governeo

FIRMA DIGITAL
ANÁLISIS DEL MARCO NACIONAL Y LAS REGULACIONES LOCALES

Julián Lopardo
Natalia Rodríguez
Felipe González Barlatay

GOVERNEO
Calle 12 N°823 1° B,
La Plata, Buenos Aires
+54 0221 4824582
info@governeo.org

RESUMEN EJECUTIVO:

En las últimas décadas las TIC han ganado protagonismo a nivel mundial, generando una comunicación fluida entre interlocutores sin ningún tipo de relación previa a través de herramientas que incrementan la velocidad de circulación de la información y simplifican operaciones complejas. Este proceso originó la necesidad de contar con un mecanismo que permita garantizar tanto la integridad de un documento como la identidad de su autor, diseñándose el sistema de Firma Digital

La Ley N° 25.506 de Firma Digital, en su art. 2, la define 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. 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", y el sistema que regula es el de Criptografía asimétrica o Criptografía de Clave pública.

En dicho marco, la infraestructura de firma digital, es la que brinda validez legal y seguridad jurídica a la aplicación mediante el diseño del sistema de operaciones, la emisión de los certificados digitales, el establecimiento y actualización de estándares tecnológicos internacionales, la supervisión de la emisión de los certificados y hasta la aplicación de sanciones.

En lo que hace a las competencias regulatorias de los diferentes niveles de gobierno, puede remarcarse que la Ley de Firma Digital contiene tanto disposiciones que hacen a la regulación de fondo, potestad del legislador nacional, como cuestiones procedimentales y de derecho público, facultad que tienen tanto el gobierno nacional –en su ámbito de competencia federal– como los gobiernos provinciales a nivel local, en ejercicio de su autonomía reconocida constitucionalmente.

De allí que la coexistencia de los regímenes propios de los diferentes niveles de gobierno, es perfectamente compatible, en tanto y en cuanto se deslinden adecuadamente sus competencias y ámbitos de aplicación, pudiendo armonizarse diversidades que, en definitiva, son la esencia misma de un sistema federal.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

1. INTRODUCCIÓN

En las últimas décadas las TIC han ganado protagonismo a nivel mundial, generando una comunicación fluida entre interlocutores sin ningún tipo de relación previa a través de herramientas que incrementan la velocidad de circulación de la información, simplifican operaciones complejas, y ofrecen un mejor nivel de servicios reduciendo simultáneamente los costos, aumentando productividad y competitividad en un mundo globalizado cada vez más demandante.

El incremento en el flujo de estas transacciones generó la necesidad de contar con un mecanismo que permita garantizar tanto la integridad de un documento como la identidad de su autor, dotando a las operaciones de seguridad y confianza. Para dar solución a dicha problemática se diseñó el sistema de Firma Digital, que utiliza un mecanismo de claves asimétricas tendientes a otorgar a las transacciones electrónicas la responsabilidad personal que todo acto jurídico necesita.

Este rediseño de las relaciones humanas, que conlleva un verdadero cambio de paradigma, se encuentra en una evolución constante hacia su efectiva masificación. Por esta razón, el Estado en su rol de gestor del interés público, prestador de servicios esenciales y garante de los derechos de los ciudadanos, debe ubicarse en el centro del sistema garantizando la transparencia de su funcionamiento e invirtiendo en la adaptación de sus procedimientos en pos de la implementación de los avances tecnológicos que lo doten de una creciente eficiencia y eficacia en sus prestaciones, con el consecuente impacto positivo en la economía de los recursos públicos y la protección del medio ambiente.

Dichas acciones se replican tanto a nivel nacional como subnacional, resultando de allí la problemática vinculada con su regulación, atento al carácter federal del diseño constitucional argentino, el cual reconoce la preexistente autonomía de los gobiernos locales en lo que hace a la regulación de sus instituciones de gobierno y de los procedimientos mediante los cuales se vinculan las administraciones con los ciudadanos.

En ese sentido, resulta pertinente revisar la adecuación del actual marco regulatorio de una herramienta trascendente en materia de gobierno electrónico, como es la Firma Digital, de forma tal que resulte una clara delimitación y coordinación de competencias entre los diversos niveles de gobierno que permita la generalización de su utilización, con los beneficios que ello traerá en materia de servicios al ciudadano, participación, colaboración, transparencia y reutilización de información fidedigna.

Por ello, repasaremos brevemente la infraestructura vinculada a la herramienta, su regulación a nivel comparado, Nacional y Local, así como las dificultades que ha traído su implementación, principalmente en lo que hace a la articulación de competencias regulatorias, para finalmente obtener algunas conclusiones en torno al correcto ejercicio de las competencias legislativas, el ámbito de aplicación de las normativas emanadas de los diferentes niveles de gobierno, y la armónica interpreta-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

ción que debe hacerse para la viabilidad del sistema en su conjunto.

Firma digital. Concepto técnico.

La Ley N° 25.506 de Firma Digital, en su art. 2, la define 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. 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".

La definición que da ese artículo de la ley no es autosuficiente, y sólo puede comprenderse en todo su alcance mediante una interpretación sistemática de todo su articulado. Asimismo, en virtud de la compleja operatoria técnica que implica, resulta necesario aclarar previamente algunas cuestiones terminológicas.

Para desarrollar con mayor claridad el concepto, nos apartaremos por un momento de la letra de la ley, definiendo a la Firma Digital como un conjunto de características técnicas y normativas. Ello es así, ya que la herramienta se define en virtud de procedimientos técnicos que permiten su operatoria en el marco de instrumentos normativos que la validan, respaldando legalmente su aptitud para producir efectos jurídicos. Este procedimiento técnico permite asociar la identidad de una persona a un documento, comprobando como correlato de ésta coincidencia su integridad. De esta manera, y a través de un conjunto de presunciones legales, se produce el principal efecto jurídico de la Firma digital que es la instrumentación de la manifestación de voluntad respecto al contenido del documento digital.

Como derivación de lo expuesto, entendemos necesario metodológicamente desagregar la definición brindada en dos partes:

1.- Procedimientos técnicos

a) Sistema de Criptografía asimétrica

El sistema que regula para la Firma Digital la Ley N° 25.506, conforme las referencias de los artículos 2, 7 y 9, es el de Criptografía asimétrica o Criptografía de Clave pública.

Etimológicamente, el término Criptografía proviene del griego Cripto (oculto), y es definido como el "Arte de escribir con clave secreta o de un modo enigmático."[1]

Existen dos tipos de cifrado:

- SIMÉTRICO: utiliza la misma clave para el cifrado y el descifrado de la información. Es un sistema básico que no cumple con los requisitos de seguridad exigidos para esta operatoria debido a que la clave "viaja" con el documento, con lo cual la operación resulta sumamente riesgosa - más aún si interactúan varios interlocutores -, ya que cualquiera que conozca la clave podría descifrar el contenido o identificarse como su autor legítimo, sin serlo.

- ASIMÉTRICO: en este caso existen dos claves, una con la que se cifra el mensaje y otra que lo descifra. Ambas claves son asignadas a una misma persona, siendo una de ellas de conocimiento exclusivo del emisor (clave pri-

1 http://www.rae.es/

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

vada, utilizada para firmar) y otra accesible para terceros (clave pública, utilizada para constatar la firma digital). Ambas claves están vinculadas matemáticamente a través de una fórmula imposible de reproducir, y guardan entre sí una relación tal, que algo que sea encriptado por la clave privada de determinado emisor únicamente podrá ser desencriptado por su clave pública.

Para ello, todo el sistema deberá basarse en una infraestructura de manejo de claves que permita identificar de manera certera a cada usuario, con su clave pública, a través de terceras partes confiables.

El mecanismo descripto garantiza la integridad y autoría del documento firmado digitalmente, mas no su confidencialidad. Para que esto último sea posible, debería encriptarse el documento con la clave pública del receptor, para que cuando éste lo reciba, pueda leerlo únicamente si aplica su clave privada.

b) Resumen hash

Al contenido del documento que se pretende firmar digitalmente con el sistema de criptografía asimétrica, el emisor le aplicará cierto algoritmo matemático, denominado función hash, y al resultado obtenido le aplicará su clave privada.-

El hash es una función matemática o algoritmo criptográfico que transforma un documento digital en una secuencia de bits; es decir que transforma el documento digital en un extracto numérico llamado resumen hash o digesto. A partir de un mismo documento, siempre se generará idéntico resumen hash, y correlativamente es imposible que existan dos resúmenes iguales de documentos distintos.

El destinatario, al recibirlo, utiliza la clave pública del emisor para descifrar el mensaje, consignando luego la misma función hash sobre el documento digital, obteniendo otro resumen hash que comparará con el adjuntado por el emisor al mensaje. Si los resúmenes coinciden, es porque el contenido del documento enviado no ha sido modificado.

Lógicamente, estas operaciones de cálculo y verificación posterior no son realizadas por el usuario, sino que las realiza automáticamente un software específico para la aplicación.

2.- Instrumentos normativos

Como correlato de la operatoria técnica descripta, debe existir una estructura legal que brinde las presunciones que validen la factibilidad de producir efectos jurídicos por medio de actos instrumentados en formato digital. De conformidad con el ordenamiento vigente, para que ciertamente podamos hablar de Firma Digital, será necesario contar con los siguientes elementos:

a) Certificado Digital

El receptor de un documento recibirá la clave pública del emisor, a través del Certificado Digital adjunto al mensaje, siendo esto lo que le otorga la validez legal a la Firma.

El Certificado Digital es un documento digital otorgado por la Autoridad Certificante que contiene los datos de identidad del firmante junto a su clave pública, el cual sirve para garantizar la veracidad de los datos contenidos, referentes a una persona física o jurídica.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Básicamente es una identidad virtual, equivalente a un documento de identidad, que garantiza que quien firmó digitalmente un documento es quién dice ser.

Para que dicho certificado tenga la capacidad de atribuir efectos jurídicos a los documentos que acompañe, es necesario que sea expedido por una autoridad certificante habilitada por un ente certificante, y que el formato sea el utilizado internacionalmente (estándar internacional[2]).

Como hemos explicado ut supra el Certificado se basa en el método de criptografía asimétrica, en el cual las claves conforman un par único y se generan en el mismo momento por el usuario, ejecutando un programa provisto por la Autoridad de Certificación desde su sitio web. Para aprobar un Certificado Digital, la Autoridad de Certificación firma con su Clave Privada la Clave Pública del Certificado Digital, constituyéndose así en la tercera entidad de confianza que asegura que la clave se corresponda con los datos del titular.

El titular del certificado debe mantener bajo su exclusivo poder la clave privada, ya que si ésta es sustraída, el sustractor podría suplantar su identidad en la red.[3]

El certificado digital contendrá los siguientes datos:

a) Identificación de su titular (Nombre y DNI) y del certificador licenciado que lo emitió;

b) período de vigencia;

c) Clave pública del titular, identificando el algoritmo utilizado;

d) Número de serie del Certificado;

e) Dirección de Internet de la lista de Certificados revocados que mantiene el certificador que lo emitió[4];

f) identificación de la política de certificación bajo la cual fue emitido;[5]

g) Firma Digital del certificador de la clave pública que emite el certificado.

---

2 El artículo 20 de la Decisión Administrativa 6/07 (JGM) (BO N.º: 14/2007) prescribe que *"Establécese como estándar tecnológico de la Infraestructura de Firma Digital de la República Argentina, en lo referente al formato de los certificados digitales y listas de certificados revocados, al estándar ITU-T X.509 (ISO/IEC 9594-8) (...)"* De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el mencionado estándar.

3 En este caso, el titular deberá revocar el certificado lo antes posible. El proceso de revocación dependerá de la AC que haya emitido el certificado.

En el caso de *ENCODE*, el usuario que quiera revocar su Certificado deberá ingresar a la aplicación de la Autoridad Certificante ENCODESINEL desde el portal del Suscriptor con su CUIT/CUIL y su PIN de revocación otorgado en el momento de la emisión; desde allí enviará la solicitud de revocación, y la AR recibirá la solicitud, registrará y archivará los datos como respaldo de la acción realizada. En el caso de pérdida del PIN de revocación se deberá solicitar en el portal del Suscriptor el reenvío del mismo. Éste se enviará a la dirección informada por el Suscriptor, en forma automática. (ver http://www.encodeac.com.ar/)

Cuando la AC sea la *ONTI*, el suscriptor deberá ingresar a la aplicación disponible en https://pki.jgm.gov.ar/app/ y selecciona la opción "Revocar". A continuación elige una de las siguientes opciones: 1. Se autentica por medio de su clave privada y procede a la revocación de su certificado de firma digital. 2. Realiza la revocación por medio del Pin de revocación que le fue suministrado al momento de la descarga de su certificado (recibido vía e-mail al emitirse la Firma Digital), y su número de documento de identidad.

