Algunas nociones de la *firma digital* en Paraguay

Por ***Javier Rojas Wiemann***[*]

Sumario

El *comercio electrónico* presenta una novedosa herramienta para la seguridad y confianza de las transacciones realizadas por medios electrónicos de una manera nunca antes conocida por el ser humano y que impacta fuertemente en las Ciencias Jurídicas, avasallada por la sociedad de la información. Es decir, tenemos por un lado una realidad indiscutible en el que el *espacio virtual*, o también denominado ciberespacio o –con el apelativo que nos gusta, de McLuhan, la *aldea global*-, ha invadido notoriamente los negocios, las interrelaciones mercantiles y en fin, las usanzas propias de la tradicional compra y venta, haciendo que la tienda de la esquina de nuestro barrio pueda ofrecer y vender sus productos a consumidores grandemente distanciados.

¿Eclipsa esto al Derecho Comercial?, ¿lo coloca en situaciones de difícil resolución?, ¿qué propone ante la avalancha de las técnicas y tecnologías modernas?

Efectivamente las respuestas no se hacen esperar y como indicábamos emerge con unas herramientas únicas con notables funcionalidades y propiedades que serán soportes eficientes de la validez jurídica del comercio electrónico.

La firma electrónica a nivel mundial resultó ser una herramienta eficiente y marcadamente su modalidad –en particular para nuestro país, pues en otras latitudes existen denominaciones disímiles-, la *firma digital* con certificación, prácticamente conquista un espacio de seguridad jurídica importantísima para la contratación vía electrónica.

Abstract

The electronic commerce, or E-commerce presents itself as a innovative tool regarding security and sureness in transactions via electronic means in a way never known before, strongly

[*] Abogado litigante. Egresado de la Universidad Católica Nuestra Señora de la Asunción, Campus Itapúa. Miembro del Instituto Itapuense de Derecho Procesal, del Instituto Iberoamericano de Derecho Procesal, de la Asociación de Abogados de Itapúa, de la Asociación Paraguaya de Derecho Procesal Constitucional, de la Asociación Mundial de Justicia Constitucional y del Colegio de Abogados Procesalistas Latinoamericanos. Autor de varias publicaciones. Correo electrónico: jrw@sanagustin.com.py. Twitter: @JAVIERROJASWIEM

impacting Legal Science, constantly bombarded by the actual cyber society. What this means is that we have on one side, an unquestionable reality in which the *virtual space*, also known as *cyberspace*- or as Mc Luhan refers to it; *global village*-, has notoriously invaded business, commercial relations, and the usual sales and trading methods, making it possible for even the smallest venture to offer and sell their products to largely distanced consumers.

Will it outshine Commercial Law? Will it present difficulties for problem solving in this legal area? What proposals will Commercial Law present towards the great amount of new techniques and technologies emerging?

The answers to these questions are offered by the technological tools we have mentioned previously, which with their unique functions and characteristics will become reliable supports to offer legal validity in electronic commerce matters.

Globally, the electronic signature turned out to be an effective instrument, and specifically, in its kind- particularly in our country, considering that its denomination is not the same for every country-, the digital signature with its formal certification, practically conquered the safe legal area, vital to contracts done electronically.

1. ¿Qué es la firma digital?

Para desbrozar esta figura tomaremos dos aristas no diferentes pero que sí responden a materias distintas, a saber una técnica y otra positiva.

1.1. Definición legal

Según nuestra normativa la *firma digital* es una firma electrónica certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría (artículo 2º de la Ley Nº 4.017).

La precisión concierta la base misma de este sistema, que es la *firma electrónica,* pero con la distinción ineluctable de la certificación digital proveniente del prestador de servicios de certificación habilitado debidamente, lo que conlleva por lo menos tres efectos característicos de

esta herramienta, a saber, la autenticidad del autor y del mensaje, la integridad y el no repudio. La certificación y todos sus pormenores los veremos en otra oportunidad.

La definición legal comprende decididamente particularidades únicas e inigualables que hacen de la *firma digital* una herramienta de gran confianza, seguridad y valor jurídico, incluso superando –en algunas facetas- a la firma manuscrita.

1.2. Noción técnica

Se requiere tomar parte de la *Informática,* del *Derecho Informático y de las Tecnologías* para obtener en esa combinación un conocimiento básico de lo que significa *firmar digitalmente.* De allí que la trasmisión de mensajes de datos por medios electrónicos, utilizando métodos criptográficos para seguridad no es otra cosa que obtener del documento una huella digital a través de una función *hash*, para que el mismo no solamente pueda ser detectado si fue modificado o alterado en su tránsito, sino también vincular al emisor con dicho archivo, gracias a la verificación con el par de claves por una autoridad certificadora. La función *hash* es un algoritmo matemático que permite calcular el valor resumen de los datos a ser firmados digitalmente. *Hash* es un algoritmo lógico que, al ser aplicado a un archivo, *devuelve un patrón determinado de letras y números*[1]. La *firma digital* es un proceso técnico que aplica una función matemática para obtener una copia exacta de datos informáticos (prácticamente lo que se conoce como una huella digital)[2], no en el sentido de contenido, sino más bien como una radiografía del documento electrónico, lo que permitirá posteriormente a través del certificado digital detectar si existió o no alguna modificación o alteración en dicho mensaje durante su tránsito.

