Kozameh, Ernesto N.
Cuadernos de Derecho Judicial nº 6 : comunicación interjurisdiccional electrónica. - 1a ed. - Buenos Aires : Universidad Austral, 2010.
v. 6, 176 p. ; 24x17 cm.

ISBN 978-950-893-735-3

1. Sístema Judicial. 2. Enseñanza Superior. I. Título
CDD 347.014

Tucumán 1471 (C1050AACC) Buenos Aires
Queda hecho el depósito que previene la ley 11.723
Impreso en la Argentina

Printed in Argentina

Tirada: 300 ejemplares
I.S.B.N. 978-950-893-735-3

MAESTRIA EN DERECHO Y MAGISTRATURA JUDICIAL

Ernesto N. Kozameh

Director: Dra. Silvana Stagna

Comunicación Interjurisdiccional Electrónica

Junio de 2010

ACLARACION A ESTA EDICION

Al momento de esta edición, el anteproyecto elaborado en este trabajo fue receptado por la Comisión de Justicia de la H. Cámara de Diputados de la Nación, y presentado a tratamiento del Congreso, tramitándose su consideración en las respectivas comisiones. Se incluyen dichas gestiones.

A Leni, mi esposa, por su comprensión
A mis hijos Nicolás y María del Huerto,
a los que se sumó Andrés
A mis nietos Tomás y María Florencia.
Con la esperanza que vivan en un mundo con Justicia

Mi reconocimiento y gratitud a los
Dres. Rodolfo Vigo, Silvana Stanga
y Jorge W. Peyrano

PROLOGO

Decía, con razón Chesterton que un optimista es "un pesimista bien informado". Es que, en verdad, la información nos cambia. Y cuánto! Emilio Lamo de Espinosa —autor español de "La sociedad reflexiva"-es ilustrativo sobre el punto: "Una vez se señaló que los virus no leen libros de biología ni las plantas leen libros de botánica, pero la gente sí lee libros de ciencias políticas, de sociología o de economía. El resultado es que eso tiende a producir un reflejo mutuo, una transformación, de tal modo que con frecuencia los modelos, que son modelos teóricos, acaban transformándose en la mente de los actores, no ya de los científicos, sociales, en estrategias de acción, con la consiguiente modificación de los cursos de conductas. El ejemplo más claro es aquel de la persona que conoce psicoanálisis, que no se comporta del mismo modo que la que ignora esta disciplina. Una persona o una organización política que tiene, aunque sea un conocimiento superficial, de la obra y de los modelos de Marx, es evidente que no se conduce en política del mismo modo que si la ignorara. El resultado es que hay lo que denomino un proceso de reflexividad, en el sentido de que hay una incidencia de los modelos sobre la propia realidad" Precisamente, nuestro autor, el Dr. Ernesto Kozameh, pretende informarnos —y lo consigue— de múltiples asuntos relacionados con el aporte de las nuevas tecnologías digitales, cuya aceptación mucho y bueno podría proporcionar en pro de la mejoría de los sistemas judiciales argentinos. Así, su pluma ágil hace desfilar *conceptos (*vgr, diferenciando lo que es firma electrónica de lo que es firma digital, exponiendo los lineamientos de la criptografía asimétrica y su importancia para la firma digital, etc.), *cronologías* (informando respecto de que la primera ley de firma digital data de 1995 y fue dictada en UTAH-EEUU y acerca de cuál ha sido la evolución normativa argentina en la materia) *exégesis* (concretando la correspondiente a la ley 25.506, de firma digital en Argentina) y *grandes nombres en la materia* (destacando el papel que corresponde reconocer en el tema a la labor desarrollada, desde 2001, por la Junta Federal de Cortes y Superiores Tribunales Provinciales, en su porfiada tarea de abrir las ventanas de los sistemas judiciales argentinos a la incorporación de las ventajas de la tecnología informática).

Claro está que Kozameh no nos ha informado gratuitamente. Lo ha hecho, seguramente, en pos de materializar, por un lado *deseos* (v.gr., la "despapelización" para dar finiquito al estado de cosas medioeval que prevalece en la gran mayoría de los estrados judiciales argentinos que siguen construyendo los expedientes con papel, aguja e hilo; y por el otro propuestas concretas (cual es el caso del encomiable proyecto que pergeña tendiente a modificar

la añosa ley 22.172 de comunicación entre tribunales emplazados en jurisdicciones territoriales diferentes; proyecto que sin tapujos aprovecha las excelencias ofrecidas por la tecnología informática con inclusión del uso de la firma digital). Debemos, además, poner de resalto que toda la obra trasunta un sentimiento que compartimos: los problemas que sufren los Poderes Judiciales argentinos no obedecen exclusivamente a la carencia de recursos de que soportan, porque también, y mucho, contribuye la falta de decisión para aprovechar debidamente los pocos con los que cuentan. Vaya un ejemplo: la regulación y aceptación de las notificaciones judiciales digitales (sobre lo que insiste Kozameh, en varios tramos del libro) se encuentra hoy al alcance de la mano, sin que ello represente mayores costos ni presuponga actitudes heroicas. Sin embargo, la inercia sigue triunfando. Por fortuna y en momentos en que estamos redactando estas líneas, ha llegado a nuestra mesa de trabajo la normativa mediante la cual, en fecha muy reciente, Mendoza —merced a modificaciones introducidas por los artículos 21 y 70 bis de su Código Procesal Civil— ha incorporado el domicilio electrónico y las notificaciones electrónicas, con firma digital.

