Firma Electrónica y Firma Digital:
"Parecido no es lo mismo"
Por el Dr. Raúl Alejandro Farías
Comisión de Informática

La nueva ley 25.506 y sus decretos reglamentarios 2628/2002 y 1628/2003 crean el marco jurídico adecuado para la implementación de la infraestructura de firma digital en nuestro país y su uso por los particulares.

Cabe recordar que la referida ley reconoce el empleo de la firma electrónica y la firma digital otorgándoles eficacia jurídica –con las limitaciones que ella misma prevé- con lo cual la equipara a la tradicional firma autógrafa, de tal suerte que es posible firmar digitalmente documentos digitales. Este juego de palabras se traduce en la simple posibilidad que tiene una persona de elaborar, por ejemplo, un contrato en su computadora personal, firmarlo digitalmente con su certificado digital y enviarlo vía e-mail a la otra parte de la relación jurídica que se instrumenta. El destinatario devolverá el documento por la misma vía firmado con su propio certificado digital, con lo cual quedará celebrado el contrato de la misma forma que ocurriría si ambos se reunieran físicamente y firmaran de sus respectivos "puño y letra". Esto es solo un simple y muy básico ejemplo. Deje el colega volar su imaginación y pronto se verá enviando escritos vía mail o web desde la comodidad de su PC, teléfono celular, agenda electrónica, dondequiera que se encuentre, a expedientes electrónicos… No, no es mera imaginación; es el futuro que se avecina y que en algunos países ya existe

Uno de los aspectos que la ley 25.506 trata y que con más frecuencia puede dar lugar a erróneas interpretaciones, es el de la firma digital y la firma electrónica, las cuales describe en sus artículos 2 y 5 respectivamente:

Art. 2º — Firma Digital*. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.*

Art. 5º — Firma electrónica*. Se entiende por firma electrónica al 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. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.*

Las diferencias en principio parecen sutiles, pero en realidad son profundas y determinan la entrada o no al juego de las presunciones que se establecen a favor de una de ellas, lo cual será de importancia capital a la hora de probar su existencia.

Antes de comenzar con el análisis de cada una, corresponde aclarar que el medio en que se crean ambos tipos de firmas, les permiten compartir la calidad de “electrónicas”, toda vez el medio digital de una computadora es esencialmente electrónico.

Firma Electrónica

Para desentrañar las diferencias entre la firma electrónica y la digital, lo mejor será recurrir en primer término al texto de la ley: En el caso de la firma electrónica, esta consiste en una serie de datos relacionados en forma lógica y vinculados con la identidad de una persona. El ejemplo más conocido lo constituyen, en general, los “password” usados para identificarse como usuario de determinada cuenta de correo electrónico, formados por un nombre de usuario y una contraseña asociados entre si y ambos a otra cantidad de información acerca de la identidad de la persona.

Otro ejemplo de firma electrónica, menos conocido que el anterior, pero que de a poco se va abriendo paso entre los usuarios de Internet, lo constituyen los procedimientos necesarios para obtener una clave de acceso a la Banca Electrónica. En la mayoría de los casos, la persona interesada debe generar una clave de 8 dígitos numéricos en una terminal de cajero automático con su tarjeta de débito. Ello supone que previamente ingresó su tarjeta y marcó la clave de acceso que ya posee para extraer dinero o pagar servicios. Luego el cajero automático le devuelve un ticket en el que figuran un nombre de usuario y una contraseña que deberá ingresar en el formulario respectivo en Internet. Esos son precisamente los datos que configuran una firma electrónica, ello, claro está, sin perjuicio de la posibilidad que ofrecen esos sitios web de cambiar más adelante la clave de acceso y contraseña por razones de seguridad.

Se puede entonces advertir que tanto el nombre de usuario como la contraseña son datos que están relacionados de forma lógica entre si y con otros datos del cliente del banco tales como su propio nombre, su documento, número de cuenta, tarjetas de crédito y demás datos secundarios formados por toda la información que un banco puede poseer de cada cliente (cónyuge, hijos, ocupación, ingresos, situación impositiva, previsional etc. por citar algunos ejemplos).

En definitiva, la firma electrónica formada por la palabra elegida como nombre de usuario y la contraseña se corresponden mutuamente y determinan una identidad, un individuo.

Eventualmente esos datos le permitirán ingresar al sitio web del banco en Internet donde existen una cantidad -cada vez mayor- de servicios que cliente puede usar (pago de tarjetas, pago de servicios, transferencias de dinero, consultas de saldos, etc). La gran mayoría de estos servicios, debido a la mecánica propia de los sitios web, ya contienen una manifestación expresa de la voluntad en estado de "vida suspendida" -si se me permite la imagen- para ser activada mediante un botón llamado "Aceptar" incluido en las respectivas páginas, con el cual se confirma la operación realizada.