La fórmula del par de claves hallada por los expertos permite que el firmante utilice una clave privada que solo él conoce para la encriptación, y luego el destinatario con la clave pública otorgada por la autoridad certificadora, corrobora la validez del mensaje. Estos mecanismos están elaborados a través de algoritmos de seguridad, hoy día bastante avanzados y con amplio éxito en el ámbito. Dependiendo de la modalidad utilizada también el emisor tiene la opción de introducir la

---

[1] **PAGÉS LLOVERAS**, R. (2015). El Derecho Procesal Electrónico en la Provincia de San Juan. En: CAMPS, C. E. (Director). *Tratado de Derecho Procesal Electrónico* (págs. 881-991). Buenos Aires: Abeledo Perrot.

[2] *«Por medio de una función matemática se genera una huella digital del documento digital, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, que se enviará adjunta al mensaje original (o se mantendrá asociada al documento digital así firmado). Esa huella o marca es única para dicho documento y sólo pudo ser producida por quien estaba en poder de la clave privada»* (**ALTMARK**, D. R & **MOLINA QUIROGA**, E. (2012). *Tratado de Derecho Informático.* Buenos Aires: La Ley, t. I, p. 565).

clave pública del destinatario por lo que el receptor será el único que podrá desencriptar el mensaje introduciendo su clave privada que sólo es conocida por él mismo.

Al «firmar», lo que en puridad se genera detrás de lo que podemos ver en el monitor de nuestra computadora, es una secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con determinado algoritmo. Así, ese correo electrónico o mensaje de datos lo denominaremos *documentos digitales* o *electrónicos* a los que se vinculará una *firma digital* que cuenta con un código de verificación impreso cada vez que sea aplicado dicho algoritmo (*función hash*), siendo improbable, a través de medios técnicos, que ese código pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo, como prácticamente imposible que otro mensaje de datos produzca el mismo código de verificación.

Hasta aquí fue cumplido recién uno de los dos procesos para *firmar digitalmente.* El primero, lo transcribimos precedente y el segundo tiene relación con la verificación que es posible gracias al certificado digital. Recuérdese que el titular de una firma digital la emite porque cuenta de forma exclusiva con un certificado digital otorgado por una entidad certificadora habilitada.

Entonces, el *proceso de firma* implica que el titular encripta el documento digital con su clave privada, enviando al destinatario y el *proceso de verificación de la firma*, opera con la recepción por parte del destinatario quien descodifica o desencripta con la clave pública del emisor y comprueba (verifica) la integridad del documento digital o también, que el titular encripta con la clave pública del destinatario y éste la desencripta con su clave privada. Mencionamos que existen otros usos y por supuesto pronto surgirán muchos más sofisticados, debido a que no se escatiman esfuerzos para mejorar la seguridad informática.

1.3. Esquema general

Vamos a ser más prácticos pues no creemos que sea necesario complicar el tema, que en definitiva de por sí es sencillo. Desde siempre fue un problema identificar al emisor, establecer con seguridad tal cuestión e igualmente asegurar el contenido del mensaje.

No ocurre con frecuencia –a modo de ejemplo de control de seguridad- que presentado un cheque a la vista en ventanilla del banco girado, el cajero toma el teléfono y llama al librador para comprobar que efectivamente esa es su voluntad. Si ello ocurre, ciertamente operó una verificación

única e inigualable, siempre y cuando también tengamos la certeza que aquel que respondió del otro lado de la línea haya sido el librador.

Sirvámonos de otro ejemplo más ejercitado a este respecto. El que utiliza el servicio de Internet conocido como *correo electrónico* sabe que para ello requiere previamente habilitar una casilla, también llamada correo electrónico y es costumbre nombrar esa dirección electrónica con el mismo nombre de la persona que la utiliza o de la compañía o de la sección de la empresa respectiva. Así tenemos por citar: tiberio_romano@webmail.com, o empresa@empresa.com, o info@empresa.com, y también, el más común, contacto@empresa.com. De allí, que al recibir un correo electrónico de esa persona o empresa, automáticamente damos por sentado que la emisión proviene de quien se dice su titular.

Sin embargo, ello puede no ser así. Las cuentas de correo electrónico son vulnerables, e incluso, duplicables y no se tiene mínimamente certeza de quién está del otro lado, lo que hace inseguro tal modo de comunicación. Además, cuando tratamos con terceros con quienes nunca tuvimos algún contacto, desconocidos y hasta –en la mayoría de los casos- personas de diferentes lugares, extranjeros, entre otros, en la realidad es alto el porcentaje de incertidumbre en tales interacciones.

En la Guía de la CNUDMI es explicado esto, señalándose que el creciente empleo de técnicas de autenticación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación ha planteado la necesidad de crear un marco jurídico específico para reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de dichas técnicas modernas[3].