Cuando la AC es *AFIP*, el titular del Certificado Digital podrá solicitar la revocación mediante los siguientes procedimientos: Ingresando al portal del suscriptor y usando su Clave Fiscal; por medio de la Mesa de ayuda de la AFIP con su código de revocación telefónico, por la presentación personal en cualquier puesto de atención de la AR de la AFIP; por medio de un tercero autorizado mediante el servicio de delegación con clave Fiscal.

La AC *ANSES* dispone que la revocación se realizará ingresando a su portal web (http://www.anses.gob.ar/firmadigitalexternos). Allí se identifica con su Clave de la Seguridad Social, que se conforma con el CUIL junto a su clave personal, y procederá a enviar la solicitud. El suscriptor debe imprimir el recibo de solicitud de revocación y remitirlo a la AR para su proceso de registro y archivo como respaldo de la acción realizada.

Estos sitios están disponibles las 24 horas los 364 días del año, permitiendo la revocación en horarios no habituales de jornada laboral, fines de semana y feriados.-

4 El listado de Certificados Revocados, sirve para que el destinatario pueda corroborar la vigencia del mismo.

5 MOLINA QUIROGA, Eduardo *"Documento y firma electrónicos o digitales"* Buenos Aires, La Ley. Año 2008.-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Los Certificados pueden ser de distintos tipos, dependiendo de los requerimientos del usuario. Los denominados "de identificación" simplemente identifican o conectan una clave pública; aquellos llamados "de autorización", validan un determinado hecho o que éste efectivamente ha ocurrido, por ejemplo determinar día y hora en que el documento fue digitalmente firmado.

b) Infraestructura

La infraestructura de firma digital (PKI[6]), es la que brinda validez legal y seguridad jurídica a la aplicación mediante el diseño del sistema de operaciones, la emisión de los certificados digitales, el establecimiento y actualización de estándares tecnológicos internacionales, la supervisión de la emisión de los certificados y hasta la aplicación de sanciones[7].

Al emitir un Certificado Digital, la Autoridad Certificante lo firma digitalmente con su propia clave privada. A su vez, dicha autoridad ha sido previamente autenticada mediante otro Certificado Digital emitido por otro organismo de mayor nivel, y así sucesivamente hasta una Entidad Certificante Raíz. Esto da lugar a un encadenamiento de entidades certificantes que se autentican, denominado comúnmente como "cadena de confianza". Para fomentar la credibilidad, publicidad y transparencia en la firma del Certificador, algunos Estados prevén la publicación en un Boletín Oficial de la clave pública del prestador de Servicios de certificación, o de ciertos datos sobre el Certificado Raíz. Esto es lo que se conoce convencionalmente como Infraestructura de Clave Pública.

Las Autoridades Certificantes podrán actuar con la previa aprobación de una Autoridad Certificante estatal (Ente Licenciante) a través de un sistema de jerarquías.

Recapitulando, la infraestructura descripta está constituida por una Autoridad Certificante raíz operada por el Ente Licenciante, por Autoridades Certificantes (AC) operadas por Certificadores Licenciados y por Autoridades de Registro (AR), que desarrollan funciones delegadas por los Certificadores Licenciados.

Con la PKI, se pretende asegurar: la confidencialidad de la información que acredita la identidad del titular del Certificado Digital, generando el par de claves (pública y privada) con absoluta reserva de su clave privada; la integridad de los datos que contiene el documento firmado, por medio de la generación del resumen hash o digesto, que permite chequear que el contenido no ha sido modificado; y la identidad del firmante.

En cuanto al sistema de reconocimiento de Certificados Extranjeros, se realiza mediante un método de Certificación Cruzada, en los cuales es necesario que Entidades Certificadoras sustancialmente equivalentes reconozcan los servicios prestados por la correlativa extranjera. Ello deberá ser reconocido y organizado por la legislación de cada país.

B1.- AUTORIDAD CERTIFICANTE RAIZ operada

6 "Public Key Infrastructure"

7 La ley 25.506 (B.O. 14/12/2001), en su Capítulo X establece las sanciones para los Certificadores licenciados. Según el art. 40, el Ente Licenciante deberá iniciar un sumario que tramitará conforme a las normas establecidas en la LNPA nº 19.549, y de este modo determinará la sanción de la que será pasible el Certificador Licenciado (conf. Art. 41 Ley 25.506).-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

por el Ente Licenciante.
El Ente Licenciante es un organismo administrativo encargado de otorgar las licencias a los Certificadores y supervisar su actividad. Su función consiste así en autorizar a los Certificadores a emitir los Certificados Digitales y a prestar otros servicios relacionados con la Firma Digital.

B2.- AUTORIDAD CERTIFICANTE operada por el Certificador Licenciado.
La Autoridad Certificante interviene en la comunicación de documentos digitales como "tercera parte confiable"; es decir que actúa como un Escribano Público virtual, emitiendo y revocando los Certificados Digitales, y verificando su correspondencia con la identidad de su titular. Tiene la misión dar fe de la utilización de la clave privada del remitente antes el destinatario y responde de manera directa por su praxis[8].
Para ello deberá disponer de políticas de seguridad que infundan confianza, utilizar tecnología acorde a su gestión, y proporcionar altos niveles de calidad en atención y disponibilidad.
Puede tratarse de empresas privadas u organismos públicos, siempre que sean autorizados por el Ente Licenciante o Autoridad Certificante Raíz para emitir Certificados Digitales y prestar los servicios relacionados a ello.

8 SALEME MURAD, Marcelo A. "*Firma Digital. Ley 25506 y Normativa Vigente*", Ed. Ad-Hoc, Bs.As. 2004, pág. 23.
El Certificador Licenciado responde solidariamente, aunque no en forma exclusiva, frente a terceros, frente al suscriptor y frente a la Autoridad de Aplicación. Será responsable aún cuando delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho que tiene de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquel sufriera como consecuencia de los actos u omisiones de éstas.

Como ya fuera dicho, las Autoridades Certificantes disponen a su vez de sus propios Certificados Digitales emitidos por la Autoridad Certificante Raíz, mediante los cuales canalizan su propia actividad.

B3.- AUTORIDAD DE REGISTRO
La Autoridad de Registro participa del proceso de verificación de datos de los particulares que solicitan la emisión de Certificados Digitales a la Autoridad Certificante. Se encarga de comprobar la veracidad de los datos que aportan los solicitantes de Certificados Digitales, actuando así como una "ventanilla de atención", para luego remitir la solicitud a la Autoridad Certificante de la cual dependen para que ésta emita el correspondiente certificado
Puede actuar dentro de la Autoridad Certificante, o fuera de ella ejerciendo funciones delegadas.

3.- Funciones de la Firma Digital

La principal valía de la Firma Digital es otorgar seguridad jurídica a las transacciones realizadas a través de los documentos digitales, mediante una identificación indubitable de la identidad del firmante y la garantía de integridad del documento.-
Así, cumple con tres funciones básicas, a saber:
a) Garantizar la identidad del firmante del documento, es decir, la autenticidad de quien dice ser el autor del documento.-
b) Asegurar la integridad del documento, de manera de asegurar que el contenido del do-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

cumento no ha sido modificado con posterioridad a la firma.-
c) Evitar que el firmante rechace el contenido del documento o la veracidad de la firma (no repudio).

4.- Beneficios de la FD

- Brinda seguridad en el intercambio de información en formato digital, otorgando garantía de autoría e integridad a los documentos, equiparando la FD con la rúbrica manuscrita. De esta forma posibilita el progresivo reemplazo de la documentación en papel, contribuyendo al proceso de "despapelización" de los procedimientos en pos de una mayor eficiencia en los servicios, economía de insumos y protección del medio ambiente.
- En el ámbito estatal, dota de transparencia y accesibilidad a los documentos públicos para su control por parte de la ciudadanía, y contribuye a optimizar la gestión posibilitando la realización de trámites por Internet en forma segura. Constituye así un pilar fundamental para el desarrollo del gobierno electrónico.

5.- Principales Aplicaciones

El abanico de posibilidades de operación con Firma Digital es inagotable, pudiendo destacarse a modo de breve enumeración, las siguientes:
Transacciones bancarias
Transacciones comerciales en general
Declaraciones impositivas
Documento de identidad electrónico (e-DNI)[9]
Voto electrónico
Certificación de los actos de gobierno
Historias clínicas
Presentaciones en sede administrativa en general

En nuestro país, el sector de importaciones fue pionero en la implementación de la Firma Digital, remitiendo electrónicamente la Declaración de Mercancías a la AFIP.[10]
Otro ámbito de aplicación es el de la Bolsa de Comercio de Rosario, organismo que emite Certificados de Firma Digital, en su carácter de Autoridad Certificante, por medio de los cuales sus titulares (corredores, vendedores y compradores) registran los contratos de Compraventa de granos.

II.- EXPERIENCIAS EN DERECHO COMPARADO

El primer antecedente de sanción de una ley vinculada con la temática que analizamos, lo encontramos en el Estado de Utah - Estados Unidos de América -, donde en el año 1995 se

9 Por ejemplo en España, donde desde el año 2006 (Real Decreto 1553/2006 modificado por el Real Decreto 1586/2009) existe el Documento Nacional de Identidad electrónico o DNIe. Este nuevo sistema incorpora un pequeño circuito integrado (chip), capaz de guardar de forma segura información y de procesarla internamente. Materialmente es una tarjeta de material plástico, que además de su uso tradicional permite acceder a los nuevos servicios de la Sociedad de la Información, que amplían las posibilidades de actuar a distancia con las Administraciones Públicas, con las empresas y con otros ciudadanos. Para su utilización es necesario contar con determinados elementos hardware y software que nos van a permitir el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.
Según los anuncios realizados por el Ministro del Interior F. Randazzo, a partir del año 2015 se podrá tramitar un e-DNI con similares características en nuestro país (Diario La Nación "El DNI inteligente, otra apuesta de Randazzo"– Edición del 28 de Junio de 2014)

10 Ley 25.986 (16 de Diciembre de 2004) incorpora de modo explícito a la Ley 22.415 (código aduanero) la posibilidad de la utilización de la firma digital.-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

dictó una ley que regulaba la Firma Electrónica.[11]

Posteriormente, en el año 1996, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional emitió una ley modelo, que sirve como guía para los distintos Estados al momento de regular la institución, siendo su principal misión eliminar los soportes materiales de los documentos por los cuales se instrumenten transacciones comerciales.

Por su parte, en Europa el primer país en reglar legalmente la firma electrónica fue Alemania[12]*, donde en el año 1997 se aprobó una ley que contempla el ya analizado concepto de criptografía asimétrica, como el equivalente funcional de los documentos electrónicos.*

Posteriormente, en mayo de 1999 se dictó para la Comunidad Europea la Directiva sobre un Sistema Común para firmas electrónicas[13]*, la que debió ser transpuesta a los distintos estados al 19 de julio del 2003.*

La normativa comunitaria impone a los Estados miembros la obligación de reconocer plenamente los efectos jurídicos y validez de la firma electrónica, siempre y cuando ésta cumpla los requisitos que en ella se explicitan.[14]

A) Firma electrónica en España

En España la aplicación de la Firma Digital fue temprana, siendo uno de los países pioneros en la utilización de la herramienta regulada en aquel momento por el Real Decreto-ley 14/1999. Fue uno de los primeros países de la Unión Europea que legisló la materia, incluso antes que la Directiva Europea sobre Firma Digital fuese oficialmente publicada.

El Marco normativo español está compuesto por:

1.- La Ley N° 34/2002 de servicios de la sociedad de la información y de comercio electrónico.

2.- La Ley N° 59/2003 de firma electrónica, por al cual se regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

3.- La Ley N° 56/2007, de Medidas de Impulso de la Sociedad de la Información.

La citada Ley N° 59/2003, clasifica a la Firma Electrónica distinguiendo tres tipos:

La firma electrónica general, que es definida como "...el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante".

La firma electrónica avanzada, conceptuada como aquella que "...permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control".

La firma electrónica reconocida, descripta

11 Ley Utah título 46, capítulo 3 (1996)- regula la firma electrónica sobre la base del sistema de criptografía, establece una autoridad licenciante de los certificadores, y reconoce efectos jurídicos a las firmas electrónicas homologándola a la firma manuscrita.-

12 Junto con la "Ley de Multimedia" (de la cual la Ley de firma digital constituyó el Artículo 3), la Ley fue debatida en el parlamento durante 1997 y sancionada como Ley el 1ro. de agosto de 1997. El objetivo y propósito de esta Ley fue crear las condiciones generales para las firmas digitales bajo las cuales se las pueda considerar seguras y que las falsificaciones de firmas digitales y las falsificaciones de información firmada puedan ser verificadas sin lugar a duda.