Sucede entonces, que algo atípico ocurre con el orden de los acontecimientos: la persona, al usar su nombre de usuario y contraseña para ingresar a su zona de banca en Internet, suscribió a priori con Firma Electrónica las eventuales manifestaciones de la voluntad que prestará a lo largo de esa sesión de "e-banking". Probablemente solo revise sus saldos y no preste ningún

consentimiento más que el de confirmar su nombre de usuario y contraseña al principio, pero es justamente en ese momento en el que usó su firma electrónica. Y subrayo: firma electrónica, no digital.
En una relación contractual básica, la firma electrónica consistiría en aquellos datos del firmante relacionados con otros datos, por ejemplo los de su cuenta de correo electrónico, que permitieran establecer su identidad

Firma digital y Certificado Digital
La firma digital es algo más complejo: básicamente consiste en aplicar a un archivo digital (ya sea de texto, video, imagen audio, etc.) un algoritmo matemático que da como resultado otro archivo llamado "hash". Este hash o resúmen de ahora en más, es en esencia la huella digital del archivo en cuestión -en nuestro ejemplo imaginemos que se trata de un contrato- y como toda huella digital, es única y no puede haber dos iguales. El firmante encripta este resúmen con su clave privada con lo cual da por concluido el proceso de firma digital del documento.
El documento principal y su resumen encriptado de la forma descripta son enviados o entregados al destinatario via e-mail o en soporte magnético u óptico. El destinatario, al recibirlos aplica al documento principal el mismo algoritmo que el remitente y genera su propio resumen. Por otro lado, usa la clave publica del firmante, que viajó junto al mensaje firmado en su certificado digital y con ella lo desencripta. Es así que obtiene dos resúmenes del mismo documento: el propio y el recibido. Al comparar ambos puede comprobar si el documento recibido ha sido alterado luego de ser firmado digitalmente ya que de no haber sufrido modificación alguna luego de la firma, el resumen propio debe ser idéntico al recibido. En sentido contrario, de existir modificaciones posteriores a la firma, el resumen propio será distinto del recibido indicando que la firma es inválida.
Pero no se asuste… todos los procesos que intervienen en la firma y su comprobación se realizan automáticamente, limitándose la intervención del usuario a unos pocos "clics" de mouse sobre iconos bien definidos.
El certificado digital es el elemento indispensable para realizar una firma digital. Básicamente vincula una persona física o jurídica con los datos que acreditan su identidad. Deben ser expedidos por un Certificador Licenciado por la Autoridad de Aplicación, quien actúa como tercera parte confiable dando fe de la veracidad de los datos consignado en dicho certificado. Además de contemplar la información necesaria para la verificación de la firma y permitir comprobar la identidad del firmante en forma indubitable, transportan su clave pública permitiendo la comprobación de la integridad del mensaje. Requisitos especiales de validez tales como: indicar su período de vigencia, ser susceptible de verificación respecto de su estado de revocación, diferenciar claramente la información verificada de la no
verificada incluidas en el certificado, identificar la política de certificación bajo la cual fue emitido, etc, se encuentran establecidos en el art. 14 de la ley.

La gran diferencia
El despliegue tecnológico necesario para producir una firma digital así como la propia regulación normativa aplicada a esos procesos y a la validez de los certificados digitales constituyen, en definitiva, los medios idóneos para que la firma digital pueda gozar de las presunciones de autoría e integridad del

documento y evitar el repudio por parte del firmante, esto es que en el futuro niegue haber firmado, principios estos establecidos a su favor en los artículos 7 y 8 de la ley y de los cuales carece la firma electrónica.
Es así que la firma electrónica, al poder prescindir de un certificado digital y de mecanismos de encriptación, tiene muchos menos requisitos para su existencia que la firma digital. Sin embargo, debe pagar su costo al no poder gozar de las presunciones de aquella, debiendo ser acreditada su validez por quien la invoque, para el caso que fuera desconocida.

Hoy por hoy
Actualmente en nuestro país la realidad es que, si bien existe el marco regulatorio para la firma digital desde noviembre de 2001 a través de la ley 25.506 y sus decretos reglamentarios, lo cierto es que, a la fecha de este artículo, la autoridad de aplicación ONTI (Oficina Nacional de Tecnologías de la Información) no ha otorgado aun licencias de habilitación a los certificadores, que precisamente son quienes emiten los certificados digitales.
De modo que, si bien existen muchas empresas extranjeras y nacionales que emiten certificados digitales conforme a los estándares tecnológicos aceptados internacionalmente y por nuestra ley, al no estar licenciados, las firmas que se creen en base a sus certificados no pueden gozar del carácter de firma digital y gozar de las presunciones de autoría e integridad que prevé la ley para las creadas en base a certificados emitidos por los certificadores una vez licenciados.

Es así que los documentos firmados digitalmente en esas condiciones, tienen en la actualidad la validez de una firma electrónica y no la de una firma digital.

Hasta tanto podamos contar con certificados digitales emitidos por certificadores licenciados en el futuro cercano, podremos usar igualmente los que existan, teniendo en cuenta que solo podremos generar firmas electrónicas.
Si aun se deseara suplir la caída de las presunciones legales a favor de la firma digital, siempre es posible celebrar convenios privados, de conformidad a lo normado en el art. 1197 del Cod. Civil, que invistan a estas firmas hoy por hoy Electrónicas de aquellas virtudes propias de la Firma Digital.

Firmado digitalmente por Farías, Raúl Alejandro - Comisión de Informática
Nombre de reconocimiento (DN): CN = Farías, Raúl Alejandro - Comisión de Informática, C = AR, L = TIGRE, S = BUENOS AIRES, O = Colegio de Abogados de San Isidro, OU = Clase 2
Motivo: Documento creado por el Dr. Raúl Alejandro Farías
Ubicación: Colegio de Abogados de San Isidro
Fecha: 2004.05.07 09:40:45 -03'00'