Por ello fue necesario implementar otro modo más seguro de transmisión de mensajes de datos, de archivos y documentos que garanticen no solamente la integridad del mismo sino también la solvencia en la detección del emisor. En eso consiste la *firma digital,* en brindar esa seguridad en las comunicaciones y transacciones. A través del uso de este servicio la *firma digital* queda equiparada a la manuscrita, salvo excepciones previstas en la ley.

2. Análisis del concepto normativo

[3] Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001. Capítulo I. A. Finalidad, punto 3.

Más arriba anotamos la definición legal. Ahora, antes de ingresar a otros detalles nos parece oportuno analizar el concepto, considerando su relevancia y tomando en cuenta que la ley imprime una noción extensa que evidentemente implica una serie de cuestiones de distintas índoles.

2.1. Es una firma electrónica

La *firma digital* es una firma electrónica por lo que conviene no confundirlas. No es cualquier *firma electrónica,* sino que la ley le da una categoría especial, jerarquizándola como: «certificada». De ahí se deduce la principal diferencia entre las mismas.

La esencia de la *firma digital* es la certificación digital que comprende el módulo en el que la entidad proveedora del servicio proceda a la verificación de la autoría e integridad del firmante, por lo que sin el *certificado* emitido de una prestadora habilitada, prácticamente no es válida ni eficaz probatoriamente como tal. El certificado da paso a la verificación del documento o comunicación electrónica que está vinculado a la *firma digital* y por ello hace presumir dos cuestiones que seguidamente analizaremos dentro del texto del concepto normativo.

¿Por qué es una *firma electrónica*? La respuesta a esta consulta es compleja, dado que primeramente debemos esquivar la confusión propia que generan estos términos, a la luz de otras legislaciones, por una parte, y por otra, que la una es el género y la es otra la especie.

Respecto a lo primero, cabe explicar el fenómeno a nivel mundial de las numerosas modalidades adoptadas por las legislaciones de los distintos países para distinguirlas, en el caso que las diferenciaran o de añadirles determinados calificativos como «simple», «avanzada» o «reconocida», entre otros. Muchas legislaciones no se ocupan de tratar de la firma electrónica u otras denominan de ese modo a la firma digital, y en fin, como ya se indicó. Es imperioso reconocer que no hay uniformidad sobre el tema.

También –en lo atinente a la segunda cuestión- mencionamos precedentemente que la firma digital es una *firma electrónica* sin detenernos demasiado en tal aserción, debido a que es imperioso no confundirlas, pues no son lo mismo, como también, comprender que evidentemente la *firma electrónica* es el género y la *digital* vendría a ser una especie más significativa, valiosa y con

mayores efectos legales que la primera. Dice SILVA-RUIZ, en resumen: la firma digital es un tipo de firma electrónica que utiliza una criptografía de llaves en par conocida, en inglés, como PKI[4].

La *firma electrónica* es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital; mientras que la *firma digital* también es todo lo citado precedentemente, pero con «certificación» emanada de una certificadora licenciada.

2.2. Es certificada

La infraestructura de una firma digital requiere de una autoridad de certificación habilitada, que es un organismo que actúa en carácter de tercero, realizando dicha operación como un ente regulador, autorizado al respecto por nuestra Ley Nº 4.017 y las reglamentaciones del Ejecutivo.

Las certificadoras licenciadas tendrán tal trascendencia para la efectividad de estas tecnologías que sus responsabilidades están enfocadas en pilares técnicos y jurídicos. En el primero centran la gestión y la actividad en cuanto a contar con la tecnología de criptografía asimétrica que le permitirá emitir certificados de firma digital, a las políticas de infraestructura de firmas digitales, planes de contingencias, confiabilidad, publicidad de las listas de certificados revocados, entre otros. Las facetas jurídicas entrañan responsabilidades civiles y en determinados casos, incluso penales.

Es por ello que debemos recordar que la legislación equipara para ciertos casos la firma *digital* a la *manuscrita,* pero la primera llega a tal calidad una vez que el proceso previsto fuere cumplido del modo determinado en el que interpreta un rol primordial el certificado digital.

Ahora bien, el concepto de «*prestador acreditado*» nuevamente dispara una batería de nociones a tener en cuenta, decantando la posibilidad de que cualquier prestador de dicho servicio logre tal calidad y por el contrario, según lo dispone el capítulo correspondiente de la ley sobre los Prestadores de Servicios de Certificación, únicamente los emitidos por aquellos habilitados logran el reconocimiento correspondiente.

---

[4] **SILVA-RUIZ**, P. F. (2002). Firma electrónica en Puerto Rico y algunos problemas. En AA.VV., *Revista de Derecho Comparado. Comercio Electrónico* (págs. 93-101). Buenos Aires: Rubinzal – Culzoni.

Estos *prestadores de servicios* no solo emiten certificados sino que acreditan la titularidad de los mismos[5], permitiendo de ese modo la necesaria confianza, imprescindible a estos efectos.

En otros términos, antes de la existencia propia de la *firma digital*, tendrá que haber sido habilitado una entidad certificadora según los parámetros exigidos en la legislación vigente.