Que, entonces, nuestro autor se sienta acompañado. No está solo. Constituimos legión los que soñamos con un Servicio de Justicia más eficiente, y para que ello ocurra debemos mirar no sólo al futuro sino igualmente al presente, que también nos ofrece posibilidades de optimizar lo que tenemos.

Rosario, 16 de julio de 2008.

JORGE W. PEYRANO

INDICE GENERAL

TERCERA PARTE

LEY DE COMUNICACION INTERJURISDICCIONAL ELECTRONICA

ANEXOS

INTRODUCCION

Hacia el año 2000 ya se había instalado en el seno de la Justicia Argentina, una genuina vocación de cambio, plasmada, por un lado, en la creación de la Junta Federal de Cortes y Superiores Tribunales de la República Argentina, y bajo su impulso, la formación en las provincias de centros de capacitación y la admisión e instrumentación de los recursos que la evolución tecnológica ofrecía, en especial la informática.

Un numeroso grupo de hombres y mujeres integrados a la Justicia, desde distintos roles, teníamos el sueño de verla remozada y dinámica, respondiendo efectiva y eficazmente, cada vez que se acudiera a ella. Evito las citas individuales, a fin de no cometer la torpeza involuntaria de alguna omisión, lo cual sin duda atormentaría mi conciencia, máxime, en esta etapa de la vida en que se saborean los recuerdos con nostalgia y afecto.

Fuimos muchos los que soñamos, algunos muy dentro del servicio de Justicia, y otros a la par, codo a codo, casi con igual pertenencia, y sin duda equiparable legitimidad.: Instituciones abogadiles, ONG, y hasta el propio Gobierno con las estructuras del Ministerio de Justicia de la Nación.

En aquellas ráfagas del viento loco de los sueños, se aglutinó el gobierno de las justicias provinciales y nació la Junta Federal de Cortes y Superiores Tribunales de Justicia de las Provincias de la República Argentina, como pasaron a denominarse los sueños.

Desde su seno se derramaron, generosos, los trazos que ayudaran a que cada justicia provincial tenga su centro de capacitación. Hoy, lucen vigorosos, como la Junta misma, sólidamente legitimada por la inclusión de todas las Provincias. En paralelo un grupo de visionarios advirtieron la necesidad de profundizar más allá del grado universitario, la específica cuestión judicial de un modo integral, y surgió la Maestría en Derecho y Magistratura Judicial de la Universidad Austral, que en forma individual fue sembrando la capacitación y el despertar a ideas innovadoras en muchas de las Justicias Provinciales.

Entre aquellos sueños estaba el dotar de agilidad a la Justicia, para que su ritmo fuera acompasado al que le reclama la sociedad a la que sirve. Soñamos con bocanadas de aire fresco, con jueces con un perfil renovado, que junto a la capacitación que comenzaba a fluir, tuvieran a su alcance los recursos tecnológicos idóneos.

En Junio de 1999, convocada por la Junta Federal, se llevó a cabo en Termas de Río Hondo, la Primera Reunión Informática de Ministros de Cortes y Superiores Tribunales de Justicia, y en paralelo, el primer Foro de sus Técnicos Informáticos, con el objetivo de abrazar la Justicia a la innovación tecnológica, y coordinar la incorporación de la informática en su seno.

Esta primera reunión sirvió de base a una segunda reunión de Técnicos celebrada en Santiago del Estero, y ambas viabilizaron el arribo al Convenio de Comunicaciones Interjurisdiccionales Electrónicas celebrado en la sede del Ministerio de Justicia de la Nación en septiembre de 2001.

Abrigábamos el sueño de habilitar la comunicación electrónica entre los jueces argentinos.

Después de ello, la crisis política, económica e institucional que se desatara en nuestra Nación, hizo añicos nuestros anhelos, y afectó de manera sensible, y en algunos aspectos hasta paralizante, aquel incipiente y entusiasta proceso, que debía concluir con el cumplimiento del Convenio y el proyecto de ley que contemplara ampliar los efectos del mismo a aquellas materias que requerían jerarquía de ley procesal.

Hoy más que ayer, la Justicia Argentina se encuentra dotada de los elementos técnicos necesarios para obviar el lento sistema de comunicación entre sus jueces que se cumple actualmente en soporte papel y con apego a la ley 22.172.

