbsoft.com.ar

[25] BALAY, Guillermo. "Enfoque informático del Decreto N° 65/998". Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.

c) Otra técnica de firma electrónica disponible en el mercado podría ser el registro de la huella digital y de ciertos factores biológicos de la piel que identifican unívocamente a la persona. El dispositivo consiste en un tablero donde la persona coloca su dedo. Allí se digitalizan la huella y los parámetros biológicos del dedo de la persona, de tal forma que es imposible reproducirlos salvo que se obligue a la persona a colocar su dedo en el dispositivo[26].

d) Verificación de la voz: la dicción de una (o más) frase es grabada y en el acceso se compara la voz (entonación, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, envejecimiento, etc[27].

e) Verificación de patrones oculares: Estos modelos pueden ser basados en patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0). Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

3.3 Sistemas de Cifrado

Históricamente, podemos destacar los cifrados por sustitución y por transposición.

a) Cifrado por sustitución: cada letra o grupo de letras se reemplaza por otra letra o grupo de letras. En el caso de sustitución monoalfabética cada letra se corresponde con otra arbitraria del alfabeto, existiendo entonces 26 claves diferentes. Se descifra fácilmente usando la frecuencia relativa de las letras.

c) Cifrado por transposición: Reordena las letras pero sin cambiarlas. Por ejemplo la transposición columnar, en la cual la clave es la palabra o frase que no contiene letras repetidas, enumerándose las columnas en el orden alfabético de las letras de la clave. Es fácil descifrarlo conociendo la clave y ordenando las columnas.

3.4 La firma digital

En el perfeccionamiento del cifrado de mensajes, llegamos a lo que se conoce como criptografía. La criptografía es la ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones.

---

[26] BALAY, Guillermo. “Enfoque informático del Decreto N° 65/998”. Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.

[27] BORGHELLO Cristian Fabian. “Seguridad Informática. Sus implicancias e implementación”. Ob. Cit., Capítulo 2, página 12. www.cfbsoft.com.ar

La criptografía es una rama de las Matemáticas -y en la actualidad de la Informática y la Telemática- que hace uso de métodos y técnicas matemáticas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a los criptosistemas que permiten asegurar cuatro aspectos fundamentales de la seguridad informática: confidencialidad, integridad, disponibilidad y no repudio de emisor y receptor[28].

Esta consiste en un sistema de codificación de un texto con claves de carácter confidencial y procesos matemáticos complejos, de manera que para el tercero resulte incomprensible el documento si desconoce la clave decodificadora, que permite ver el documento en su forma original. De ahí es que surgen dos tipos de criptografía:

a) de clave secreta o simétrica: las partes en los dos procesos de cifrado y descifrado comparten una clave común previamente acordada. Debe ser conocida solamente por ambas partes para evitar que un tercero ajeno a la operación pueda descifrar el mensaje transmitido. Esta tiene como desventaja que si se realiza en redes abiertas (Internet) puede ser interceptada por un tercero y además no sirve si el tercero que deba participar no tiene la clave.

b) de clave pública o asimétrica: este sistema fue creado en 1976 en Estados Unidos y consiste en que ambas partes deben tener un par de claves que no son iguales sino que son asociadas, o sea, una clave privada en poder del titular, conocida sólo por él, y una clave pública, que se relaciona matemáticamente con la clave privada, y que puede estar tranquilo que sólo el destinatario va a poder descifrar su mensaje.

La accesibilidad a las claves pueden satisfacerse mediante la distribución manual (disquetes, CD) pero es un sistema no seguro.

La firma digital entonces, es “aquella que se crea usando un sistema de criptografía asimétrica o de clave pública”[29].

Como consecuencia del auge de las firmas digitales, ha sido necesaria la creación de una infraestructura de las claves, surgiendo así la Infraestructura de Clave Pública (ICP), más conocida por su nombre en inglés, como PKI (public key infrastructure). Por lo tanto, decimos que ésta es el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados digitales que pueden

[28] RAMIÓ AGUIRRE Jorge. “Curso de Seguridad Informática”. Universidad Politécnica de Madrid.
[29] MARTINEZ NADAL Apol-lonia. “Comercio electrónico, firma digital y autoridades de certificación”. Ob. Cit.

ser utilizados para autenticar cualquier aplicación, persona, proceso u organización de una red de empresa, extranet o Internet[30].

La idea de una infraestructura de clave pública es simple, consta de varios componentes y elementos.

1. Los llamados componentes de una Infraestructura de Clave Pública, pueden ser:

a) Autoridad Certificante Raíz

b) Autoridades de Registro

c) Archivo

2. Los elementos de la PKI son:

a) Sistema de autenticación

b) Políticas de Certificación

c) Personal capacitado

La criptografía continúa desarrollándose y actualmente se habla de que un cubo de cristal podría ser la llave criptográfica perfecta. Este cubo tendría el tamaño de un sello de correos y podría ser la llave criptográfica más segura para las operaciones económicas. Cada cubo contiene miles de pequeñas gotas de plástico que se leen con un láser especial. Cada gota de plástico tiene una forma y orientación única. Cuando el láser pasa a través de ellas, dibuja y proyecta una forma determinada en una superficie, que entonces se traduce en una llave criptográfica de 2400 bits de longitud. Si se altera la posición de las gotas la llave cambia completamente y deja de ser útil[31].

La encriptación de doble clave, debido a los avances en el aumento de potencia de procesamiento de los ordenadores, se convierte día a día en un sistema menos seguro. Científicos del MIT han demostrado este nuevo tipo de llave criptográfica, usando un objeto físico en lugar de una función matemática, confiando en que dicho objeto sea virtualmente imposible de duplicar. Sus desarrolladores confían en que dentro de poco podrán disminuir el tamaño de estos cubos e incluirlos como medida de seguridad dentro de las tarjetas de crédito.

En 1997 en Bonn (Alemania) se realizó una reunión de los países de la Unión Europea, elaborándose la Declaración gubernamental de Bonn sobre redes de información mundial, en la que se valoró positivamente la opción de cifrar la

[30] RODRÍGUEZ Beatriz. "Autoridades de certificación". XIII Ciclo de Encuentros Técnicos Regionales". Rivera, 26 de julio de 2003. Edita Asociación de Escribanos del Uruguay.
[31] http://enlaceweb.net/mailman/listinfo.cgi/interlink

información transmitida vía redes usando sistemas criptográficos de acuerdo con las leyes vigentes, considerándose a la criptografía "de carácter fuerte", aludiendo con esta expresión a claves compuestas por números de cifrados amplios, como un requisito imprescindible para el desarrollo de la Sociedad de la Información y el Comercio Electrónico (www.echo.lu/bonn/conference.html)[32].

4. Reflexión final

La tecnología nos ofrece no solamente nuevas formas para entablar relaciones jurídicas electrónicas y telemáticas, sino también las herramientas para operar con una seguridad óptima.

Acostumbrarnos a adoptar medidas de seguridad informática no nos parece sencillo y no confiamos en ellas. Pero este no es un hecho o creencia con un sustento real, sino que es necesario un cambio de mentalidad colectiva, un proceso de adaptación social.

Desde el punto de vista jurídico es fundamental la consagración a texto expreso del pleno valor probatorio del documento electrónico y de la posibilidad de utilización de las firmas electrónicas y digitales como equivalente funcional de la firma ológrafa.

Montevideo, 18 de setiembre de 2005

[32] JIJENA LEIVA Renato y otros. "El Derecho y la Sociedad de la información: la Importancia de Internet en el Mundo Actual". TEC de Monterrey. México, 2003. Página 195.