2.3. Es creada por el firmante y sujeta a su control

Otro factor determinante con respecto a la firma digital es el de su creación. A diferencia de otros documentos electrónicos, éste necesariamente es generado a través de un proceso motivado e ineludible. Al igual que cualquier otra actividad, «firmar» digitalmente exige en forma imperiosa y manifiesta que el documento o mensaje de datos pase por dicho proceso de exteriorización, a fin que reúna los efectos técnicos y jurídicos esperados.

Cabe aclarar que la *firma digital* será vinculada al *documento digital, electrónico, correo electrónico, mensaje de datos* o cualquier otro de esta índole. Agreguemos a lo expuesto precedentemente que esa labor o gestión representa para el titular o firmante la utilización de medios que mantiene bajo su exclusivo control. LORENZETTI expone que siendo un elemento de imputación de autoría, es lógico que se requiera que esté bajo el control del titular, ya que sólo él es quien decide qué declaraciones de voluntad son suyas. Concluye que por eso es necesario *que la firma pertenezca únicamente a su titular y se encuentre bajo su control exclusivo*[6].

JUANES añade que *la conservación del secreto de quien genera la clave privada es esencial* para mantener su carácter privado, y ello impide su falsificación o mal uso, ya que no es posible acceder a la firma digital sin conocer la respectiva clave con la cual fue generada[7] y agreguemos, que es también irrealizable la deducción de la clave privada a través de la clave pública, pues no tienen vinculación o relación alguna entre sí.

2.4. Es verificable

---

[5] **FERNÁNDEZ DOMINGO**, J. I. (2006). *La firma electrónica. Aspectos de la Ley 59/2003, de 19 de diciembre.* Madrid: Reus, p. 23.

[6] **LORENZETTI**, R. L. (2002). La ley argentina de firma digital. En AA.VV., *Revista de Derecho Comparado. Comercio Electrónico* (págs. 103-141). Buenos Aires: Rubinzal – Culzoni.

[7] **JUANES**, N. (2003). *Comercio electrónico y seguridad de las transacciones.* Córdoba: Advocatus, p. 46.

Con lo anterior tenemos que es creada por el titular quien la mantiene bajo su control, de manera que lo identifique y relacione a los datos.

El cotejo concibe en principio dos procesos; el primero gracias a la certificación, es posible la detección posterior de cualquier modificación del documento digital, verificándose de tal manera la integridad del mismo; el segundo, también merced al certificado digital, la comprobación de la identidad del titular, lo que conlleva a un efecto probatorio denominado *de no repudio,* es decir, esto último impide que el emisor desconozca la integridad del documento y su autoría.

3. La comparación de las características principales de la firma tradicional y las modernas

Este servicio comenzó a tener éxito desde que acredita la autenticidad e integridad del documento que está vinculado a su autor, por lo que a partir de allí cosecha incontables beneficios.

Las interrogantes han surgido de este modo. ¿Podrá la firma digital reemplazar a la firma manuscrita?, ¿tienen las mismas características?, ¿cuál es la más importante?

Las preguntas abundan y algunas respuestas podremos brindar en estas líneas.

Dentro del análisis que corresponde efectuar, previamente encontraremos aquello atinente a los elementos que componen la "firma".

Elementos:

La firma tiene varios elementos, pero analizaremos en particular tres de ellos.

El primero es el objetivo (material o formal), el siguiente es el subjetivo, es decir intencional o intelectual. El tercero se aparta de esa línea y más bien encierra las aplicaciones, que es el funcional.

El elemento formal es el signo personal, es decir el componente material de la firma y el grafismo mismo. El funcional, es el elemento de identificación y autenticación, que opera como resultado de la expresión de cierta voluntad.

Por último, el elemento subjetivo, también conocido como el *animus signandi*, presupone la intencionalidad, la expresión de la voluntad ratificatoria del firmante.

Realizaremos el cuadro sobre la base de esos factores agregándole al elemento funcional otras características que le son propias, a saber: la *identificación* y la *autenticación*, que son más

conocidas, y además, la *confidencialidad*, *integridad* y *no repudio*, que surgen actualmente con el desarrollo de las modernas tecnologías.

Las características de la *firma digital* conforme se observa son superiores no solamente a la *firma electrónica*, sino también a la misma *firma* tradicional.

Cabe aclarar que este resumen no necesariamente es compartido por toda la doctrina, dado que existen diferenciaciones importantes en cuanto a las perspectivas adoptadas, principalmente en cuanto a la *identificación* y a la *autenticación*, por lo que podrían encontrarse notas diferentes a las expuestas precedentemente.

3.1. La firma como signo personal y de identificación

Indudablemente que la esencia misma de la rúbrica de cada persona conlleva esa connotación individual que a la vez hace a la identificación del signatario. El mismo artículo 43 del Código Civil establece que toda persona tiene derecho a suscribir con su nombre sus actos públicos y privados, en la forma que acostumbre a usarlo, e incluso, toda persona tiene derecho a adoptar la firma que prefiera.

Todos los modos de suscribir cumplen de algún modo con esta particularidad, principalmente la *manuscrita* y la *digital*. En lo que respecta a la *firma electrónica* cabe mencionar que la misma justamente adosará todo aquello que sirva como algún signo característico del firmante.