Es más, después de la edición anterior, la incorporación de tecnología e informática a la Justicia ha crecido exponencialmente, en tal grado, que en la presente pueden aparecer omitidos algunos logros y avances de las justicias provinciales. Situación que lejos de menguar la viabilidad del proyecto, evidencia la conveniencia y oportunidad de su sanción.

Es sobreabundante resaltar el flagelo de la mora en el sistema judicial argentino. El actual procedimiento de comunicaciones entre jueces, es una de las razones dilatorias del proceso. Cada vez que, durante el desarrollo de un proceso, el Juez debe recurrir a su uso, aquél es víctima de una demora excesiva, casi nunca proporcional a la diligencia, y ésta muchas veces infructuosa.

Todo ese laberinto puede ser sustituido con la inmediatez instantánea del uso de la informática, la red que nos vincula, y la seguridad derivada del cumplimiento de los recaudos que la ley ya ha previsto.

Casi tan simple como trasladar al seno de la Justicia, la celeridad en las comunicaciones a las que nos hemos habituado en nuestra vida privada, y por imperio de una ley, que se proyecta en este trabajo, insertar ese aporte tecnológico en el proceso.

Con la norma diseñada se revitaliza, así, aquel sueño, nacido en el interior de nuestra Patria, como símbolo del federalismo que campea en su finalidad y destino.

Trabajo y proyecto que me toca modestamente instrumentar, pero cuya génesis y embrión, debe buscarse sin duda en esa labor reseñada de la Junta Federal de Cortes y Superiores Tribunales Justicia de la República Argentina y de la Maestría en Derecho y Magistratura d e la Universidad Austral en cuyo seno se plasma.

No dudo que quienes hoy ejercen la magistratura, sus órganos de gobierno, y en general quienes abrazan la Justicia, sueñan hoy, como soñamos ayer. Por ello, y para ellos, este trabajo, anhelando humildemente, les sea útil, en su tarea de intentar llevar a cabo esa noble misión.

PRIMERA PARTE

HACIA UNA VISION REVISADA DEL PROCESO

I. Marco propicio para la transformación esbozada

I.1. Nuevas herramientas en el proceso y los protagonistas del cambio

Las consideraciones generales sobre la Justicia, y especiales del ámbito procesal, que acá se vierten, pueden parecer ajenas a la temática central de este trabajo. No se asombre el lector; más adelante se centra el análisis en punto a la informática en la Justicia. Pero considero conveniente, previo a ello, una breve referencia al marco propicio en el seno de la Justicia, a los fines de acoger los cambios que implican el uso de las nuevas tecnologías.

Tengo asumido que una de las cuestiones centrales del achaque a la Justicia, es su falta de agilidad y dinamismo, y en ese contexto, y dado que el tema de este trabajo, aborda esa misma preocupación, pueden resultar convenientes algunas reflexiones sintéticas a los protagonistas, destinatarios o usuarios de la herramienta propuesta, como asimismo una rápida mención, de algunas herramientas procesales, instaladas desde hace tiempo en la doctrina, y en algunos casos hasta receptadas jurisprudencial y o legislativamente, y lamentablemente de escaso uso, pese a la celeridad que podrían aportar.

En otras palabras su breve enunciado no hace sino aludir a la necesidad de disminuir la resistencia al cambio por parte de los protagonistas.

Las estadísticas insisten en que son dos las causas más notorias que vician al proceso, con el consecuente descrédito en la Justicia:

En primer lugar, la morosidad

En segundo lugar, la preeminencia de la verdad formal en desmedro de la verdad real.

Ambos escollos se presentan como el vallado que divorcia el servicio de Justicia, del ciudadano que debe acudir a ella, o que de ella espera

Ello genera un abismo entre el juez y el ciudadano, minimizando la autoridad de aquel y obviamente, perturbando su tarea.

A poco de esbozar el inicio del tema, se advierte que sobre él cabalga necesariamente la definición del perfil del juez.

En efecto, si este habrá de permanecer en su rol de buchón de la ley, ungido jefe burócrata de un organismo del Estado y en el apego irrestricto a las formas; sin duda no gozará de la flexibilidad y permeabilidad que le permitan receptar las innovaciones que en los tiempos que corren se le ofrecen y que son sin duda convenientes para menguar la distancia existente entre la sociedad y su Justicia.

Por tanto el eventual rol benéfico de los instrumentos que se proponen, presupone la existencia de un juez con un perfil decididamente activo que se niega a ser un mero convidado de piedra.

Queda claro que es muy difícil, sino imposible, lograr la transformación buscada, sin que la cabeza y timón del proceso, el juez, haya asumido la voluntad de cambiar y corregir el déficit judicial.