13 Directiva 1999/93/CE del Parlamento Europeo y del Consejo.

14 Art. 5.1 de la Directiva 1999/93/CE.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

como "...la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel".

Vemos entonces que la firma electrónica reconocida es la única que tiene eficacia equivalente a la firma manuscrita.

En su normativa de aplicación, se define como Certificados Reconocidos a los certificados electrónicos expedidos por un Prestador de Servicios de Certificación que cumpla los requisitos establecidos por la Ley N° 59/2003 en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, y a la fiabilidad y las garantías de los servicios de certificación.[15]

El Prestador de Servicios de Certificación es la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. En la legislación española, la prestación de estos servicios no está sujeta a autorización previa, y se realizará en un régimen de libre competencia.[16]

Asimismo se prohíbe el establecimiento de restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo.

Conforme lo dispuesto por el artículo 2.11 de la Directiva 1999/93/CE, los Proveedores de Servicios de Certificación, son "...la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica. También son conocidos como prestadores de servicios de certificación o entidades de certificación."

La Ley 59/2003 (art. 2) por su parte, los define como "...la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica."

Más allá de que los servicios de certificación no requieran licencia previa del Estado, deben cumplir con requisitos y obligaciones vinculados a estándares tecnológicos y políticas de seguridad, en pos de garantizar la confianza del sistema.

Entre los requisitos y obligaciones que deben cumplimentar los Prestadores de Servicios de Certificación, pueden citarse:

- No almacenar ni copiar los datos de creación de firma de la persona.

- Proporcionar al solicitante, antes de la expedición del certificado, la información mínima que establece la Ley de forma gratuita. (Declaración de Prácticas de Certificación y Políticas de Certificación).

- Mantener un directorio actualizado de certificados en el que se indiquen los certificados expedidos y su vigencia.

- Disponer de un servicio de consulta pública sobre la vigencia de los certificados que sea rápido y seguro.

Para aquellos Prestadores de Servicios de Certificación Reconocidos, la exigencia es aún mayor, debiendo:

- Disponer de las medidas técnicas y organiza-

15 Art. 11 Ley 59-2003
16 ART. 5 Ley 59-2003

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

tivas que garanticen la fiabilidad y seguridad de los servicios (hardware, software, procedimientos de operación y personal empleado).
- Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años.
- Constituir un seguro de responsabilidad civil (o garantía mediante aval bancario o seguro de caución) por un importe de al menos 3.000.000 de euros, para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.

En cuanto a su responsabilidad, como principio general, los Prestadores responden civilmente por los daños y perjuicios que pudieran causar a sus usuarios o a terceros cuando actúen con negligencia en el cumplimiento de sus obligaciones.[17]

En cuanto a su extensión, parte de la doctrina española[18] *coincide que existen límites a la responsabilidad de los Prestadores, que pueden vincularse a su utilización, emitiendo el certificado únicamente para un uso determinado, excluyendo así su responsabilidad cuando el Certificado se aplique en alguna operación diferente; o bien a la cuantía, atento al importe hasta el cual podrán realizar operaciones los titulares de los Certificados emitidos.*
En cuanto a la supervisión, conforme lo estipula el art. 29 de la Ley Española, el Estado, a través de la dependencia competente, controlará el cumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en la ley, y supervisará el funcionamiento del sistema.
En dicho marco, la Ley N° 17/2009, transposición de la Directiva 2006/123/CE, prevé que las Administraciones Públicas pongan en marcha un sistema de ventanilla única a través del cual los prestadores de servicios podrán llevar a cabo en un único punto, por vía electrónica y a distancia, todos los procedimientos y trámites necesarios para el acceso a las actividades de servicios y su ejercicio.
En este sentido, y a efectos de facilitar el uso transfronterizo de las ventanillas únicas con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y el Consejo, relativa a los servicios en el mercado interior, se prevé que cada Estado miembro de la UE publique una «Lista de confianza» que contenga una información mínima referente a los prestadores de servicios de certificación que expidan certificados reconocidos al público, supervisados en ese Estado. Esta Lista debe cumplir las especificaciones técnicas recogidas en el Anexo de la Decisión de ejecución de la Comisión 2013/662/UE, por la que se modifica la Decisión 2009/767/CE en lo relativo al establecimiento, el mantenimiento y la publicación de listas de confianza de proveedores de servi-

17 Art. 26, Ley N° 59/2003.

18 DIAZ BERMEJO, Guillermo *"La Firma electrónica y los servicios de Certificación"*. En publicación de Noticias Jurídicas (en línea) Diciembre 2007. Disponible en Internet: http://noticias.juridicas.com/articulos/20-Derecho-Informatico/200712-123456789.html

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

cios de certificación supervisados o acreditados por los Estados Miembros.

En el ámbito de la UE, los certificados de seguridad han sido expresamente definidos como: "...la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta..."[19].

La Ley española define al certificado electrónico en su artículo 6 como "...un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad".

Estos certificados son emitidos por los Prestadores de Servicios de Certificación o Autoridades de Certificación. Como ya se adelantara, al existir una firma electrónica general y otra cualificada, habrá, correlativamente certificados ordinarios y certificados reconocidos. Éstos últimos son certificados que ofrecen mayores garantías, ya que reúnen una serie de requisitos que aumentan su seguridad:

En el art. 11 de la referida Ley N° 59/2003 se establecen los datos que contendrá el certificado reconocido:

La indicación de que se expiden como tales.

El código identificativo único del certificado.

La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellido completo y su número de documento nacional de identidad, o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

Los datos de verificación de firma que correspondan a sus datos de creación, que se encuentren bajo el control del firmante.

El comienzo y el fin del período de validez del certificado.

Los límites de uso del certificado, si se establecieran.

Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecieran.

Si los certificados reconocidos admiten una relación de representación deben incluir una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente[20].

En cuanto a su vigencia, los propios certificados indican la fecha y hora del inicio y de la finalización de su validez. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

Por regla general, los certificados serán revocados una vez que cumplan el período temporal de validez por el cual fueron creados. Sin embargo, también cabe la posibilidad de que

19 Artículo 2.9 de la Directiva 1999/93/CE

20 art. 13 apartado 2 Ley 29-2003

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

el certificado sea objeto de una revocación anticipada, generalmente cuando la clave privada ha sido puesta en peligro (perdida o extraviada), por lo que puede ser utilizada por personas no autorizadas o para fines ilegítimos.

Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

Resolución judicial o administrativa que lo ordene.

La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c y g del art. 8 de la Ley.-

Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

Asimismo, la Ley 59/2003 reseña como otras causas de extinción, además del vencimiento del plazo por el que fueron emitidos, las siguientes:

Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

Resolución judicial o administrativa que lo ordene.

Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento o extinción de la personalidad jurídica del representado; incapacidad sobreviniente, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.

Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

En los supuestos de expiración de su período de validez, la extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Respecto de la Autoridad Certificante Raíz, al no necesitar en el caso español autorización estatal para funcionar, la misma Autoridad emite su Certificado Digital, es decir que la entidad raíz se auto-firma su certificado de clave pública. De la misma forma, dentro de la jerarquía tiene la capacidad de emitir certificados para Autoridades de Certificación subordinadas e intermedias, y también podrá emitir Certificados al usuario.

B) Firma Digital en Brasil.

En Brasil, con el dictado del Decreto N° 3587 del 5 de septiembre de 2000, se instruye la creación de la infraestructura de Claves Públicas del Poder Ejecutivo Federal, mediante un sistema de Firma Digital basado en criptografía asimétrica, para ser usado en el sector de la Administración Pública Federal.

La Infraestructura de Firma Digital está regulada a través de una medida provisoria (nº 2.200-2), figura legislada en el art. 62 de la Constitución de la República Federativa de Brasil, por la cual se habilita al Presidente a dictar medidas provisorias por razones de necesidad y urgencia, debiendo dar inmediatamente intervención al Congreso. Cuentan con la misma fuerza que las leyes, resultando un equivalente a los Decretos de Necesidad y Urgencia propios de nuestro ordenamiento nacional.

Sancionada en el año 2001, aprueba la Infraestructura de Firma Digital con el objetivo de dotar de validez jurídica, y garantizar de integridad y autenticidad de documentos electrónicos y de las aplicaciones que utilicen Certificados Digitales.

La ICP- Brasil (Infraestructura chave publica do Brasil) está formada por la autoridad Gestora de Políticas, la Autoridad Certificante Raíz, las Autoridades Certificantes, y las Autoridades de Registro. Pero reconoce también Autoridades Certificantes independientes de la ICP Brasil[21], es decir, sin vínculos jerárquicos respecto de ella. Esto fue viable a raíz de una enmienda producida en la Medida Provisoria original, luego de que muchos sectores de la doctrina Brasilera criticaran el monopolio estatal de la actividad certificadora.

La Medida Provisoria designa como Autoridad Gestora de Políticas -lo que en nuestro ordenamiento se conoce habitualmente como Autoridad de Aplicación - al Comité Gestor de la ICP- Brasil, dependiente de la Presidencia de la República, que se encargará de:

1.- Adoptar las medidas necesarias y coordinar la implantación y funcionamiento de la ICP- Brasil.

2.- Establecer la política, criterios y normas técnicas para el licenciamiento de las Autoridades Certificantes, Autoridades de Registro y demás prestadores del servicio de soporte de ICP Brasil, en todos los niveles de la cadena de certificación.

3.-Establecer la política de certificación y las reglas operacionales de la Autoridad Certificante Raíz.

4.- Homologar, auditar y fiscalizar a la Autoridad Certificante Raíz y sus prestadores de servicios.

5.- Establecer directrices y normas técnicas

21 Art. 10 2do párrafo MP 2.200-2/2001

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

para la formulación de políticas de certificados y reglas operacionales de la Autoridad Certificante y de las Autoridades de Registro y definir los niveles de la cadena de certificación.

6.- Aprobar las políticas de certificación, las reglas operacionales, y licenciar y autorizar el funcionamiento de las Autoridades Certificantes y las Autoridades de Registro.-

7.- Identificar y avalar las políticas de ICP externas, negociar y aprobar acuerdos de certificación bilateral, certificación cruzada, reglas de interoperabilidad y otras formas de cooperación internacional. Podrá certificar, cuando fuera el caso, su compatibilidad con la ICP Brasil, observando lo dispuesto en tratados o acuerdos internacionales.-

8.- Actualizar, ajustar y revisar los procedimientos y prácticas establecidas para la ICP Brasil, garantizando su compatibilidad, y promover la actualización tecnológica del sistema y su conformidad con las políticas de seguridad.

La función básica de la Autoridad Certificante Raíz es ejecutar las políticas de certificación y normas técnicas y operacionales aprobadas por el Comité Gestor, actuando en la emisión, expedición, distribución, revocación y gerenciamiento de Certificados Digitales de Autoridades Certificantes de nivel inmediatamente inferior al suyo, llamadas Autoridades Certificantes Principales. También se encarga de la lista de Certificados revocados, emitidos y vencidos, y de la fiscalización y auditoría de las Autoridades Certificantes, Autoridades de Registro, o prestadoras de servicio de soporte habilitadas en el marco de la ICP- Brasil.

La Medida Provisoria designa al Instituto Nacional de Tecnología de la Información como Autoridad Certificante Raíz, dotándolo de autarquía. Está Integrado por un Presidente, una Dirección de Tecnología de la Información, una Dirección de Infraestructura de Clave Pública, y una Procuraduría general.

En ejercicio de sus atribuciones, tiene potestades fiscalizadoras y sancionatorias.

Las Autoridades Certificantes tienen competencia para emitir, expedir, revocar y gerenciar los Certificados, colocar a disposición de los usuarios las listas de Certificados Digitales revocados y mantener el registro de sus operaciones. El par de claves criptográficas emitido, será generado por el titular, y su clave privada de FD será de su exclusivo control, uso y conocimiento.

Son auditadas por la Autoridad Certificante Raíz antes de iniciar la prestación del servicio. Mediante una auditoría, se constatará que se cumplan con las exigencias previstas para la ICP- Brasil, y luego se les otorgará el licenciamiento.

Con posterioridad a su licenciamiento, también deben ser auditadas de manera anual, donde el Instituto verifica que se estén cumpliendo con las normas y exigencias impuestas por la legislación de la ICP Brasil.

Las Autoridades de Registro –al igual que en los sistemas ya descriptos- están operacionalmente vinculadas a determinada Autoridad Certificante. Les corresponde identificar y registrar a los usuarios de Certificados Digitales y son las responsables del proceso final en la cadena de Certificación Digital, atendiendo a

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

los interesados en adquirir Certificados y recolectando la documentación pertinente. Son también auditadas por el ITI (Instrucción Normativa nº 07/2006).[22]

La Medida Provisoria, permite que sean Autoridad Certificante y Autoridad de Registro de la ICP- Brasil todos los órganos o entidades públicas y personas jurídicas de Derecho Privado que cumplan con los requisitos establecidos por el Comité Gestor para licenciarse.