La *firma manuscrita* comprende escribir los nombres y apellidos, o solamente el apellido, o un garabato entendible o inentendible (como ocurre muchas veces), u otras modalidades a gusto del suscribiente. Un autógrafo encierra los elementos característicos de la individualidad caligráfica de su autor[8].

La *firma electrónica* en el espectro propio en el que es creada, ya representará en cuanto a las variedades propias de la electrónica o la informática o incluso, la biometría, también incontables formas de suscripción.

[8] **GONZÁLEZ GÓMEZ**, P. M. (2006). *Equiparación del comercio electrónico en el Derecho Civil.* Buenos Aires: Nova Tesis, p. 54.

Las más estándares, contadas como ejemplo, son las individualizaciones realizadas por las personas que al utilizar el correo electrónico en la parte final del mensaje colocan alguna imagen de la empresa y sus datos, como ser nombre y apellido, dirección, teléfono y otros.

La *firma digital* al respecto adolece también como la *electrónica* de las libres modalidades indicadas para las *manuscritas* y está más bien supeditada al certificado digital y las funciones de autenticación propias de la misma.

3.2. La firma como expresión de voluntad

Como fue señalado en párrafos anteriores, aquel que estampa su rúbrica lo hace con *intención* y conocimiento, ya sea obligándose de algún modo o expresando su conformidad.

Como sea del texto o contexto, tanto para la firma *manuscrita* como para la *digital,* signar en tal sentido acarreará fuertes implicancias para el firmante, y con menos energías en el caso de la *electrónica,* que para el efecto su eficacia es inferior.

Para las relaciones jurídicas, estampar la *firma* implica una manifestación inequívoca que para cada modalidad existente en la actualidad, como hemos indicado, representará diferentes alcances.

Cuando *firmo,* ¿expreso mi voluntad? La respuesta es harto conocida en cuanto a la firma manuscrita, pues superando los vicios prescriptos en la legislación civil, se entiende que quien suscribe efectivamente plasma su intención y ello conlleva el conocimiento de lo signado y sus efectos. Ahora, tenemos nuestros reparos en lo atinente a la *firma electrónica*, dada la vulnerabilidad muy propia de los sistemas actuales de comunicación y es por eso que la ley expresamente impone que en caso de ser desconocida corresponde a quien la invoca acreditar su validez (artículo 18 de la Ley Nº 4.017). Sobre la *firma digital* no hay duda, salvo las impugnaciones fundadas en la pérdida del control de la misma o los mismos vicios del consentimiento.

3.3. La firma como autentificación

Para nuestro enfoque, la *autentificación* es el proceso que permite saber la vinculación entre el firmante y el mensaje, es decir, conocer la autoría del emisor y allí afianzar que el mensaje procede de quien se dice que lo remite.

Así, para cada tipo de firma este proceso opera de un modo diferente. Para la firma manuscrita en ciertos casos se requerirá un reconocimiento posterior, aunque para la mayoría de los actos, la misma conlleva el testimonio respectivo.

Casi lo mismo ocurre con la firma *electrónica*, dado que su misma definición comprende a un conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación.

Pero el distingo en particular está centrada en la firma *digital*, que cuenta con una presunción *iuris tantum* que le brinda mayor eficacia preliminar que las demás y comprende con el mismo proceso su fuerza probatoria, sin necesidad de ninguna actividad posterior de reconocimiento o ratificación.

4. Sus características esenciales

Antes de proseguir es apropiado mencionar que HOCSMAN los trata como *principios de la firma digital* y existen razones para ello, pero nos apartamos de tal categorización porque consideramos que son más bien métodos o propiedades sistemáticas antes que exigencias fundantes. De allí que para nuestra opinión son *características esenciales de la firma digital* y no principios.

Hemos compartido las peculiaridades que asisten a cada tipo de firma, pero en particular, nos corresponde en esta instancia examinar con más detalles las que son propiedades de la firma digital, que en ese orden son tres, a saber la *autenticidad*, *integridad*, y *no rechazo* o *repudio*, mientras que una cuarta es añadida por alguna doctrina y resistida por otras, dado que la *confidencialidad* no guarda un resquicio fundamental como las anteriores, pero es usual su tratamiento.

4.1. Autenticidad

Diremos que esta función de seguridad garantiza la *identidad* del que remite el mensaje y permite *asegurar* que ese mensaje procede de quien se dice que lo envía[9].

La *autentificación* tiene directa vinculación con la *identificación* del emisor y con la inserción de la *firma digital* en un mensaje de datos, la prerrogativa dirige directamente la cuestión al plano de las presunciones de autoría o autenticidad.

Señalan los tratadistas ALTMARK y MOLINA QUIROGA que la *presunción de autoría implica* que el documento firmado digitalmente se presume válido y emitido por su autor identificado por su firma digital, y como *consecuencia en el caso de que alguien invoque la falsedad del mismo,* es decir, quien eventualmente impugne dicha validez y presunción de autoría, cargará con la prueba de la falsedad que invoca[10].

HOCSMAN expresa que la infraestructura de *firma digital* y la expedición de *certificados* tienen como principal finalidad *garantizar la identidad de la persona* que firma digitalmente[11].