Mucho se ha escrito al respecto, y, simple y sintéticamente, en respeto a los límites de estas consideraciones introductorias, he de reiterar, que la mejora supone indudablemente la presencia de un juez pro-activo, que dirige su tribunal y los juicios a su cargo desterrando el perfil burócrata habitualmente ligado a una escasa incidencia en el proceso. Sin duda las mejoras en la justicia, vendrán de la mano de un juez protagonista en el juicio que dirige, permeable y flexible a los cambios benéficos, creativo, imaginativo e innovador.

Pese a su importancia, no he de poner el acento en este punto, sobre el que otros, y de mejor modo, ya se han explayado. Me consta que hay muchísimos jueces que han asumido ese nuevo perfil y dirigen tribunales y procesos a su cargo, aplicando todas las exigencias que se auto-impusieran mediante la capacitación que han logrado.

Del mismo modo, es también fundamental el equivalente y proporcional cambio, en el otro protagonista del proceso: el abogado.

La mayoría de las instituciones que les aglutina, muy meritorias casi todas ellas, hacen enormes esfuerzos en capacitar a sus colegiados, pero, es tal vez hora de acentuar una nueva orientación dirigida a un cambio en el perfil del abogado, como se ha hecho desde el ámbito de la justicia, con relación a los jueces.

Es indudable su protagonismo y por tanto destaco la necesidad de inyectar en este ámbito del foro, una tarea formativa que tienda a definir en los abogados un perfil que acompañe la tarea de ese juez que pueda haber evolucionado en el rumbo diseñado.

Lamentablemente es frecuente observar dilaciones procesales que en muchos casos no son atribuibles a la burocracia judicial, sino que reconocen su origen en la inconducta profesional. Agazapados, en supuestos actos de defensa, los hay, y muchos, que buscan el beneficio de demorar, sino evitar, el cumplimiento de una obligación.

No ha de pretenderse restricciones al ejercicio de la defensa. Sin duda antes que ello habrá de soportarse la mora.

Pero tampoco hay duda que desde hace años y bajo el manto protector del resguardo del derecho de defensa, se ha tejido una maraña inextricable, impenetrable, aún, cuando se suponga el ejercicio, por parte del juez, de todas las herramientas correctoras a su alcance.

Estas facultades del juez de evitar las conductas abusivas de las partes no sólo desde el texto de las normas procesales, sino desde el espíritu de ellas y desde los principios procesales, además de insistirse en la capacitación judicial, deben ser tópicos profundamente instalados en el ámbito abogadil, como reverso de ese nuevo perfil de abogado que debe cincelarse para lograr un acompañamiento de este protagonista.

He señalado un déficit frecuente por acción desde la función que desempeñan, y que estimo imprescindible corregir.

Pero advierto que lo hay también por omisión.

Peyrano ha llamado la atención, más de una vez, de la escasa recurrencia de los letrados a las acciones ofrecidas en leyes como las de defensa del consumidor y de protección al ambiente.

Su vastedad, riqueza y celeridad, permitirían sin duda la pronta solución de muchos conflictos de ciudadanos que luego alzan sus demandas en contra de las demoras judiciales, con reproches incluso a sus propios abogados.

Creo que el déficit, reitero, tanto por acción como por omisión, en el análisis del rol de éste protagonista, demanda una intensa tarea formativa con destino a delinear ese nuevo perfil de abogado conviviente con una nueva mentalidad dinámica de asumir el proceso, capaz de entender y hablar el mismo idioma del juez que se esfuerza en definir y ejercer su nuevo perfil.

El excesivo apego a las garantías procesales, nos llevó a rechazar una prudente flexibilidad en la tolerancia, por ejemplo, de la conveniente corrección de los dispositivos de una sentencia con manifiesta irritación al derecho, más allá de las rectificaciones de errores materiales, siempre que se den determinadas condiciones. Me refiero a la *revocatoria in extremis.* Desde otro ángulo se ha advertido, sin que tampoco afecte garantía alguna, que el anticipo del reconocimiento y protección de un derecho verosímil, lejos de irritar el orden jurídico, evita el pernicioso efecto de la demora. Aludo a *la sentencia anticipada*.

Es que aquella flexibilidad apuntada, parece ganar terreno en el campo de la doctrina y jurisprudencia en desmedro de una rigidez que había anquilosado el proceso.

En tanto en la primera se registran límites al efecto de cosa juzgada, y la posibilidad de revisión, ante las írritas consecuencias del fallo firme, la segunda habilita un adelantamiento tutelar por parte del tribunal, anticipadamente a la

tramitación del proceso, logrando una agilidad en la protección de derechos por los que se acude a los estrados judiciales.

No debe olvidarse en ese contexto la *reconducción de las postulaciones*, que posibilita al Juez el arribo a la solución justa que barrunta, evitando que la rigidez del proceso lo limite o a veces impide.

Todos estas, y muchas otras que no se citan en homenaje a la brevedad, pero de similar valía son instrumentos procesales que requieren, para su ejercicio, protagonistas con ese nuevo perfil antes descripto, aludiendo a ello, sólo como una breve referencia atento constituir, el entorno, en el que se propicia implantar el proyecto.