Las declaraciones de los documentos en formato electrónico producidos con la utilización de certificación en el marco de la ICP Brasil, se presumen válidos en relación a los signatarios en la misma forma en que lo determina el Código Civil. Esto significa que los Certificados emitidos por una Autoridad Certificante no perteneciente a la ICP Brasil, no tienen la misma investidura que los emitidos por una Autoridad Certificante que sí depende de ella.

En lo que hace al ámbito de la Administración Pública Federal, el Decreto N° 4414/2002 reglamenta la prestación de Servicios de Certificación Digital, estatuyendo que solamente mediante previa autorización del Comité Ejecutivo del Gobierno Electrónico los órganos y las entidades de la Administración Pública Federal podrán prestar o contratar servicios de Certificación Digital, debiendo hacerlo en el marco de la ICP- Brasil.-

Especial interés reviste el caso Brasileño, a nivel de derecho comparado, en relación con su organización federal. Su ordenamiento de competencias establece claramente que la sanción de la ley es competencia de la "unión" (Nación) ya que la firma es el medio por el cual se le confiere autenticidad a los documentos privados y públicos, y es materia civil. Ello es atribución de las autoridades nacionales, tanto desde el punto de vista normativo, como desde el punto de vista de su ejecución - al reglamentar una infraestructura de Claves Públicas -.

En el mismo sentido, los Estados locales (entendidos como equivalentes a las provincias en nuestra organización política) no pueden rechazar Autoridades Certificantes o de Registro sin violar las reglas de la ICP Brasil. Estas autoridades integran un sistema público centralizado que tiene como primera autoridad de la cadena a la Autoridad Certificadora Raíz.

Así, los Estados reconocen en su normativa local de procedimientos administrativos, la validez de los Certificados emitidos respetando la infraestructura nacional.

III.- MARCO NOMATIVO.[23]

A) Antecedentes

El primer antecedente legislativo en el país relativo a la materia que estamos tratando, data del año 1995, con la sanción de la Ley N° 24.624, que en su art. 30 autoriza el archivo y conservación de documentación en soporte electrónico u óptico indeleble dentro de la Ad-

22 Web del Gobierno de Brasil, ver: http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Documentos%20principais/DOC-ICP-03_Credenciamento_das_Entidades_Integrantes_da_%20ICPBrasil_Versao_4.6.pdf

23 El presente trabajo no incluye modificaciones normativas realizadas a nivel nacional y provincial con posterioridad al año 2015.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

ministración Pública.

Durante el año 1997, se comenzaron a gestar las bases para la operatoria de la Firma Digital. Como primera medida, se dictó el Decreto N° 554/97, mediante el cual se declaró de interés Nacional el acceso de los ciudadanos a Internet. Ese mismo año, la Secretaría de la Función Pública, autorizó la incorporación de la tecnología de la Firma Digital en los procesos de información del sector público. También se concretaron varios proyectos referentes a la implementación de la Firma Digital y Documentos Digitales, a saber: el Ministerio de Trabajo y Seguridad Social dictó la Resolución N° 555/97[24], sobre Normas y Procedimientos para la Incorporación de Documentos con Firma Digital; la Superintendencia de Administradoras de Fondos de Jubilación y Pensiones dictó la Resolución N° 293/97, sobre la Incorporación del Correo Electrónico con Firma Digital; al mismo tiempo, el Ministerio de Justicia de la Nación dio inicio a la elaboración de proyectos concernientes a Instrumento Digital y Firma Digital.

En 1998, la Secretaría de la Función Pública elaboró un proyecto de decreto regulando la Infraestructura de Firma Digital para el Sector Público Nacional, que fue plasmado mediante el dictado del Decreto N° 427/98[25], de Firmas Digitales para la Administración Pública Nacional. Este antecedente es el puntapié inicial para toda la estructura que funciona actualmente.

B) Marco Normativo Nacional

El marco normativo nacional en la República Argentina, en materia de Firma Digital, está constituido por la Ley Nº 25.506 (B.O. 14/12/2001), el Decreto Nº 2628/02 y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

La ley Nº 25.506 establece una Infraestructura de Firma Digital de alcance federal. La norma deroga el anterior Decreto Nº 427/98, por cuanto cubre sus objetivos y alcance.

Más allá de que la normativa en análisis regula cuestiones de derecho de fondo (firma digital, documento electrónico), la invitación que el legislador establece en el art. 50 "... a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente" genera interrogantes que intentaremos dilucidar a lo largo de este trabajo, vinculados con el carácter de fondo o procedimentales de las cláusulas que la conforman.

La necesidad de desentrañar dicha naturaleza, se vincula con la distribución y articulación de competencias entre los diversos niveles de gobierno en el marco del diseño institucional estatuido por la Constitución Nacional, el cual asegura a las provincias su autonomía y regulación de procedimientos administrativos.

El art. 6 de la norma analizada, otorga reconocimiento jurídico al Documento Digital, en el marco de lo establecido por el ordenamiento de fondo.

En el art. 1, a la vez que se define el objeto

24 Resolución MTSS N° 555/97: define el documento digital, la firma digital, el certificador de clave pública, el certificado, la clave privada, la clave pública y dispone que los documentos digitales se considerarán válidos y eficaces, surtiendo todos los efectos legales y probatorios cuando estén firmados digitalmente.

25 (BO 16/04/1998)

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

de la ley, se otorga validez jurídica, tanto a la Firma Digital como a la Firma Electrónica, las cuales constituyen dos subespecies de identificación digital diferenciadas únicamente por el cumplimiento o no de los requisitos establecidos por la ley, más allá de su similitud –o equivalencia- técnica.

En el art. 2 la Ley describe lo que entiende por Firma Digital, 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."

En el renglón siguiente, menciona las dos características básicas que tiene la Firma Digital, a saber: "...ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante (autoría) y detectar cualquier alteración del documento digital posterior a su firma." (Integridad).

La presunción de Autoría implica que se estima, salvo prueba en contrario, que toda firma digital pertenece al titular del CD.

Por otra parte, la Integridad significa que se presume, salvo prueba en contrario, que el documento firmado digitalmente no ha sido modificado desde el momento de su firma.

Ambos caracteres descriptos, son la fuerza interna que hacen a la Firma Digital susceptible de ser considerada como una alternativa válida a la exigencia de firma manuscrita , constituyendo ésta una de las cuestiones más trascendentes del sistema, ya que al equipararla con la firma ológrafa, incorporó a nuestro derecho de fondo el instituto de la Firma Digital.

El art. 2 continúa diciendo que: "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." Según el Decreto N° 2628/02 , la Autoridad de Aplicación será la Jefatura de Gabinete de Ministros.

El art. 3 de la Ley, como ya expresáramos anteriormente, equipara la Firma Digital a la firma manuscrita.

En la normativa Civil vigente en aquél momento que no preveía esta herramienta por su anacronismo, la firma ológrafa era el elemento esencial para la validez de todo acto, ya que no podía ser reemplazada por signos o iniciales.

Lo mismo en el caso de los instrumentos públicos, a los cuales se los sanciona con la nulidad absoluta cuando carecieran de la firma de las partes.

Este artículo entonces vino a modificar las disposiciones mencionadas, salvo en lo que respecta a la aplicación de las excepciones contenidas en el art. 4 de la Ley N° 25.506, donde el legislador, en razón de la naturaleza de los actos allí enumerados, excluye la aplicación de la Ley, no sólo en lo atinente a la aplicación de la Firma Digital, sino también en lo relativo a la posibilidad de conservarse los documentos donde se los instrumente en soporte digital, porque quedan excluidos de todo el plexo normativo.

Ahora bien, el Proyecto de Código Civil y Comercial de la Nación recientemente sancionado, incorpora este precepto, adaptando la

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

normativa de fondo a la ley en estudio.

Así, el art. 286 establece que: "La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos".

Asimismo, el art. 288 referido a la firma, establece que: "La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure razonablemente la autoría e inalterabilidad del instrumento".

Aquí debemos detenernos brevemente en la redacción del último artículo, principalmente en cuanto a la denominación que utiliza para el medio de prueba de autoría.

Al utilizar literalmente la expresión "firma digital", el nuevo Código parece reconocer sólo esa modalidad para probar la autoría de un documento, excluyendo de esta forma la firma electrónica, también regulada con anterioridad por la Ley N° 25.506.

Si bien este no es el objeto del presente trabajo, resulta una cuestión interesante a abordar en sucesivos análisis sobre la materia, a los efectos de dilucidar la correcta interpretación que cabe asignar a la modificación legislativa, concluyendo si se trata de una derogación del instituto de la firma electrónica, o simplemente un modo de referirse a los medios digitales de identificación en sentido genérico, debiéndoselo interpretar armónicamente con las especies reguladas por la Ley de Firma Digital.

Continuando con el análisis del texto legal, el art. 9 de la Ley N° 25.506 enumera taxativamente los requisitos necesarios para que la Firma Digital sea válida, a saber:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la norma, por un certificador licenciado.

Previamente, en su art. 5, la Ley define a la "firma electrónica" como 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, que carezca de alguno de los requisitos legales para ser considerada firma digital". De esta manera, cabe concluir que entre la Firma Electrónica y la Firma Digital –dando por válido que aún coexisten ambos tipos, pese a la literalidad del nuevo Código Civil y Comercial– se da una relación de género-especie, donde la Firma Digital aparece como la especie, contando con mayores exigencias y recaudos.

Si bien en el art. 1 se le reconoce validez jurídica tanto a la Firma Digital como a la Firma

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Electrónica, la diferencia entre una y otra es que a la Firma Electrónica le faltan alguno de los requisitos de validez establecidos en el art. 9 de la Ley.

Es por ello que el valor probatorio atribuido a cada una es diferente, reconociéndose sólo a la Firma Digital las presunciones de autoría e integridad.

De allí que, en el caso de la Firma Digital, el firmante no puede desconocerla sin probar en contrario a la validez del acto; mientras que en el caso de la Firma Electrónica, corresponde a quien la invoca acreditar su validez.

Junto con el Certificado Digital, un documento digital firmado con Firma Digital generará los efectos jurídicos allí establecidos, salvo que quién sea reputado como autor decida cuestionar judicialmente su autoría o integridad, debiendo para ello cumplir con la respectiva carga probatoria.

En conjunto, estas presunciones constituyen la denominada "garantía de no repudio", y otorgan a la operatoria un alto grado de seguridad jurídica y confiabilidad en las transacciones que la incorporan, aún mayor que el que brinda la firma ológrafa.

Según nuestra legislación, habrá Certificado Digital cuando estemos ante un "... documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular." Su función es verificar que la clave pública específica pertenece efectivamente a un individuo determinado.

El art. 3 del Decreto Reglamentario N° 2628/02, establece que "los CD contemplados en el art. 13 de la Ley serán aquellos cuya utilización permite disponer de una FD amparada por las presunciones de autoría e integridad establecidas en los art. 7 y 8 de la ley citada."; y en el art. 2 del mismo Decreto, se dispone que los Certificados Digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica.

Los requisitos de validez que establece el art. 14 son dos:

a) ser emitidos por un Certificador Licenciado por el Ente Licenciante.

En este caso, el inciso nos remite al art. 17 y al punto 5 del glosario del Decreto Reglamentario, en el cual se define al Certificador Licenciado, situándolo en el rol de entidad de confianza que sostiene la infraestructura de la Firma Digital.

b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación.

Esto inserta a nuestra normativa en el ámbito internacional, abriendo un abanico de posibilidades para reconocer la autenticidad de los Certificados Digitales emitidos en el extranjero. La autoridad de aplicación es la Jefatura de Gabinete de Ministros de la Nación ; y el formato estándar reconocido internacionalmente es el "X.509" en su versión 3.

En virtud del art. 16, se considerará válido un Certificado Extranjero siempre que exista pacto de reciprocidad entre el país de origen y el nuestro. Asimismo se requiere que al certificado Extranjero, en su ámbito de origen, se le exijan los mismos recaudos que al nacional. En cuanto a la competencia para la suscrip-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

ción de esta clase de convenios de reciprocidad, el art. 28 del Decreto Reglamentario, faculta para ello a la Jefatura de Gabinete de Ministros de la Nación.

Luego, la Ley establece los recaudos que deben satisfacer los Certificados Digitales, enumerando: I) identificar indubitablemente a su titular y al certificador licenciado que lo emitió; II) indicar el período de vigencia; III) determinar que no ha sido revocado; IV) reconocer claramente la inclusión de información no verificada y; V) identificar la política de certificación bajo la cual fue emitido.