De igual modo, la utilización de esta *firma* para acceder a determinados servicios en la Red o autenticarse ante servidores de la misma, evita ataques comunes, utilizándose lo que se denomina los analizadores de protocolos (*sniffers*).

Entonces cabe sostener que la identificación del firmante es unívoca e incluso, casi imposible de ser suplantada. Si el titular de la firma la mantiene bajo su control y protección, ya sea ello con su clave privada o a través de la tarjeta, podrá estar seguro que el proceso matemático utilizado por estos sistemas efectúa una tarea que impide la falsificación o suplantación de la identidad. Esta particularidad es la que dio tanto éxito a este servicio. Para el comercio electrónico resulta lógicamente una herramienta de inestimable valor.

La *firma digital* permite garantizar la identidad del emisor de la transacción. La revolución y el impacto que genera esta herramienta abreva principalmente en las ventajas que ofrece, siendo una de ellas la garantía de la autoría del mensaje. Gracias a su composición técnica y al proceso generado a través de los diferentes algoritmos de este sistema, la *firma digital* añadida a un mensaje de datos o documento electrónico, vincula exclusivamente a su emisor.

El destinatario tiene la seguridad que el mensaje recibido procede efectivamente del remitente, debido a que el *certificado digital* que integra dicha comunicación así lo garantiza.

---

[9] **MARTÍNEZ NADAL**, A. (2001). *Comercio electrónico, firma digital y autoridades de certificación.* (3ra. ed.) Madrid: Civitas ediciones SL, p. 37.
[10] **ALTMARK**, D. R & **MOLINA QUIROGA**, E. (2012), t. I, p. 598.
[11] **HOCSMAN**, H. S. (2005). *Negocios en Internet.* Buenos Aires: Astrea, p. 389.

Este *certificado* es un *documento electrónico* asignado por la Autoridad de Certificación que relaciona la identidad del titular, en este caso en su carácter de emisor pero también puede serlo como receptor, con una clave pública.

Cualquier persona puede verificar dicha información, dado que la clave pública queda exclusivamente a cargo de la Autoridad correspondiente.

¿Y por qué esta presunción o carácter tan firme? La respuesta está ajustada a las políticas de certificación que exigen y obligan a las prestadoras de servicios que instalen protocolos eficientes y adecuados para individualizar e identificar previamente a la persona física que solicite una firma digital, ya sea ello en carácter personal o en representación de un ente societario.

La reglamentación prevista para las autoridades certificantes impone necesariamente que van a *requerir que el solicitante de un certificado presente todos los datos respaldatorios necesarios para garantizar* su *identidad*[12], esto reiteremos, previamente a la emisión del certificado.

4.2. Integridad

Es un elemento que comprende la inalterabilidad del mensaje durante su tránsito. Así, este atributo de *integridad*, consiste en la mitigación del riesgo de alteración del mensaje de datos. Durante el tránsito por la red es factible la manipulación del mensaje de datos, de cualquier forma y únicamente con esta función, el destinatario verifica si ello aconteció o no.

La *firma digital* garantiza de una forma extraordinaria la integridad del mensaje electrónico, a base de unas funciones matemáticas que son obtenidas prácticamente al momento de la creación, como una huella, más conocida como *huella digital* y que luego permiten su verificación por parte del destinatario.

Gracias a esa función, el emisor del mensaje tiene la certeza que el documento será verificado por el destinatario corroborándose su inalterabilidad, como también el receptor está seguro que lo que está receptando no fue adulterado durante la transmisión, y si lo fue, podrá también tener la precisión de ello.

Al realizarse el cotejo respectivo entre el documento emitido y el recibido, lo que la aplicación hace es determinar si existe o no alteración alguna entre estos, o sea, si son o no iguales.

---

[12] **HOCSMAN**, H. S. (2005), p. 389.

Así, se detecta cualquier modificación en su almacenamiento o manipulación telemática del documento o datos firmados.

Como hemos explicado en el cuadro demostrativo, la *integridad* resulta ser una característica aplicable únicamente a la *firma digital*, y no así a la *electrónica* y mucho menos a la *manuscrita.*

Al advertir cómo funciona todo el proceso de *signar digitalmente*, hemos señalado que el acto de *firmar* genera a la vez una ecuación matemática irreproducible del documento. Esto en concomitancia significa que ni una firma digital es igual a otra, por más que el emisor siempre sea el mismo.

Luego, esa ecuación matemática es conocida como *huella digital*, producida a través de la función hash. Ese complejo archivo firmado digitalmente es la suma del documento original más un algoritmo cifrado del mismo documento, un resumen matemático del mismo, encriptado con la clave pública del receptor.

Remitido y ocurre que en el transcurso de su tránsito por la red, sufriere alguna modificación o alteración de cualquier tipo, por mínima que fuere, el destinatario al comparar ese algoritmo y el creado a partir del documento original, corroborará la integridad del mensaje.