En sintonía con un nuevo perfil de Juez, acompañado de abogados, receptivos ambos de ese nuevo marco, la tecnología debe ir incorporándose en la vida forense. Con esfuerzo, desvaneciendo las resistencias que se le oponían, lo ha venido haciendo.

En este orden y evolución quedaron pendientes e inconclusas algunas tareas; entre ellas habilitar de modo definitivo, formal y procesalmente la comunicación electrónica entre los jueces de Argentina, mediante el uso de la firma digital. Esta cuestión es la que abordo.

I.2. Las comunicaciones interjurisdiccionales por medios electrónicos

La temática se nutre de una vertiente legal y otra tecnológica y constituye el objeto central de este trabajo.

Las comunicaciones entre jueces de distintas jurisdicciones encuentran, hoy en nuestra Argentina, su normativa específica en la ley 22.172, la que determina de modo explícito los requisitos que debe reunir el oficio que contiene la orden del juez de extraña jurisdicción que pretende su cumplimiento allende su territorio.

La ley 22.172 es, en rigor, una norma nacional que aprobara el convenio oportunamente suscripto entre la Nación y las distintas provincias que fueron adhiriendo sucesivamente al mismo.

El tema que nos ocupa es, en definitiva, la inserción, en el mencionado contexto, del uso de la firma digital que posibilite la comunicación electrónica entre los jueces de distinta jurisdicción.

Con la sanción de la ley 25.506 se asimila a la firma digital a la firma reglada por el Código Civil, empero, para que ella pueda cumplir con su función propia, es menester contar con una autoridad certificante.

Habiendo llegado a este punto resulta conveniente detenernos a repasar brevemente el funcionamiento de este mecanismo que constituye la base de nuestro análisis.

La firma digital es un sistema de códigos alfanuméricos encriptados, al que sólo tiene acceso el titular de la firma, y que, a la vez, se encuentra reservado en una autoridad certificante, que no es sino una entidad confiable y seria que, con tecnología informática suficiente, y prácticamente en forma simultánea al tiempo en que el titular de la firma digital emite un documento firmado, autentica ante el tercero destinatario la correspondencia de la misma a quien se atribuye la calidad de firmante del documento.

Por ser un tema profusamente estudiado y agotado, no me detendré a señalar las dificultades y demoras que enfrenta un proceso, y en consecuencia, las partes, sus abogados y el tribunal, cada vez que debe diligenciarse una medida en extraña jurisdicción. En la mayoría de los casos los plazos se cuentan en meses, y en muchas oportunidades deben ser reiteradas, porque si en casa ocurren extravíos; en la distancia son más que frecuentes. Sin duda este tema constituye uno de los elementos centrales a la hora de generar morosidad.

Los poderes judiciales argentinos se han dotado en los últimos años de herramientas informáticas suficientes, llegando algunos de ellos al desarrollo de planes informáticos y redes de elevado nivel técnico.

Hoy todos ellos cuentan con tecnología suficiente y recursos humanos capacitados para asimilar la propuesta que se formula.

Como se esbozó en la Introducción, el seis de septiembre del año 2001 se celebró el Convenio de Comunicación Electrónica Interjurisdiccional entre todos los poderes judiciales de los estados provinciales argentinos. El mismo fue corolario de dos reuniones previas llevadas a cabo, la primera, en Termas de Río Hondo, provincia de Santiago del Estero, y, la segunda, en la capital de este estado provincial. Estas reuniones previas nuclearon en forma simultánea a los Ministros representantes de cada una de las Cortes provinciales, por un lado, y, por otro lado, a los técnicos informáticos de cada una de ellas, constituyéndose el Foro permanente de estos últimos.

Reza el artículo (en adelante art.) 4 del citado Convenio (06-09-2001): "Las partes suscriben el presente convenio con el propósito de complementar lo dispuesto por la ley 22.172 y de incorporar progresivamente el uso de las nuevas tecnologías en las comunicaciones interjurisdiccionales"; y el art. 5 dice: "La comunicación directa entre organismos judiciales y Ministerios Públicos de distinta jurisdicción territorial podrá realizarse a través de correo electrónico..."

Se dejaba pendiente y a cargo de las respectivas autoridades de cada poder judicial la tarea de certificar la firma digital.

En aquella oportunidad de la firma del convenio, campeaba la idea de la existencia de una limitación, al propósito de regular íntegramente el tema mediante un convenio. Por ello se inserta el concepto de "complemento" a la ley 22.172. En tal sentido y como se expone mas abajo creo que es conveniente el agregado de uno o más artículos a la ley 22172, que modificándola,

en definitiva, habilite de modo expreso la comunicación electrónica entre los jueces de distinta jurisdicción.