Hay diversas causales de revocación de un CD, enumeradas en el art. 19 de la Ley y el art. 23 del Decreto Reglamentario . En virtud del necesario y permanente control que debe hacerse sobre este extremo, el Certificador Licenciado deberá confeccionar y publicar un listado con los Certificados revocados. Asimismo, la Ley establece, dentro de las obligaciones del titular del Certificado, la de "...solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma".

En cuanto a la Infraestructura de Firma Digital (IFD o PKI) en nuestro país, la Ley N° 25.506 y su Decreto Reglamentario N° 2628/02 dedica la mayor parte de su articulado a establecer cómo funcionará, siendo sus actores los siguientes:

1) Ente Licenciante: la Secretaría de Gabinete y Coordinación Administrativa , otorgando, denegando o revocando las licencias de los certificadores licenciados, y supervisando su accionar, administra la Autoridad Certificante Raíz, la cual constituye la única instalación de su tipo y reviste la mayor jerarquía de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, y emite certificados digitales a las Autoridades Certificantes de los certificadores licenciados, una vez aprobados los requisitos de licenciamiento.

2) Certificador Licenciado: "...toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos" (art. 17, Ley N° 25.506).

Ante una solicitud de licencia realizada por una Empresa u Organismo, se determinará su admisibilidad o no, otorgándose una licencia para cada política de certificación que presente el certificador. La licencia durará 5 años y podrá renovarse, quedando los Licenciados sometidos a auditorías anuales.

En caso de que el Certificador Licenciado cometa alguna falta, el Ente Licenciante podrá instruir un sumario y aplicar sanciones, dentro de las previstas en el capítulo correspondiente de la Ley N° 25.506 según la gravedad de la falta. Más allá de la sanción aplicada, el Certificador Licenciado deberá responder ante terceros por los daños provocados por su

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

conducta.

En nuestro país se han autorizado las siguientes autoridades certificantes: a) ONTI -Oficina Nacional de Tecnología de la Información-, b) AFIP, c) ANSES, d) ENCODESIN (se trata de una empresa privada, siendo ENCODE S.A. el Certificador Licenciado, y la Autoridad Certificante ENCODESIN), e) Poder Judicial de la Provincia de Chubut.

Cabe destacar que existen también otras organizaciones que han sido admitidas en el proceso de licenciamiento, pero aún no han obtenido su aprobación definitiva, tales como la Suprema Corte de Justicia de la Provincia de Buenos Aires, EDICOM S.A. y Tecnología de Valores S.A., entre otras.

Al respecto, el inconveniente que aún no se ha superado en pos de la masificación del uso de esta herramienta, es que la política de registro estatal de los certificadores, propia de nuestro ordenamiento en la materia, y la complejidad que implica cumplir con los requisitos para el licenciamiento, se vuelven una barrera para su utilización fuera del ámbito estatal, e incluso para los poderes provinciales, afectándose así la pronta implementación de servicios que aprovechen la seguridad, celeridad y economía de insumos, derivados de la Firma Digital.

Esto, será objeto de un análisis crítico al final del presente documento, principalmente en lo que hace a su utilización para el ejercicio de la función administrativa de carácter local, dado que puede existir una afectación de las autonomías provinciales en función de la primigenia licencia que deben obtener en el ámbito del Ente Licenciante Nacional y la consiguiente interpretación que se ha extendido en la práctica sobre la correcta aplicación del régimen normativo y sus efectos sobre las presunciones de los documentos firmados digitalmente.

Por tal motivo, analizaremos la competencia provincial en materia regulatoria de herramientas digitales aplicadas a los procedimientos administrativos y a la interrelación administración-ciudadano, y su correcta articulación con el sistema nacional, deslindando su ámbito de aplicación.

3) Autoridades de Registro: Son aquellas entidades que tienen a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados.

Dichas funciones son delegadas por la Autoridad de Certificación, quién además deberá determinar cuál será el procedimiento a utilizar. Como ya se dijera, se comportan como una suerte de “ventanilla de atención”, o puerta de entrada al sistema por parte de los eventuales usuarios (solicitantes de Certificados Digitales), así como asumen también la función de custodios de la documentación pertinente para la acreditación de identidad de los titulares, y garantes de la debida confidencialidad de los datos que aquellas contienen.

4) Autoridades de sello de tiempo y Autoridades de competencia: Estas figuras fueron incorporadas mediante la Decisión Administrativa N° 927/2014 para la prestación de nuevos servicios de certificación.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Las primeras podrán emitir "sellos de tiempo", entendiéndose esto como la indicación de la fecha y hora cierta asignada a un documento o registro electrónico por una entidad habilitada a tal fin y firmada digitalmente por ella, según lo dispuesto en el Anexo I al Decreto N° 2628/02 y sus modificatorios.

Las Autoridades de sello de tiempo podrán prestar sus servicios previa autorización del ente licenciante (art. 22, D.A. N° 927/2014).

Las segundas, denominadas Autoridades de competencia, podrán emitir "sellos de competencia" como herramienta para la confirmación de roles tales como condición de titularidad de las matrículas profesionales, o los cargos en distintas organizaciones o atribuciones de carácter similar.

Las Autoridades de competencia podrán brindar sus servicios constituyéndose como certificadores licenciados u obteniendo un certificado emitido por un certificador licenciado, previa autorización del ente licenciante, aclarándose que las autoridades de competencia pertenecientes al Sector Público sólo podrán emitir sellos de competencia para funcionarios y agentes públicos y cuando sea requerido para el ejercicio de sus funciones (art. 23, D.A. N° 927/2014).

A partir de lo precedentemente expuesto, entre los servicios de certificación digital que podrán brindarse en el marco de la Infraestructura de Firma Digital de la República Argentina, coexistirán certificados digitales que vinculan los datos de verificación de firma a su titular, y sellos de tiempo con indicación de la fecha y hora asignada a un documento o registro electrónico. Adicionalmente, podrán emitirse sellos de competencia, que indican cargo, rol o cualquier otra atribución de su titular.

5) Suscriptores de los Certificados: así denomina la Decisión Administrativa N° 927/14 a los titulares de certificados digitales.

El acuerdo establecido entre el Certificador Licenciado y el suscriptor determina derechos y obligaciones de las partes en lo que respecta a la solicitud, aceptación y uso de los certificados digitales, estando los contenidos mínimos del mismo establecidos mediante Anexo V de dicha norma.

6) Terceros Usuarios: Son las personas físicas o jurídicas receptoras de un documento firmado digitalmente y que consultan para verificar la validez del certificado digital correspondiente.

Los terceros usuarios que sean personas jurídicas y que implementen aplicaciones que requieran Firma Digital, tienen la facultad de definir las características y requerimientos que deben cumplir las Políticas de Certificación a los efectos de aceptar documentos electrónicos firmados digitalmente utilizando certificados digitales amparados por dichas Políticas.

Tales características y requerimientos deben ser manifestados previamente en forma clara y transparente a los titulares de certificados que pretendan operar con ellos.

7) Autoridad de Aplicación: Está determinada en el art. 29 de la Ley N° 25.506, y es la Jefatura de Gabinete de Ministros, quien está

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

facultada para establecer las normas y procedimientos técnicos necesarios para la efectiva implementación de la ley.

8) Sistema de Auditoría: será establecido por la Autoridad de Aplicación con el concurso de la Comisión Asesora, y su objeto es evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de datos, como así también el cumplimiento de las especificaciones del manual de procedimientos y planes de seguridad y contingencia aprobados por el Ente Licenciante.
En cuanto a los Sujetos pasivos de las auditorías son el Ente Licenciante y los Certificadores Licenciados.
Las auditorías podrán hacerse directamente por la Autoridad de Aplicación, o a través de terceras personas habilitadas expresamente a tal efecto; pudiendo tales terceros habilitados ser las Universidades y organismos científicos o tecnológicos nacionales o provinciales, colegios y consejos profesionales que acrediten experiencia profesional en la materia.

Para finalizar el análisis del marco legal, debemos resaltar que la Ley N° 25.506 utiliza una técnica amplia, es decir, regula únicamente el marco legal (método amplio), a fin de poder adaptar la normativa vigente al progreso tecnológico que pudiera experimentar el software aplicable a la Firma Digital, consagrando el principio de neutralidad tecnológica (art. 2).
Cabe aclarar, que esa neutralidad es tal en tanto y en cuanto comprendamos que regula únicamente la herramienta de Firma Digital, no así otros métodos biométricos que pudieran aplicarse a los efectos del reconocimiento de identidad, tal como se aclarase al comienzo de este trabajo al referirnos a las críticas formuladas a la terminología utilizada por parte de la doctrina.
En tal sentido, recepta los principios establecidos internacionalmente de libertad económica, y de equivalencia entre el medio electrónico y el documento en soporte papel y la no discriminación de los medios electrónicos.
Al respecto, enseña Illescas Ortiz[26] *que "...el significado de la regla de la equivalencia funcional debe formularse de la siguiente manera: la función jurídica que en toda su extensión cumple la instrumentación escrita y autógrafa –o eventualmente su expresión oral- respecto de cualquier acto jurídico lo cumple igualmente su instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, alcance y finalidad del acto así instrumentado.* La equivalencia funcional, en suma, implica aplicar a los mensajes de datos electrónicos una pauta de no discriminación respecto de las declaraciones de voluntad o ciencia manual, verbal o gestualmente efectuadas por el mismo sujeto: los efectos jurídicos apetecidos por el emisor de la declaración deben de producirse con independencia del

26 ILLESCAS ORTIZ, Rafael, "*Derecho de la Contratación electrónica" Ed.* Civitas, España, 2001, pág.41.Esta autor recuerda que la primera formulación positiva de la regla tuvo lugar en el artículo 11.2 de la Convención de las Naciones Unidas sobre Garantías independientes y cartas de crédito contingente de 1995, el que establece: "La promesa podrá disponer, o el garante/emisor y el beneficiario podrán convenir en otra parte, que la devolución al garante emisor del documento que contenga la promesa, o algún trámite funcionalmente equivalente a esa devolución, de haberse emitido la promesa en forma que no sea sobre papel, será necesaria para la extinción del derecho a reclamar el pago".

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

soporte escrito –eventualmente oral- o electrónico en el que la declaración conste".

Estos principios (equivalencia y no discriminación) constituyen dos caras de una misma moneda. Decir que el documento digital tiene el mismo valor probatorio que el documento escrito, o decir que una declaración de voluntad emitida mediante un mensaje de datos no puede ser discriminado jurídicamente por el sólo hecho de serlo, es defender, mediante técnicas diferentes, al nuevo medio de expresión.

IV.- NORMATVAS PROVINCIALES, ADHESIONES Y REGLAMENTACIONES LOCALES.

A) Provincias con Infraestructura de Firma Digital propia.

1.- Ciudad Autónoma de Buenos Aires

La Ciudad Autónoma de Buenos Aires adhirió a la Ley Nacional mediante la Ley N° 2751 del año 2008. Ese mismo año, dicta su Decreto Reglamentario Nº 1181/08.-

Por su intermedio, se designa como Autoridad de Aplicación a la Jefatura de Gabinete de Ministros del gobierno de la Ciudad Autónoma de Buenos Aires, como Autoridad Certificante a la Agencia de Sistemas de Información (art. 9 del Decreto Reglamentario) y como Autoridad de Registro a la Dirección General de la Escribanía General. El ámbito de aplicación se limita en principio al Poder Ejecutivo, pero en el art. 15 del Decreto Reglamentario se invita a los demás poderes a dictar las normas que resulten necesarias a fin de implementar la Firma Digital.

Ese mismo año 2008, mediante Decreto 417/08 se instituye la obligatoriedad de la utilización del correo electrónico institucional como medio de comunicación fehaciente para comunicaciones internas no productoras de efectos jurídicos directos – nuevamente se excluye así a los actos administrativos en sentido estricto -, entre organismos que integran la administración pública de la ciudad.

En el año 2009, a través de la Resolución 17/09 se establece la reglamentación para los procedimientos de solicitud, emisión, uso, renovación y revocación de los Certificados Digitales para el empleo de la Firma Electrónica[27]*, y se formula la Política de Certificación para el empleo de la misma en el ámbito del Gobierno de la Ciudad Autónoma de Buenos Aires.*

En el año 2013 la Legislatura de la Ciudad Autónoma dicta la Ley N° 4.736 de Firma Digital del Gobierno de la Ciudad Autónoma de Buenos Aires, regulando la implementación de la misma en todo el sector público de la Ciudad de Buenos Aires.

