

Firma Digital en Argentina: manteniendo la ilusión.

Por Marcelo Temperini

Desde la sanción de la Ley 25.506 en Diciembre del 2001 venimos hablando de la Firma Digital. En el ámbito público, se utiliza poco y nada, mientras que en el ámbito privado, sigue brillando por su ausencia. ¿Porqué? Explicaremos en esta nota, el contexto de nuestro país y algunos de los motivos de la inexistencia de ACLs que emitan certificados digitales para privados en Argentina. El estado vegetativo de la Firma Digital, nos deja esperando una ilusión que no se pierde, pero que tampoco mejora.

Un repaso por la Firma Digital

No buscaré aquí hacer un análisis exhaustivo de la Ley de Firma Digital N° 25.506, dado que su desarrollo y extensión, hacen que el mismo exceda el objeto de este artículo. No obstante, si haremos un breve repaso de los conceptos y características que más se destacan.

Debemos comenzar sabiendo que en Argentina, a través de esta ley mencionada, se reconoce la eficacia jurídica tanto de la **Firma Digital (FD)**, como de la **Firma Electrónica (FE)**, diferentes en sus características, por lo que no deben ser tomadas como sinónimos.

La Ley define a la FD, como el “resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control.” A renglón siguiente, la ley menciona las dos características básicas que tiene la FD: “ser susceptible de verificación por terceras parte, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.” (Autoría e Integridad).

Para pasar a comprender ambos caracteres, previamente debemos comprender el concepto de Documento Digital, que de acuerdo al art. 6, es toda “representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.” El mismo artículo, termina afirmando que “un documento digital también satisface el requerimiento de escritura”, cuestión más que importante, ya que a través de este artículo, cada vez que algún acto jurídico requiera la forma escrita, ahora también podrá ser realizado a través de un documento digital.

La Autoría significa (de acuerdo al art. 7) que se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permita la identificación de dicha firma.

La Integridad significa (de acuerdo al art. 8) que se presume, salvo prueba en contrario, que este documento digital firmado digitalmente no ha sido modificado desde el momento de su firma.

Ambos caracteres, son la fuerza interna que hacen que la FD sea considerada por esta ley (en el art. 3), como una alternativa válida a la exigencia de firma manuscrita. El hecho que una firma digital válida (ver condiciones de validez en art. 9), sea considerado legalmente como suficiente para reemplazar los casos donde sea necesario la firma manuscrita, es avanzar 10 casilleros hacia el frente en materia de la digitalización de los documentos y procesos.

Basta dejar salir a jugar un rato la imaginación, para comprender que de esta manera, los negocios vía internet tendrán la validez y la certeza que hasta el momento venía frenando a aquellos que aún no se habían sumado a este nuevo canal por los miedos (fundados) a los fraudes y dificultad probatoria de hoy en día.

Para aquellos que viven a diario el mundo digital, es cuestión de minutos para ilusionarse, para entusiasmarse en todas aquellas aplicaciones que podríamos darle, el aumento de la productividad en una gran cantidad de trámites y procesos, con su consecuente disminución de costos, tiempos, hasta incluso espacio físico... Todo es alegría y color hasta volver a darnos cuenta que estamos en Argentina y que si bien la normativa es buena e interesante, todavía queda camino por recorrer para que el sueño se vuelva una realidad.

Privilegio Público

Tal como hemos dicho anteriormente, la FD si está activa y funcionando en el ámbito público, tanto nacional como provincial, donde ya se han realizado algunas implementaciones. Algunas de ellas muy interesantes, otras sólo han quedado en proyectos, y otras dependencias todavía no saben que existe la FD.

La legislación mencionada establece como obligación del Estado Nacional la utilización de esta tecnología en su ámbito interno y en sus relaciones con los administrados, estableciendo un plazo máximo de cinco años para que la misma sea aplicada a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas del Sector Público Nacional (Ley N° 25.506, arts. 47 y 48). Han pasado ya más de 8 años, y este objetivo aún se ve lejos de concretarse.

Certificadores Licenciados

En nuestro país, la PKI (Public Key Infraestructure), está encabezada por su ACR (Autoridad Certificante Raíz) que es (tras algunas idas y vueltas) la Subsecretaría de Gestión Pública de la Nación (SGP), dependiente de la Jefatura de Gabinete de Ministros, que a su vez han delegado las funciones de Ente Licenciantes a la Oficina Nacional de Tecnologías de la Información (ONTI).

El Ente Licenciantes (ONTI) ha designado hace no mucho tiempo, a dos ACL (Autoridad Certificante Licenciada): AFIP y ANSES, ambas autorizadas para la emisión de certificados digitales dentro del ámbito de sus funciones (es decir, ámbito público).

De manera que en la actualidad, en nuestro país, no existe ACL que emita certificados digitales para su utilización en el ámbito privado, dejando a esta potente herramienta tecnológica sólo para unos pocos privilegiados del ámbito público, donde la realidad muestra que la real utilización de la FD es bastante escasa.

La única alternativa existente hoy en día para los ciudadanos, es la emisión de certificados digitales que realizada la propia ONTI, pero a no ilusionarse, porque sólo son certificados digitales de correo electrónico, que lo único que hace es verificar la existencia de la dirección de correo electrónico del emisor, pero sin comprobar de ninguna manera su identidad. Como bien lo dice en los propios procedimientos oficiales, es sólo para experimentar como sería tener una firma digital, pero que carece de sus características.