Cuando ya parecía plasmarse esa realidad, contenida en el convenio, y que sin duda hubiera impulsado la pertinente adecuación legislativa, sobrevino la crisis que enturbió a la sociedad toda, su dirigencia, su economía, y lo que es más grave su tejido social. Pero desde aquel 2001 han transcurrido muchos años, sin que se haya puesto en marcha esta herramienta de tanta utilidad a la hora de buscar modernizar la Justicia y, en especial, de abreviar sus tiempos.

En tal sentido, debo destacar que la Junta Federal de Cortes y Superiores Tribunales de Justicia de las Provincias Argentinas, solicitó formalmente al organismo competente, por intermedio del Ministerio de Justicia, el otorgamiento a dicha Junta de la calidad de autoridad certificante. Creo que a efectos de la aplicación de la comunicación electrónica por uso de la firma digital (tarea de certificación) en el marco de una modificación de la ley 22.172 es quien representa a las justicias provinciales y la institución adecuada para llevar a cabo dicha tarea, con la responsabilidad que el caso requiere, en conjunto con quienes representan las otras esferas judiciales argentinas, la Corte, como cabeza de la nacional y federal y el Ministerio Público.

Como conclusión y, a la vez síntesis, de este Capítulo primero, y en atención a los tópicos propuestos deseo remarcar las siguientes cuestiones:

En primer lugar, estimo que en el ámbito del Poder Judicial se abrió en los últimos tiempos un espacio importante en beneficio de la capacitación de sus jueces, y, en ese ámbito se ha definido un nuevo perfil de juez, que, al menos como paradigma, está presente en la mayoría o muchos de los magistrados.

También es importante la tarea que al efecto han llevado a cabo las instituciones abogadiles, pero que estimamos, debe intensificarse, y acentuarse en la orientación sugerida, no sólo por el rol del abogado en el proceso, sino por constituir el universo nutriente de la magistratura, y en tal sentido sería útil una labor de impregnación de idearios comunes con los Centros o Escuelas de Capacitación con los que cuentan los poderes judiciales.

En segundo lugar, destaco que en la actualidad se han desarrollado pretorianamente una serie de herramientas procesales que propenden a imprimirle al proceso mayor eficiencia, eficacia y celeridad.

En respeto a la brevedad con la que debo referirme al tópico precedente— simplemente como marco, por no ser el eje central— invito al repaso de la rica y vasta creatividad de Jorge Peyrano, quien ahonda en el tema específico. Y, en efecto, pone el énfasis en aquellos remedios que, despejando algunas formas, y a veces desmitificando algunos supuestos dogmas procesales incomprensibles para el hombre común, permiten reducir los plazos o acceder a una tutela efectiva, preventiva y lograda en tiempo.

Por último y en lo que sí habrá de constituir la temática del ulterior desarrollo, destaco la labor llevada a cabo por los poderes judiciales provinciales, y la Junta que los nuclea, con grandes esfuerzos presupuestarios, en beneficio de la informática, como herramienta destinada a lograr la agilidad que su dinámica permite. Debo destacar que con su actual integración la Corte ha puesto especial interés en receptar e implementar los recursos tecnológicos, y en especial informáticos.

El abismo entre sociedad y Justicia es un llamado permanente a quienes de algún modo y desde algún sector estamos involucrados. Allí están las herramientas. Su uso o habilitación para su operatividad, depende de nuestro esfuerzo en tender ese puente para desterrar aquel abismo, y comenzar a regirnos por tiempos y modos, que la comunidad, en muchos casos, demanda con razón.

Peyrano tiene la grata y delicada costumbre de concluir sus exposiciones con alguna cita literaria, por lo general, poemas de buen gusto y factura relacionados de algún modo con el tema. Con humildad permítaseme, antes de desarrollar el tema central y cerrando este capítulo introductorio, imitar su gesto, parafraseando a Hemingway: *"...No preguntes por quien doblan las campanas... doblan por ti"*.

SEGUNDA PARTE

DOCUMENTO ELECTRONICO Y FIRMA DIGITAL

I. Documento

I.1. Introducción

Estructuralmente, el documento es una cosa corporal que nos muestra algo, está constituido por un elemento material y un elemento intelectual. Carnelutti, dice que es una cosa que sirve para representar a otra. (1) Se hace énfasis entonces en el aspecto probatorio del documento. Una definición de documento escrito dice que es una "expresión en soporte escrito de un acto o hecho con repercusión jurídica, a la cual el derecho confiere valor probatorio. Así, la prueba documental o prueba de documentos es la constituida por material documental, bien de naturaleza pública o bien de carácter privado".

Podemos decir que un documento tiene las siguientes características:

a. ocupa un lugar en el espacio;

b. se ubica en un tiempo específico;

c. tiene relación entre el autor y lo querido y expresado por éste, y;

d. un valor probatorio, propio del documento jurídico.