En su art. 3, designa al Poder Ejecutivo como licenciante y como encargado de implementar la Infraestructura de Firma Digital del Gobierno de la Ciudad Autónoma de Buenos Aires, coordinando con los Poderes Legislativos y Judicial su operatividad y puesta en funcionamiento.[28]

27 Al no contar aún la Ciudad con un Certificador Licenciado por el Ente Licenciante nacional, en el marco de la Ley N° 25.506, las herramientas que aplicaba carecían de uno de los requisitos necesarios para ser consideradas Firma Digital, formando parte entonces del género Firma Electrónica.

28 Art. 2º. Ley N° 4.736: Ámbito de Aplicación. La presente Ley es de aplicación a todas las dependencias del sector público de

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Mediante el Decreto N° 518/14 se estableció que la Secretaría Legal y Técnica será el Ente Licenciante del Gobierno de la Ciudad Autónoma de Buenos Aires, conservándose a la Agencia de Sistemas de información (ASI) como Autoridad Certificante. Las Autoridades de Registro serán la Dirección General de Escribanía General y la Dirección General de Mesa de Entradas, salidas y archivo, ambas dependientes de la Secretaría Legal y Técnica del Gobierno de la Ciudad de Buenos Aires.

Luego la Secretaría Legal y Técnica, en su calidad de Ente licenciante dictó la Resolución nº 283/14 que aprobó la política de certificación del Gobierno de la Ciudad Autónoma de Buenos Aires.

Los certificados emitidos por la Autoridad Certificante podrán usarse para la firma electrónica o cifrado de cualquier informe o documento, y como mecanismo de identificación ante servicios o aplicaciones informáticas implementados por el gobierno de la Ciudad Autónoma de Buenos Aires.-

Quienes podrán suscribir Certificados así emitidos serán:

1.- personas físicas que requieran un Certificado Digital del GCABA para su desempeño como funcionarios o agentes del Sector Público de la Ciudad de Buenos Aires

2.- personas físicas que requieran un Certificado Digital del GCABA para el ejercicio de los derechos y obligaciones que resulten de los procesos de contrataciones de bienes y servicios y de obra pública iniciados en el Sector Público de la Ciudad de Buenos Aires

3.-personas físicas que requieran un Certificado Digital del GCABA para utilizar los servicios del Sector Público de la Ciudad de Buenos Aires.

Finalmente, cabe puntualizar que los certificados emitidos en el marco de la Política de Certificación del GCABA, verifican la autoría e integridad de:

a) documentos electrónicos presentados por personas físicas externas al Sector Público de la Ciudad de Buenos Aires.

b) documentos electrónicos emitidos por el Sector Público de la Ciudad de Buenos Aires.

2.- San Luís

La provincia de San Luis Adhirió a la Ley Nacional mediante la Ley V-0591-2007 y DR 428- MP- 2008, designando a la Universidad de La Punta como Autoridad de Aplicación del mencionado régimen legal, así como también Ente Licenciante de la Provincia de San Luis, lo cual constituye una particularidad a destacar por no tratarse de una dependencia de la Administración Pública central.

Por Resolución Rectoral Nº 2020013-ULP-2009, de fecha 2 de febrero de 2009, se creó en la órbita de la Universidad de La Punta, el Instituto de Firma Digital de la Provincia de San Luis al que se le asignaron las funciones de Ente Licenciante Provincial, encargado principalmente, de otorgar las licencias a los

la Ciudad de Buenos Aires incluidas en las previsiones del artículo 4º de la Ley 70.

Art. 3º. Ley N° 4.736: Infraestructura de Firma digital. El poder Ejecutivo, en su carácter de licenciante, implementa la infraestructura de firma digital del Gobierno de la Ciudad Autónoma de Buenos Aires, que debe ser utilizada por la totalidad de las dependencias alcanzadas por esta Ley, conforme se establece en el artículo 2º, coordinando con los Poderes Legislativo y Judicial su operatividad y puesta en funcionamiento.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Certificadores y de supervisar su actividad.
En esta medida – constitución de un Ente Licenciante propio -, se advierte una clara contradicción con la Ley nacional, la cual seguramente se debe a que, aun cuando en el plano formal el Estado Provincial adhirió a la normativa nacional, no pudo conseguir la autorización que emite la Oficina Nacional de Tecnologías de Información (ONTI) para funcionar como Certificador Licenciado conforme lo establece el artículo 17 de la ley referenciada.
Así, al igual que en el caso de la CABA, resulta motivo de análisis la verdadera naturaleza de la herramienta reglamentada, ya que aun cuando a nivel local se la denomine como Firma Digital, lo cierto es que para la normativa nacional sus efectos se reducirían a los reconocidos a la Firma Electrónica, distinción que surge de los artículos 2 y 5 de la Ley N° 25.506.

B) Provincias sin infraestructura propia

1.- Neuquén

Adhirió a la Ley nacional por medio de la sanción de la Ley N° 2578, reglamentada por el Decreto N° 444/2011.
La normativa provincial, no organiza una infraestructura propia, sino que reconoce a la ONTI como Organismo Certificante (AC), designándose como Autoridades de Registro provinciales al Poder Judicial y a la Secretaria de Gestión Pública.
Su ámbito de aplicación está conformado por el Poder Judicial y el Poder ejecutivo, respectivamente.

2.- San Juan

Formuló su adhesión a la Ley Nacional mediante la sanción de la Ley N° 8128, del año 2010, reglamentada mediante el Decreto N° 1/2014.
El art. 5 del Decreto Reglamentario, instituye como Autoridad de Aplicación de la Firma Digital en el ámbito provincial a la Secretaría de Gestión Pública, a través de la Dirección General de Recursos Humanos y Organización, facultándola para constituirse en Autoridad de Registro de la Autoridad Certificante ONTI.

3.- Santa Fe

El 17 de marzo del año 2005, se firmó un Convenio de Cooperación en materia de Firma Digital entre la Subsecretaría de Gestión Pública de la Jefatura de Gabinete de Ministros de la Nación y el Gobierno de la Provincia de Santa Fe, aprobado por la Legislatura provincial mediante la sanción de la Ley N° 12.492.-
En diciembre de ese mismo año, y sobre las bases del Convenio citado, se sanciona la Ley de adhesión a la Ley Nacional de Firma Digital Nº 12.941.-
En ese derrotero, mediante la Resolución N° 0386/07 del Ministerio de Hacienda y Finanzas provincial, se designó como Oficiales de Registro de la Autoridad de Registro dependiente de la Autoridad Certificante ONTI, a la Dirección General de Recursos Humanos de la Provincia[29]*.*

4.- Tierra del Fuego

29 La ONTI, por Disposición N° 0015/07 convalidó las designaciones del personal de la Dirección General de Recursos Humanos de la Provincia como Oficiales de Registro.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Originariamente adhirió a la Ley Nacional mediante la sanción de la Ley Provincial Nº 633/2004. Esta ley nunca fue reglamentada, y finalmente, en el año 2013, se dictó la Ley N° 955 que implementó la Firma Digital en la Provincia.

Su reglamentación fue instrumentada a través del Decreto N° 1/2014, designándose como Autoridad de Aplicación a la Secretaría de Informática y telecomunicaciones (art. 2 del anexo del Decreto Reglamentario). Al igual que en los casos anteriores, se reconoce la infraestructura nacional y se designan como Autoridades de Registro, dependientes de la Autoridad Certificante nacional ONTI, a los Poderes Ejecutivo y Judicial de la provincia.

5.- Tucumán

Adhirió a la normativa nacional mediante la sanción de la Ley N° 7.291, reglamentada por Decreto N° 1190/10. El marco provincial se limitó a reconocer la Infraestructura nacional, designándose como Autoridad de Registro de la Autoridad Certificante ONTI al Poder Judicial, a la Legislatura y a la Secretaría de Coordinación y Gestión Pública.

6.- Chaco

La Legislatura provincial sancionó la Ley de adhesión Nº 6.711 en el año 2010, reglamentándose a través del dictado del Decreto N° 99/11.

Reconoce en una primera instancia en su totalidad la Infraestructura nacional hasta tanto exista un Organismo provincial con licencia y en condiciones de certificar la Firma Digital, facultando a cada poder del Estado para que, a través del área de Recursos Humanos, se constituya en Autoridad de Registro. Así, hasta el día de la fecha, en este marco transitorio y según el listado actualizado de las Autoridades de Registro dependientes de la Autoridad Certificante ONTI, sólo se han constituido como Autoridad de Registro dentro de la Provincia el Poder Ejecutivo y el Poder Judicial.

C) El caso de la provincia de Buenos Aires

1.- Marco general

Al igual que lo que sucede a nivel nacional, en el ámbito provincial existen diversas normas relativas a la firma digital.

En primer lugar debemos mencionar la Ley N° 13.666 por la que se adhiere al régimen instaurado por la Ley nacional N° 25.506, con el propósito de asimilar al derecho local los institutos regulados por leyes nacionales que resulten necesarios a los efectos de garantizar la vigencia de la normativa de fondo. Esta ley se encuentra reglamentada por el Decreto N° 305, del 9 de mayo de 2012, derogatorio del Decreto N° 1388/08.

Por el decreto reglamentario se ha dispuesto que la autoridad de aplicación de la Ley N° 13.666 sea la Secretaría General de la Gobernación. [30]

La ley local señala como ámbito de aplicación a los Poderes Ejecutivo, Legislativo y Judicial de la provincia, los Municipios, la Administración Centralizada y Descentralizada, los Organismos de la Constitución, Entes Autárquicos

30 Decreto N° 305/12, artículo 2°.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

y todo otro Ente en que el Estado Provincial o sus Organismos Descentralizados tengan participación suficiente para la formación de sus decisiones. La autoridad de aplicación ejercerá la coordinación de las acciones vinculadas a la implementación y utilización de la firma digital en el ámbito de aplicación de la ley.

Con respecto a los estándares tecnológicos y de seguridad aplicables, la Autoridad de Aplicación será la encargada de determinar dichos criterios, así como los procedimientos de firma, verificación, certificación y auditoria, los que deberán ser consecuentes con los utilizados por el Gobierno Nacional y las regulaciones internacionales.[31]

Por otra parte, el Decreto Reglamentario destina un artículo a la Infraestructura de Firma Digital del Gobierno provincial, la que estará conformada por Organismos Certificadores, Autoridades de Registro, titulares de certificados digitales y el conjunto de equipamiento, software, normas, políticas y procedimientos requeridos para la generación, almacenamiento y publicación de los Certificados Digitales.[32]

El Organismo Certificador previa autorización de la Autoridad de Aplicación, podrá inscribirse como Certificador Licenciado en los términos de la Ley Nacional Nº 25.506 y Decreto Reglamentario Nacional Nº 2.628/02. Para el cumplimiento de las responsabilidades a su cargo, el Organismo Certificador deberá delegar en Autoridades de Registro las funciones de recepción y registro de las presentaciones y trámites que le sean formuladas, y la validación de identidad y otros datos de los suscriptores de certificados.

En este punto, el decreto reglamentario designa a la Secretaría General de Gobernación como Organismo Certificador para la Administración Pública Provincial central, autorizándosela a requerir su reconocimiento como Certificador Licenciado.[33]

En cuanto a los certificados digitales, el artículo 7 de la Ley determina que las certificaciones para agentes de la Administración Pública Provincial y Municipal, destinados a la gestión interna de los Organismos, y la Certificación de particulares para cumplimiento de trámites ante la Administración Pública Provincial y Municipal, con la correspondiente generación de la clave pública, serán emitidas por el Organismo Provincial ya aludido.

Sin perjuicio de ello, la Secretaría General de Gobernación podrá reconocer certificados de particulares emitidos por certificadores de otras jurisdicciones para la realización de trámites ante la Administración Pública Provincial y Municipal, mediante la firma de convenios con otras jurisdicciones para el reconocimiento recíproco de certificados emitidos por sus propios certificadores.

La titularidad de los Certificados Digitales podrá recaer en todos los agentes y funcionarios del Estado Provincial, así como las personas físicas o jurídicas que se relacionen con la misma.[34]

Por último, se establece que las Autoridades de Registro asociadas a Organismos Certificadores Licenciados, sean éstos provinciales

31 Ley N° 13.666, artículos 3 y 4.
32 Decreto N° 305/12, artículo 4.
33 Decreto N° 305/12 artículo 8.
34 Decreto N° 305/12 artículo 7.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

o nacionales, podrán ser constituidas previa notificación a la Secretaría General de Gobernación; y finalmente designa a la Dirección Provincial de Personal de la Provincia de Buenos Aires y sus Delegaciones Sectoriales como Autoridad de Registro para el ámbito de la Administración Pública Provincial central.[35]

2.- Modificaciones introducidas por el Decreto N° 305/12

Como enunciáramos anteriormente el Decreto N° 305/12 vino a reglamentar la Ley N° 13.666, derogando de ese modo la anterior reglamentación del citado cuerpo legal, que había sido dispuesta por Decreto N° 1388/08 del Poder Ejecutivo Provincial.