La interrogante más pronta a esta cuestión es ¿y qué interesa que el documento responda o no a un estándar de integridad? Para el ámbito probatorio la *presunción de integridad* que la misma legislación le recarga al documento con firma digital lo privilegia, pues se lo presume válido e íntegro, salvo prueba en contrario, y a la vez, no está obligado a demostrar la integridad del documento quien la invoca, sino a la inversa, la carga pesa sobre quien afirma la alteración y en tal sentido impugne el documento.

Trayendo a colación un caso práctico, ocurrido no hace un tiempo atrás, diremos que dos importantes comerciantes venían realizando en forma periódica transacciones comerciales. Uno, encargaba los pedidos que del otro, y previo depósito del monto respectivo en seña, enviaba las mercaderías al lugar convenido. Un tercero logró infiltrarse en la comunicación vía electrónica que mantenían los dos comerciantes e introdujo en uno solo de los mensajes, un número de cuenta diferente al que el vendedor había puesto. El comprador depositó las sumas requeridas y esperó la mercadería, que nunca llegó.

Intimó al vendedor a que despache los productos comprados, a lo que el vendedor respondió que primeramente y como estaban acostumbrados, deposite las sumas correspondientes en pago.

Ambos, al momento, cayeron en la cuenta que habían sido estafados, sin existir siquiera un atisbo que evidencie lo acontecido.

El caso mencionado se produjo antes de implementada la firma digital, y con ella, aquella estafa no hubiera sido posible, pues cualquier alteración en la comunicación hubiera sido descubierta inmediatamente.

4.3. No repudio

La legislación atribuye a este medio la imposibilidad para el emisor de negar el envío del mensaje de datos y para el receptor la de refutar su recepción.

Aclaremos que este atributo está fortalecido en los anteriores citados, dado que según la presunción de *autoría*, está asegurada la identidad del remitente y que el mensaje procede del mismo, y de acuerdo a la presunción de *integridad*, que dicho mensaje no sufrió adulteración, manipulación o alteración alguna en el tránsito.

De allí que no tiene mayor sentido para el emisor impugnar un documento con *firma digital*, salvo determinados y excepcionales casos.

¿Quién firmó puede luego alegar que no lo hizo? Dependerá cómo signó.

La *firma manuscrita*, ha ocurrido y seguirá ocurriendo siempre en el fuero tradicional, es negada en ocasiones por su autor y tras una pericia caligráfica queda al descubierto la falacia.

Con la firma *electrónica* la trama cae en una esfera específicamente de medios de pruebas que coadyuven en caso de ser desconocida, pues corresponderá a quien la invoca acreditar su validez.

Pero no están dadas tales posibilidades con la *firma digital*, siendo esta otra de las fortalezas distinguibles sobre las citadas anteriormente. A diferencia de las anteriores, ésta conlleva el impedimento del repudio, por lo que su autor imprime expresamente su *identidad* y *autoría*, agregándose a estas dos facetas en el la *integridad* mencionada anteriormente. MOSQUERA HINESTROZA alude que de este modo el método permite identificar al iniciador de un mensaje de datos e indicar que el contenido cuenta con su aprobación[13].

¿Por qué el impedimento para el repudio? Y la respuesta reposa en el mecanismo propio de esta herramienta que le irradia certeza jurídica para las partes contratantes, lo que motiva a compilar

[13] **MOSQUERA HINESTROZA**, J. S. (2015). *Comercio electrónico*. Bogotá: Ediciones Nueva Jurídica, p. 39.

como regla y razonablemente, en exiguos casos y por eventos o circunstancias extraordinarias, las excepciones. El mecanismo induce con certeza que quien dice firmar, así lo hizo.

Ocurre, como se anotó al tratarse sobre la *firma electrónica,* que el signatario podía desconocer en cualquier momento lo enviado y pesa sobre quien invoca la validez de la firma, la carga de probar la validez de la misma.

Pero a través de la *firma digital* ello encuentra otra derivación formal, ofreciendo la presunción legal a su favor. Al emisor no le asiste la posibilidad de retractarse de lo enviado, salvo que aduzca hechos determinados que logren destruir tales presunciones. Estos casos son la pérdida del control de los datos de creación de la firma digital y el uso no autorizado, lo que llevaría al entredicho.

4.4. Confidencialidad

Aclaremos que ésta no es exclusivamente una característica propia de la *firma digital* como las anteriores, sino más –a nuestro criterio- es un complemento, marcadamente efectivo y valioso para las comunicaciones y de allí en más también para estos medios.

El criterio de *confidencialidad* en puridad es bastante extenso como para procurar medirlo con la simpleza de nuestro cuadro demostrativo y valga por ello esta explicación, a fin de evitar confusiones innecesarias. Para el efecto tomemos algunos ejemplos ilustrativos. En el ámbito de las comunicaciones por vías electrónicas, gracias a la criptografía, el secreto en estas interacciones es posible. En particular, un determinado documento electrónico debidamente encriptado es confidencial y únicamente lo abrirá quien cuente con la clave respectiva, salvo la vulneración por expertos. El correo tradicional también es confidencial y de hecho cuenta con enormes protecciones constitucionales y legislativas de orden penal para los resguardos correspondientes.