La escritura sobre papel, tiene varias cualidades que durante mucho tiempo la tornaron irremplazable: durabilidad, inalterabilidad, legibilidad y debidamente individualizada y firmada posee, además confiabilidad. (2)

Cuando se habla de documento electrónico se habla de un documento que ha sido generado por el hombre y se almacena o reproduce por intermedio del ordenador o que el propio computador genere el contenido del documento a partir de alguna combinación de la información disponible con ciertas instrucciones que operan en su sistema.

---

(1) CARNELUTTI, F., Sistema de Derecho Procesal Civil, Tomo II, pág. 414, Bs. As, Ed. Depalma, 1994.

(2) GUIBOURG, R., Manual de Informática Jurídica, pág. 235 y ss, Bs. As., Editorial Astrea, 1996.

Por tanto, las características del documento electrónico son las siguientes:

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

b) sólo puede hacerse público mediante tecnología informática;

c) es inmaterial;

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

I.2. Documento escrito y documento electrónico.

Los autores se encuentran divididos en sus opiniones respecto a los mismos.

Algunos entienden que los registros informáticos no constituyen un documento escrito basándose en sus diferencias.

Otros, encuentran muchas similitudes y opinan que el documento electrónico es otra forma de escribir. Creo que ambos tienen razón, existen diferencias, pero también existen aspectos en que ambos se parecen.

Las diferencias entre ambos podemos decir que son las siguientes:

a. Básicamente, ambos se diferencian desde el punto de vista estructural. Un documento escrito no puede concebirse sin el soporte material que es el papel, su corporeidad.

Al respecto dice Bill Gates: "Durante más de 500 años, todo el volumen del conocimiento y de la información humanos se ha almacenado en forma de documentos de papel. (...) el papel estará siempre con nosotros, pero su importancia como medio de buscar, preservar y distribuir información está disminuyendo ya". (3)

En el documento electrónico se transforma su corporalidad, sus elementos materiales cambian, de tal manera, que su soporte será un sistema de conformación electrónica, expresado a través de un lenguaje binario. (4)

b. El registro informático puede ser fácilmente modificado, mientras que el documento escrito resulta más difícil de modificar. Con la aclaración que el registro informático, anotará la huella de su alteración.

c. La firma ológrafa es típica del documento escrito. La firma electrónica y digital son típicas del documento electrónico.

---

(3) GATES, B., Camino al Futuro, Madrid, Editorial Mac Graw-Hill España, 1996.

(4) GAETE GONZALEZ, E. A., Instrumento público electrónico, pág. 177, Madrid, Ed. Bosch, 2000.

d. En el documento informático desaparece la diferencia entre la copia y el original.

Cuando una persona firma un documento en papel está manifestando su voluntad y lo que hace es dibujar sobre él una serie de símbolos que lo identifican.

Pablo Palazzi define la firma como "el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad". (5)

"Si se encuentra un medio que reemplace a la firma ológrafa en ambientes digitales, éste nuevo medio deberá cumplir con las funciones tradicionales de la firma. Estas son:

a) indicativa: informa acerca de la identidad de un autor;

b) declarativa: se refiere al acuerdo respecto al contenido del acto;

c) probatoria: permite vincular al autor con el signatario." (6)

Reconociendo la fuente de Freitas (Código Civil, Esboço, art. 740) el art. 1012 del Código Civil, en adelante, expresa que "la firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por iniciales de los nombres o apellidos".

Se entiende por firma el trazo escrito de una manera particular, mediante el cual una persona rubrica sus instrumentos en forma habitual. (7)

En la nota al art. 3639, dice Velez Sarsfield "la firma no es la simple escritura que una persona hace de nombre o apellido: es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad".

En principio este trazo escrito debe corresponder al nombre y apellido del firmante, no siendo relevante que el mismo sea legible o no. Lo que es fundamental es el carácter de habitualidad, es decir que el trazo sea siempre el mismo, sin perjuicio de las alteraciones de detalle que pudieran producirse con el tiempo.

En tal sentido dice López Olacirregui que "la firma es firma aunque sea ilegible y no es firma aunque sea legible si no corresponde a la habitual forma de suscribir los actos el sujeto jurídico que la estampó". (8)

---

(5) PALAZZI, P. A., "Firma digital y Comercio Electrónico", VI Congreso Iberoamericano de Derecho Informático, Montevideo, 1998.

(6) ibídem.

(7) LLAMBIAS, J., Tratado de derecho civil, Parte General, 4ª edición, Tomo II, pág. 404, nº 1585, a, Bs. As., 1970.

(8) SALVAT — LOPEZ OLACIRREGUI, Tratado de Derecho Civil Argentino, Parte General, Tomo II, pág. 449, Bs. As., 1964.