Nos propondremos en este acápite analizar los cambios introducidos por la nueva reglamentación, a la luz del régimen que estaba anteriormente vigente.

No se observan cambios en lo que respecta a los estándares tecnológicos y de seguridad aplicables y a los procedimientos de firma, verificación, certificación y auditoría, ya que en ambos supuestos se previó que estuvieran en consonancia o conformidad con los utilizados a nivel nacional y las regulaciones internacionales (artículos 2 y 5 del Decreto N° 1388/08 y artículo 3 del Decreto N° 305/12).

Con relación a la Infraestructura de Firma Digital no se registran alteraciones sustanciales, toda vez que la misma está integrada por similares elementos: a) Organismos Certificadores, b) Autoridades de Registro, c) titulares de certificados digitales y d) el conjunto de equipamiento, software, normas, políticas y procedimientos requeridos para la generación, almacenamiento y publicación de los certificados digitales. Sólo se advierte que el Decreto N° 1388/08 se refiere a la figura de Autoridad Responsable de la Infraestructura Tecnológica (Dirección Provincial de Comunicaciones, conforme lo establecido en los artículos 26 y 27 del referido Decreto), cuestión soslayada en su similar N° 305/12. Sin perjuicio de ello, estimamos que esta omisión resulta irrelevante en la medida que el Decreto N° 666/12 asigna a la Dirección Provincial de Sistemas de Información y Tecnologías la responsabilidad de asistir al Secretario General y a las restantes áreas que integran la jurisdicción, así como a los restantes organismos y jurisdicciones que integran la Administración Pública Provincial y Municipal, en los asuntos vinculados al desarrollo de la Firma Digital Ley Nº 13.666, su reglamentación y dictado de normas modificatorias y complementarias en lo que hace a la competencia de sistemas y tecnologías.

Adentrándonos ya en el terreno de las diferencias, debemos señalar fundamentalmente que el Decreto derogado preveía la existencia de un Certificado Digital Raíz del Estado Provincial, el cual daba origen y sostén a la infraestructura de firma digital. El titular de dicho Certificado resultaba ser el Poder Ejecutivo Provincial y su administración quedaba a cargo de la Autoridad de Aplicación (Secretaría General de la Gobernación).

También se hablaba de un Certificado Digital Raíz del Organismo Certificador, el cual era

35 Decreto N° 305/12 artículo 10.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

asignado por el Administrador del Certificado Digital Raíz del Estado Provincial. Conforme surge del artículo 17 del Decreto derogado la Escribanía General de Gobierno de la Provincia de Buenos Aires era la autoridad designada como Organismo Certificador para todo el ámbito de aplicación descripto en el artículo 2 de la Ley. Es decir que era una autoridad única para todo el Poder Legislativo y Judicial, Municipios, Administración Centralizada y Descentralizada, Organismos de la Constitución, Entes Autárquicos y todo otro Ente en el que el Estado Provincial - o sus Organismos Descentralizados - tuviera participación suficiente para la formación de sus decisiones.

Luego cada Poder debía designar, en el ámbito de su competencia, al Organismo que cumpliría en rol de Autoridad de Registro, para los agentes y funcionarios de su jurisdicción (artículo 20). En el ámbito del Poder Ejecutivo se asignó dicha función a la Dirección Provincial de Personal de la Provincia de Buenos Aires, y como Autoridades de Registro de cada Repartición, a sus Delegaciones Sectoriales (artículo 21).

Esta mención al Certificado Raíz provincial, ponía a la provincia en una situación similar a los casos analizados anteriormente de la Ciudad Autónoma de Buenos Aires y de la provincia de San Luis, ya que aun cuando legislativamente se hubiese adherido a la normativa nacional, cierto es que el sistema provincial escapaba a sus previsiones basándose en un certificado primigenio que no había sido emitido por el ente Licenciante nacional.

Es decir que, conforme la ley nacional de Firma Digital, los certificados emitidos por las Autoridades Certificantes que se constituyeran a nivel provincial, no serían válidos como Firma Digital, sino que caerían en el género Firma Electrónica, no contando por ello – fuera del ámbito de la provincia de Buenos Aires – con las presunciones que otorgan seguridad jurídica a transacciones informáticas firmadas digitalmente.

Para subsanar dicha incongruencia, el Decreto N° 305/12 modificó las cuestiones apuntadas evitando la mención al concepto de Certificado Digital Raíz del Estado Provincial propio del anterior Decreto.

La actual reglamentación (artículo 8) se designa como Organismo Certificador para la Administración Pública central a la Autoridad de Aplicación (Secretaría General de la Gobernación).

Asimismo, el artículo 7 encomienda a la Autoridad de Aplicación la designación de los Organismos que actuarán como Organismos Certificadores Licenciados en los términos de la Ley Nacional N° 25.506 para el ámbito de aplicación de la Ley N° 13.666, estableciendo que los Organismos designados serán autorizados por la Autoridad de Aplicación para requerir su reconocimiento como Certificadores Licenciados ante la autoridad nacional competente, en el plazo que la misma fije al efecto.

También se dispone (artículo 8 in fine) que la Autoridad de Aplicación podrá desempeñarse como Organismo Certificador Licenciado respecto de cualquiera de los entes enumerados en el artículo 2° de la Ley N° 13.666 que así lo requieran.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

La infraestructura descripta, nos permite entonces advertir nuevas diferencias respecto de la reglamentación anterior. En el régimen anterior el Organismo Certificador (Escribanía General de Gobierno) era único para todo el ámbito de aplicación de la Ley, y por ende el mismo para todos los poderes que sólo podían designar sus Autoridades de Registro; mientras que el actual permite la constitución de otros Certificantes Licenciados ante las autoridades nacionales, previa autorización de la Autoridad de Aplicación.[36]

3.- Resolución SG N° 23/13[37]. Prueba Piloto de Firma Digital

Con la finalidad de avanzar en la sensibilización de los agentes y funcionarios que componen la Administración provincial, la Secretaría General de la Gobernación diseñó en el año 2013 una prueba piloto, -aprobada mediante el dictado de la Resolución SG N° 23/13[38] - por la cual se constituyó, a través de la Dirección Provincial de Sistemas de Información y Tecnologías, en Autoridad de Registro dependiente del Certificador Licenciado ONTI (de nivel nacional, como ya se explicara anteriormente).

Este proyecto, tal como se desprende de la motivación de la Resolución que lo origina, tiene como objetivo avanzar en el proceso de digitalización de los procedimientos administrativos y servicios que brinda la Administración Pública provincial, a través de la progresiva utilización de la tecnología de Firma Digital, con un horizonte temporal de dos años estimado suficiente para lograr la estabilización de la infraestructura necesaria para constituirse la propia Secretaría General en Autoridad Certificante, tal como se reglamentara oportunamente.

Al respecto, debe destacarse que, en virtud de la atribución conferida por el artículo 2° del Decreto N° 305/12, le corresponde a la Secretaría General de la Gobernación – como Autoridad de Aplicación - coordinar las acciones tendientes a implementar la utilización de Firma Digital en el ámbito de aplicación definido por el artículo 2° de la Ley N° 13.666, quedando facultada para el dictado y aprobación de la normativa que resulte necesaria a tal efecto.

Es en virtud de dichas atribuciones es que se procedió al desarrollo de la prueba piloto, la cual no hace más que generar una instancia transitoria a los efectos de dotar de plena validez y eficacia jurídica a los certificados digitales a ser utilizados durante su transcurso, permitiendo en forma inmediata obtener avances en la despapelización y digitalización de las comunicaciones internas de la administración y la prestación de servicios a los ciudadanos, en un esquema similar al aplicado en los casos ya analizados de provincias que no cuentan con infraestructura propia.

Tales adelantos, constituirán un cúmulo de información y experiencia que permitirán un paso no traumático hacia la generalizada uti-

36 En el régimen actual cada poder puede establecer y solicitar el reconocimiento de su propio Organismo Certificador, previa autorización de la Secretaria General de la Gobernación y siempre que se obtenga el dictamen favorable del ente licenciante raíz (Jefatura de Gabinete de Nación), tal como acontece en el expediente actualmente en trámite bajo el N° 2100-13558/12

37 B.O. 25-09-2013.

38 La prueba piloto fue recientemente prorrogada por 2 años, extendiendo su vigencia hasta el año 2018.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

lización de la Firma Digital, una vez que la Secretaría General de la Gobernación se encuentre habilitada por el Ente Licenciante nacional para operar como Certificador Licenciado.

V.- NATURALEZA DE LA FD Y COMPETENCIAS REGULATORIAS.

Descripto el marco legal aplicable, tanto a nivel nacional como local, y relevados algunos sistemas comparados, resulta necesario efectuar un análisis crítico de la actual estructura, a los fines de aventar las dudas interpretativas que se han suscitado en la última década y media, desde la sanción de la Ley N° 25.506, con motivo de las diferentes modalidades de adhesión provincial.

Es claro en esta instancia que la Ley de Firma digital contiene tanto disposiciones que hacen a la regulación de fondo, potestad del legislador nacional, como cuestiones procedimentales y de derecho público, facultad que tienen tanto el gobierno nacional –en su ámbito de competencia federal– como los gobiernos provinciales a nivel local, en ejercicio de su autonomía reconocida constitucionalmente.

Es decir que allí donde nos encontremos ante preceptos normativos que rijan en forma abstracta relaciones jurídicas que eventualmente se entablen entre particulares, la competencia del Congreso Nacional resulta indiscutida.

Mientras que en lo que hace a la regulación e implementación de procedimientos administrativos, que encaucen la relación entre los estados locales y los habitantes de las provincias, la facultad regulatoria se encuentra en cabeza de las Legislaturas provinciales, debiendo el Estado Nacional abstenerse de avanzar en tal sentido.

En ese derrotero, resulta necesario en primer lugar clarificar la naturaleza de las disposiciones legales vinculadas con la firma digital y, derivado de ello, la instancia regulatoria –nacional o local– a la cual efectivamente le compete su dictado y organización.

Como ya lo adelantáramos, los preceptos que conforman el texto de Ley N° 25.506, no revisten una única naturaleza, adentrándose su primera parte principalmente en la regulación de fondo del instituto de la Firma Digital, para luego abarcar también cuestiones procedimentales, régimen sancionatorio, de auditorías y competencias propias de las dependencias del Poder Ejecutivo nacional que deben ser reputadas como pertenecientes al Derecho Público.

Esto último explica la invitación que se formula en el artículo 50 a las jurisdicciones provinciales para su adhesión, ya que, en lo que hace a los procedimientos administrativos propios de su organización institucional, los poderes constituidos nacionales no tienen injerencia regulatoria, debiendo ser voluntaria la incorporación de las provincias al sistema.

En dicho marco, las adhesiones a la cadena de confianza regulada a nivel nacional no representan mayores dificultades regulatorias o interpretativas -tal el caso de la provincia de Buenos Aires-, pero diferente será el análisis que deba efectuarse cuando la adhesión no sea plena, o bien directamente las jurisdiccio-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

nes locales regulen su propia infraestructura de Firma Digital o Electrónica (cuestión meramente nominal), asignando a los certificados que por ella se emitan idénticas presunciones a las que el Legislador nacional atribuyó a la Firma Digital.

Dicho análisis, no se vincula estrictamente con lo normativo, sino que debe partir de cuál es la utilización de los medios digitales de identificación de autoría. Es decir que no cabe partir de qué es lo que regulamos, sino a qué aplicamos dicha regulación. Aclarando más la cuestión, entendemos que no debemos centrarnos en la naturaleza del precepto legal, sino en la esencia de la relación jurídica a la cual aplicamos dichas disposiciones normativas.

Siguiendo este razonamiento, allí donde estemos ante un negocio jurídico entre privados, regido por lo tanto por el derecho de fondo, la Ley N° 25.506, así como su reglamento de ejecución, serán íntegramente aplicables en todo el territorio provincial; mas cuando se trate de un procedimiento administrativo que sustancie la relación de colaboración que debe existir entre el Estado y los particulares, sólo será aplicable cuando la parte pública de la vinculación esté encarnada por el Estado Nacional, mientras que en los procedimientos administrativos locales, las legislaturas provinciales podrán adecuarse o no a la norma nacional, conforme acepten la invitación a adherir formulada por el Congreso Nacional.

Es esta la única interpretación armónica que puede hacerse a los fines de compatibilizar la integridad del texto de la Ley N° 25.506, con la autonomía que la Constitución Nacional reconoce a las provincias preexistentes para su organización institucional local.