¿Porqué estamos como estamos?

La situación es clara: no tenemos ACL para los privados. La pregunta que surge es ¿porqué?. En la Ley 25.506 y su normativa complementaria, al analizar los requisitos para constituirse como ACL en nuestro país, se pueden deducir algunos de los temas de más relevancia que hacen que hasta el momento, y en todo el tiempo transcurrido, no exista ninguno constituido.

En principio, se debe contar con una infraestructura técnica que permita hacer frente a los requisitos para su constitución formal. En la DA 6/2007, se aprobaron los requisitos para el licenciamiento de certificadores, en su Anexo I. En dicho Anexo, en el punto 2, señala los documentos a presentar para ser evaluados: Política de Certificación (PC), Manual de Procedimientos de Certificación (MPC), Acuerdo tipo con suscriptores, Términos y condiciones tipo con terceros usuarios (“relying parties”), Resumen de la PC/MPC para suscriptores (“PKI Disclosure Statement” en caso de existir), Política de Privacidad del Certificador, Direcciones, protocolos y medios para acceder a la información que se publica (para los CRLs). Además, como documentación complementaria se exigen los contratos de tercerización, el Plan de Cese de actividades, Plan de Seguridad (política y procedimientos de seguridad), Plan de Contingencia y la descripción de la plataforma tecnológica del solicitante.

Como se verá, contar con la infraestructura para postularse como ACL no es cuestión sencilla, ni de un día para otro. Además, la auditoría que comprobará la satisfacción de estos requisitos, será realizada anualmente para controlar el mantenimiento y adecuación de los mismos (art. 32 de la DA 6/2007).

Otro de los grandes obstáculos al momento de pensar ser un certificador licenciado, es el tema de la responsabilidad, regulado en el Cap. IX de normativa. En la misma, si bien en principio la relación entre el certificador licenciado y el titular del certificado es regida por el contrato entre las partes, existe una obligación legal que el certificador no puede desligar, y es la del art. 38, sobre Responsabilidad de los certificadores licenciados ante terceros, afirmando que “El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos

a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.”

La Ley también tiene previsto un sistema de sanciones para los casos de incumplimientos por parte de la ACL en alguna de sus obligaciones. En el art. 41 se regula la posibilidad de aplicación de apercibimiento, multa (de \$10.000 a \$500.000), y caducidad de la licencia, todo de acuerdo a la gravedad del incumplimiento de la ACL. Además, el artículo termina afirmando que dichas sanciones no eximirá a la ACL a responder frente a eventuales reclamos por daños y perjuicios causados a terceros o sus bienes, como consecuencia del contrato y/o los incumplimientos de sus obligaciones.

Otro elemento más de garantía exigido es la constitución de un seguro acorde a las responsabilidades asumidas, a fin de garantizar el cumplimiento de las obligaciones (art. 30 del Decreto 2628/2002 y art. 38 de la DA 6/2007). Este requisito, no es necesario en caso de las ACL del ámbito público.

Conclusión

Como vemos en el contexto actual de la FD en Argentina (del cuál sólo hemos visto algunos aspectos), se ha regulado de manera estricta los requisitos para constituirse como ACL, cuestión que tiene su lógica al comprender los riesgos de la prestación de un servicio irresponsable por parte de alguna empresa. Creo que estos requisitos, tendrían consecuencias positivas en nosotros ciudadanos que contratemos con ellos, pero me queda la duda si el contexto económico social de nuestro país, brinda las herramientas como para que empresas u organismos interesados puedan cumplir con tales demandas.

Con ello no quiero decir que se deban bajar las exigencias, sino que reflexiono acerca de la posibilidad real de que las condiciones fácticas se puedan dar, para que finalmente existan empresas que tengan interés en emitir certificados digitales válidos en nuestro país.

Sé que todos los requisitos son perfectamente cumplibles, y en otros países, muchas empresas en su normal funcionamiento (y sin llegar a prestar un servicio de esta importancia) ya cuentan con la mayoría de lo requerido aquí. Lamentablemente este no es el caso de las empresas argentinas, para las que pensar en tener la infraestructura necesaria, parece inalcanzable.

En fin, por un lado el Estado utiliza la FD poco y nada en el ámbito público, y dista de querer hacer algo más que eso (como constituir una ACL con destino a privados). Por otro, la situación para las empresas u organizaciones que quieran ser ACL, tampoco tienen un panorama alentador para meterse en el negocio de los certificados digitales, esencialmente por la magnitud de los requisitos (fundados) y las obligaciones que se contraerían.

Por un motivo u otro, o por otros tantos que escapan a mi consideración en este texto, la conclusión es que mientras tanto, debo volver a acomodarme en mi sillón y seguir viendo por internet las novedades de otros países que siguen inventando día a día nuevas maneras de utilizar una herramienta tan potente como la Firma Digital. La ilusión es lo último que se pierde, así que a seguir esperando...

Marcelo Temperini, Director de la Red Iberoamericana de Derecho Informático (elderechoinformatico.com), Socio Director de AsegurarTe (Consultora en Seguridad de la Información).