Sin embargo, el correo postal con un tanto de picardía, osadía o lisa y llanamente con dolo, dejará de ser privado ante la violación y ruptura del sobre que contiene dentro la epístola que automáticamente es vulnerada. Es decir, su nivel de seguridad es ínfimo y el documento podrá ser interceptado, alterado o destruido sin que el emisor o el destinatario lo confirmen. El mensaje será leído, salvo que haya sido codificado.

Ello no ocurre con lo aludido a las vías electrónicas que cuentan con claves de seguridad, salvo que un técnico especializado (*hacker*) las intercepte o las vulnere. El *mensaje* así está más protegido y despliega mayor confidencialidad.

Estamos ante un atributo particular de cualquier documento o archivo informático. Como es sabido, gracias a ciertas funciones de cifrado, es posible colocar contraseñas a documentos y archivos, incluso de ingreso a sistemas y demás, todo ello utilizando el sistema simétrico, ya explicado anteriormente.

Sin embargo, dicho sistema no ha sido funcional para la *firma digital,* siendo más aplicable el sistema asimétrico, que permite la creación de dos claves, una privada y otra pública.

Un emisor requiere enviar determinado mensaje de datos a un destinatario, utilizando su firma digital. Para el efecto, una vez elaborado el documento firmará digitalmente el mismo e introducirá la clave pública del destinatario. Al cifrar con la clave pública del destinatario, lo que hace es cerrar el candado que únicamente la llave (clave privada) que posee el destinatario podrá abrir. Al recibir el mensaje el receptor solamente debe introducir su clave privada, verificando así la *autoría* del mensaje y su *integridad.*

Cabe destacar que el nivel de confidencialidad estará dado también por la capacidad técnica de las partes intervinientes a fin de incrementar el sistema con la introducción de contraseñas en los documentos y otras modalidades.

5. Conclusiones y propuesta para su utilización

Las respuestas brindadas por estas herramientas tecnológicas a las grandes dificultades que fueron generándose debido a la inseguridad reinante en las redes siguen siendo notoriamente relevantes para todo el sistema de comunicaciones, como también para el portentoso ámbito que emerge a pasos galopantes denominado *comercio electrónico.*

Las razones para los particulares de incorporar este servicio, a más de los criterios de seguridad e integridad esgrimidos anteriormente, son concomitantes con los medios tecnológicos actuales de comunicación e interrelación, que como hemos citado en cuanto al correo electrónico, por mencionar uno de los productos comunes de Internet, repercuten en un todo ante la economía, ahorro de recursos, prontitud en la relación, participaciones y respuestas, eficiencia en los procesos,

control y administración generados dentro y fuera de la empresa, entre otras meritorias cuestiones que arrojan al sector a escalar presurosos hacia estas inventivas.

Esas acciones fueron reflexionadas por el sector público llegándose a comprender luego de muchos años que claramente el ente estatal al darle las espaldas a estas modernas herramientas atentaría contra sí mismo, por lo que pronto fue implantada la necesidad de alistarse a las mejores maneras de fusionar dichos medios.

En definitiva, y conforme al resumen del *derecho comparado*, los sistemas positivos de los diferentes países fueron introduciendo poco a poco el reconocimiento de la validez jurídica de los actos efectuados a través de los modernos medios tecnológicos y hasta inclusive, en algunos casos, el incentivo para fomentar mayores desarrollos, investigaciones y fortalecimiento de todo ese campo.

Particularmente sobre este tema, de acuerdo a las experiencias existentes, la promoción está centrada principalmente en garantizar a todas las partes interesadas la interrelación sin temor de fraudes, de vulneración de la información, de seriedad en las negociaciones ante la revelación clara y contundente del otro usuario –consumidor o empresa- que se encuentra en frente, entre otras variantes.

Las transacciones comerciales concretadas y garantizadas a través de estos medios fortalecerán el comercio electrónico, actividad que hoy día representa un cúmulo importante para la economía de cualquier país.

Existe en general siempre un temor a lo nuevo, solo por el hecho de cambiar lo tradicional por algo desconocido. Así, cuando surge la propuesta de modificar alguna legislación emerge en forma paralela la desconfianza y recelo por la innovación. Pues estas no son ajenas a esas generalidades. Superar las desconfianzas que subyugan ciertas ideas con respecto a las funciones operativas que estos sistemas generan será una tarea que tanto el sector privado como el público deberán descollar de manera trascendental para nuestro país a fin de colocarlo al nivel regional y mundial requerido.

En particular, hemos aguardado con ansias que se haga efectiva la Ley Nº 4.017, que dos años después recién fue complementada y puesta a punto para arrancar con la utilización del servicio, pero tampoco fue finalmente así. Recién con la reglamentación decretada por el Ejecutivo y transcurrido luego de allí otro tanto de tiempo, fueron habilitados, entre otros andamientos, la

Autoridad de Aplicación, la Dirección General de Firma Digital y Comercio Electrónico, y finalmente, las prestadoras de servicios de certificación. Mucha agua todavía queda por pasar.

Palabras claves

Tecnologías. Comercio electrónico. Firma digital.

Key Words

Technologies. Electronic Commerce (E- commerce). Digital Signature.