Ahora bien, cabe preguntarse qué sucede con los certificados emitidos en aquellas provincias que no adecuaron su infraestructura de Firma Digital al texto de la Ley nacional aludida, ya sea porque formularon una adhesión parcial, o porque directamente decidieron regularlo en forma independiente -tales los casos de la provincia de San Luis o la Ciudad Autónoma de Buenos Aires-.

Estaríamos entonces en presencia de la otra cara de la moneda. Allí donde las provincias regulen cuestiones atinentes a su vinculación con los particulares en lo que hace a normas procedimentales de carácter administrativo, tendrán amplia libertad regulatoria; mas no podrán adentrarse en cuestiones que hacen a los negocios del ámbito del derecho privado, so pena de caer en una manifiesta inconstitucionalidad.

Recapitulando, podemos recordar que la firma digital no solamente se utiliza como medio de prueba de autoría de un documento, sino que también existen los denominados Sellos de Competencia, que tienen como finalidad acreditar una calidad determinada del firmante. Es decir, que con ello puede comprobarse que el documento ha emanado de un representante de cierta organización o del funcionario que ostenta la competencia propia de un cargo en el ámbito de la administración pública.

En este último caso -es decir en lo referido al ejercicio de la función administrativa-, adquieren particular relevancia este tipo de

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

herramientas tendientes a acreditar competencia, ya que al actuar los funcionarios públicos como órganos de la administración (CSJN, "Vadell, Jorge Fernando c/ Provincia de Buenos Aires s/ indemnización", Fallos 306:2030), y no como personas del derecho privado, como lo hacen en el cotidiano de su vida de relación, los sellos de competencia serían elementos claramente subsumidos en el ámbito de regulación subnacional, dado el carácter local de los órganos que conforman los gobiernos provinciales y municipales.

De allí, que dichos certificados sólo podrían ser emitidos en el marco de la regulación emanada de las Legislaturas provinciales, ya sea mediante la adhesión a la Infraestructura nacional, como a través de un sistema íntegramente local, y las presunciones de autoría e integridad que se otorgue a tales documentos sólo podrán ser evaluadas a la luz de la normativa provincial.

En este punto, debemos detenernos en el criterio sentado por la CSJN en el caso "Barreto, Alberto Damián y otra c/ Provincia de Buenos Aires y otro s/ daños y perjuicios" (Fallos 329:759), que al precisar y acotar el concepto de "causa civil" para determinar la competencia originaria del Máximo Tribunal, estableció claramente que la validez -o por el contrario su nulidad- de los actos de los órganos de la administración, sólo puede ser analizada desde la óptica de la regulación local, o sea, por normas de Derecho Público en el marco de nuestra organización constitucional.

Es decir que, allí donde intenten hacerse valer actuaciones de carácter administrativo en las cuales se hayan aplicado herramientas digitales para probar autoría e integridad, sea dentro del ámbito provincial o fuera de él, quienes deban interpretar la validez de dichas actuaciones, deberán hacerlo tomando como marco regulatorio el correspondiente a la jurisdicción donde se emitió dicho acto o se sustanció tal procedimiento.

Siguiendo dicha lógica, las presunciones asignadas a los documentos firmados digitalmente en el marco de las regulaciones dictadas por aquellos Estados locales que no resuelvan voluntariamente adherir a la PKI nacional, serán plenamente válidas y oponibles en todo el territorio nacional -y ante cualquier autoridad-, siempre que se vinculen con actos o procedimientos administrativos, y no con negocios jurídicos del ámbito del Derecho privado.

De todas maneras, resta aún un punto de conflicto entre la interpretación propuesta y las normas reglamentarias dictadas a nivel nacional.

Si bien el por el artículo 50 de la Ley N° 25.506 se invita a las Provincias a dictar los instrumentos necesarios para adherir al sistema, se generan dudas acerca de la constitucionalidad del sistema conforme los términos del artículo 37 del Decreto Reglamentario N° 2628/02, el cual extiende al ámbito de aplicación de las disposiciones de la Ley nacional y su Decreto Reglamentario a la digitalización de procedimientos y trámites internos no sólo en el ámbito de la Administración Pública Nacional, sino también en el caso de las Administraciones Públicas Provinciales, y de los Poderes Legislativos y Judiciales del orden

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

nacional y provincial.

Aquí nuevamente debe primar un criterio interpretativo que atienda a compatibilizar armónicamente la totalidad del sistema, concluyendo que la disposición reglamentaria se refiere únicamente a aquellos casos en los cuales las provincias hayan adherido íntegramente a la regulación nacional en el marco de la invitación formulada, pero no alcanza –ni por lo tanto invalida– aquellos procesos de digitalización de trámites regulados en forma independiente a nivel local.

Como conclusión, podemos aseverar que la coexistencia de los regímenes propios de los diferentes niveles de gobierno, es perfectamente compatible, en tanto y en cuanto se deslinden adecuadamente sus competencias y ámbitos de aplicación, pudiendo armonizarse diversidades que, en definitiva, son la esencia misma de un sistema federal.

Sin perjuicio de ello, resulta atendible la inquietud en torno a la necesidad de coordinar acciones y políticas de certificación, necesarias para dotar de estabilidad, confianza y previsibilidad a todo el sistema en el territorio nacional. Pero entendemos que en el marco de nuestra organización federal, tales acciones deben surgir de la voluntad mayoritaria expresada en el seno de organismos interjurisdiccionales de concertación federal, donde todos los gobiernos -incluyendo al nacional-, puedan exponer sus necesidades y proyectos en ejercicio de su autonomía, arribándose a soluciones consensuadas y no impuestas desde una lógica centralista.

De allí, tomando como ejemplo a seguir algunas experiencias comparadas analizadas en el presente trabajo, pueden surgir instrumentos legales modelo que se repliquen luego en los Estados locales; o bien políticas de seguridad comunes con estándares mínimos que aseguren la fiabilidad de las infraestructuras locales, de forma tal de contribuir a la confianza en la totalidad del sistema sin avasallar las autonomías provinciales.

En síntesis, la lógica derivada de una diversidad federal moderada por mecanismos consensuados de coordinación, resultará en la progresiva extensión de la utilización de las nuevas herramientas digitales, contribuyendo al proceso de modernización de los estados y facilitando una actividad gubernamental cada vez más ágil, eficaz y eficiente, en un marco de participación, colaboración y transparencia.

VI. CONSIDERACIONES FINALES

Hemos procurado a lo largo de la investigación realizada analizar los aspectos técnicos y legales vinculados a la firma digital, con el objetivo de comprender cabalmente el instituto, emprendiendo luego la tarea de relevar la realidad de su aplicación a nivel provincial.

Como corolario de ello, podemos afirmar que si bien los avances han sido sustanciales a lo largo de la última década, no se ha conseguido aún la utilización generalizada de los sistemas electrónicos de identificación que aseguren la mayor velocidad de las transacciones entre privados, así como una eficiencia creciente en la prestación de servicios por parte de la administración pública.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

Sin duda ello se debe a múltiples factores que exceden al marco de este trabajo, sin perjuicio de los cual podemos señalar, como ruta para futuros estudios complementarios, la necesidad de clarificar aún más la naturaleza de las disposiciones legales vinculadas con la firma digital y, derivado de ello, la instancia regulatoria – nacional o local – a la cual le compete su dictado y organización.

Claro es que, allí donde nos encontramos ante transacciones entre particulares, la firma digital se comporta como un instituto de fondo, resultando el legislador nacional su natural regulador.

Pero mayores dificultades ha suscitado su utilización por las autoridades locales en el ejercicio de función administrativa, ello en razón de las competencias atribuidas por el marco regulatorio de la firma digital a órganos que conforman la administración nacional, sujetándose, a primera vista la implementación de la firma digital en los procedimientos locales a determinados requisitos de autorización ante entes nacionales que pueden resultar contradictorios con el carácter local de los procedimientos administrativos.

En función de ello, dado el inevitable cruce de competencias regulatorias de distinto nivel, y la dispar aplicación de la herramienta, según se trate de actos de derecho privado o administrativos, resultaría adecuada una revisión integral del sistema que considere la experiencia recogida y, mediante mecanismos de concertación federal, proyecte alternativas superadoras de las dificultades constatadas.

Este punto debe ser profundizado, no por un mero apego a las cuestiones teóricas, sino porque del relevamiento efectuado acerca de la evolución local de la utilización de la firma digital surge que allí se han suscitado las más arduas discusiones, marchas y contramarchas, demorándose el objetivo común de agilizar los servicios que se brindan al ciudadano.

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

BIBLIOGRAFÍA:

- *AIRTON, Roberto Guelfi.* "Análise de elementos jurídico – tecnológicos que compoem a assinatura digital certificada digitalmente pela Infra-estrutura de chaves publicas do brasil –ICP- Brasil." Universidade de sao Paulo. Escola Politécnica. Sao Paulo 2007.-

- *ARAUJO CASTRO, Aldemario.* "O Documento eletrônico e a assinatura digital (Uma visão geral). Disponible en: www.aldemario.adv.br/doceleassdig.htm

- *Autoridad Certificante de la Administración pública.* https://pki.jgm.gov.ar/app/

- *BARBERÁN, BARBERÁN, BONTEMPO, LENS, PEREZ WILIAMS, SCATTOLIN, "Firma Digital".* Master en Dirección de Empresas- Universidad del Salvador (Argentina) – Universidad Deusto (España)- Cátedra Marco Legal – Año 2004. Disponible en http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosFirmaDigital.htm

- *BAUZÁ MARTORELL, Felio José "Acceso Electrónico de los ciudadanos a los servicios públicos liberalizados"- España- Disponible en: http://estuderecho.com/sitio/?p=1097*

- *CABULI, Ezequiel, "Las nuevas tecnologías en el Proyecto de Código".* Publicado en LA LEY 22/02/2013. AR/DOC/6066/2012.-

- *DIAZ BERMEJO, Guillermo "La Firma electrónica y los servicios de Certificación".* En publicación de Noticias Jurídicas. Diciembre 2007. Disponible en Internet: http://noticias.juridicas.com/articulos/20-Derecho-Informatico/200712-123456789.html

- *FARRÉS, Pablo; "Firma Digital", Buenos Aires, Ed.* Lexis. Año 2005.

- *FERRARO, Ricardo H.* "AFIP implementó la gestión de autorizaciones electrónicas para firma digital". AR/DOC/5276/2012.-

- *GONZALEZ GOMEZ, Pedro M.* "Equiparación a la ológrafa de la firma informática argentina" Publicado en: Sup. Act. 12/04/2007.-

- *ILLESCAS ORTIZ, Rafael, "Derecho de la Contratación electrónica" Ed.* Civitas, España. Año 2001.-

- *Instituto Nacional de Tecnologia da Informação.* Disponible en www.iti.gov.br

- *Jefatura de Gabinete de Ministros de la Nación- Proyecto de Modernización del Estado.* Disponible en: http://www.jefatura.gob.ar/archivos/pme/actividades/467.pdf

- *Ley modelo de la CNUDMI sobre firmas electrónicas.* La guía para su incorporación al derecho interno. Disponible en: www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

- *LYNCH, Horacio M.,* "Comentario a la ley 25.506 de firma y documento digital." Publicado en ADLA 2002-A, 1555. Ed. La Ley, Boletín informativo año 2001, Nro. 34.-

- *MOLINA QUIROGA, Eduardo.* "Ley de expedientes digitales y notificaciones electrónicas judiciales". LA LEY 22/06/2011.-

- *MORA, Santiago, "Documento digital, firma electrónica y digital" Publicado en LA LEY 31/12/2013 – Enfoques 2014 (Febrero)- AR/DOC/3995/2013.-*

- *Observatorio de políticas públicas - Coordinación general del cuerpo de Administradores gubernamentales – Jefatura de gabinete de ministros.* "E autenticación. Firma Digital y Firma electrónica. Panorama en la República Argentina. Agosto 2007.-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org

- *RAUEK DE YANZÓN, Inés.* "La implementación del principio procesal de digitalización" Publicado en: Sup.Act 07/12/2006.-

- *TEMPERINI, Marcelo.* "Firma Digital en Argentina: manteniendo la ilusión"- Disponible en: http://www.elderechoinformatico.com/publicaciones/mtemperini/Firma_Digital_en_Argentina_Temperini.pdf

- *VENTURA, Gabriel O.* "Firma Digital Análisis exegético de la ley 25.506" Disponible en: www.acaderc.org.ar

- *VERNET, Tomás.* "FIRMA DIGITAL" Universidad Abierta Interamericana. Sede Regional Rosario, Facultad de Derecho. Agosto 2003.-

GOVERNEO
Calle 12 N°823 1° B, La Plata, Buenos Aires
+54 0221 4824582 - info@governeo.org