La regla general es de libertad en la expresión gráfica, puede contener sólo su apellido, sus iniciales, o ser ilegible, pero lo importante es que contiene los trazos particulares del individuo, y su habitualidad en el uso, que además de individualizar a quien interviene, su firma inserta en un documento implica la conformidad del firmante con su contenido. (9) Por ello el art. 1028 C.C. establece que el reconocimiento de la firma implica el del texto suscripto con ella. (10)

Lo que la ley ha previsto es una suerte de inescindibilidad entre el reconocimiento de la firma y el reconocimiento del cuerpo del instrumento y por ello se ha resuelto, como principio general, que la exigencia de la firma como condición esencial del instrumento privado constituye una garantía para los particulares, consistente en que nadie puede juzgar instrumentos en su contra sin la intervención del propio interesado. (11)

Ver cuadro comparativo en Anexo VII

II. La firma digital

II.1. Introducción

Un breve repaso de algunas de las diferentes técnicas utilizadas para firmar electrónicamente un documento:

a. Una metodología es el uso de una tableta sensible y un lápiz magnético conectados a un PC donde se registra la presión, velocidad y coordenadas donde el operador apoya el lápiz. Esos datos se combinan matemáticamente para formar la "firma electrónica" de la persona. Posteriormente, se puede comparar esa firma almacenada con otra para verificar si pertenecen a la misma persona. (12)

b. Emisión de calor: se mide la emisión de calor de un cuerpo, termograma, realizando un mapa que individualiza a cada persona.

c. Otra técnica de firma electrónica puede ser el registro de la huella digital y de ciertos caracteres de la piel que identifican a la persona. En un tablero donde la persona coloca su dedo.

d. Allí se digitalizan la huella y los parámetros biológicos del dedo de la persona, de tal forma que es imposible reproducirlos salvo que se obligue a la persona a colocar su dedo en el dispositivo. (13)

---

(9) ídem, pág. 451.
(10) ídem, pág. 455.
(11) CNCiv., 5/3/81, ED, 93-580.
(12) BALAY, G., "Enfoque informático del Decreto 65/998", Presidencia de la Nación, Oficina Nacional del Servicio Civil, 1998.
(13) ibídem.

e. Verificación de la voz: la dicción de una, o más frases, es grabada y en el acceso se compara la voz, entonación, agudeza, etc. Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, envejecimiento, etc. (14)

f. Verificación de patrones oculares: Estos modelos pueden ser basados en patrones de verificación observando el cuerpo por el iris o d la retina. Se los considera entre de los de mayor efectividad, dado que la probabilidad de coincidencia es casi nula.

g. He dejado para el final la mención de los sistemas criptográficos que, por configurar su aplicación la base del mecanismo de la firma digital, y ser una cuestión eminentemente técnica se desarrolla en extenso en anexos respetando y reproduciendo, como allí se indica, la terminología y conceptos de sus fuentes.

La eficacia probatoria de los elementos informáticos reconoce dos pilares procesales en que se asienta: por un lado, consta en la facultad de ofrecer y producir pruebas en contrario; y, por otro, reside en el prudente ejercicio de la sana crítica judicial para apreciar la fuerza de convicción de las pruebas informáticas en los litigios, observando las reglas sobre inalterabilidad de los soportes utilizados y los métodos sustitutivos de la firma que concurren a individualizar a los sujetos procesadores de datos y asegurar la autenticidad. (15)

Es conveniente analizar los conceptos de autenticidad, integridad, exclusividad y no repudio. (16) Además de la inalterabilidad y perdurabilidad de la información y de cómo éstos se relacionan con el concepto de la firma digital.

a) Autenticidad. Se refiere a la autenticidad del origen del mensaje. Este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo nadie suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación. (17) El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.

b) Integridad. Esto significa que la información no carece de ninguna de sus partes, que no ha sido modificada. La integridad es una cualidad imprescindible para otorgarle validez jurídica a la

---

(14) ibídem.

(15) GUASTAVINO, E. P., "La prueba informática"; L.L., año 1987 "A", págs. 1144 y ss.

(16) DEVOTO, M., "Claves para el éxito de una infraestructura de firma digital", L.L., año LXIV, Nº 39, 2001.

(17) MAC: Message Autentication Code.

información. Hace referencia a la integridad de la información es decir, la integridad del documento, es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

c) Exclusividad. Es decir que se encuentre bajo el exclusivo y absoluto control del firmante. Esto se relaciona con la voluntad de éste, es decir, que pueda realizarla con intención, discernimiento y voluntad, y que ésta, no se encuentre adulterada por ningún vicio.

d) No repudio: Esto es, que sea susceptible de verificación mediante un perito informático. En caso de duda y petición de algunas de las partes puede intervenir un profesional para confirmar la validez o no de la firma.

e) Inalterabilidad: La inalterabilidad no se refiere a la información en sí, sino a su medio de almacenamiento. La firma digital no impide que la información se altere, sino que detecta si ésta ha sido alterada.

f) Perdurabilidad. Significa que la información perdura en el tiempo y es una cualidad del medio de almacenamiento.

II.2. Firma electrónica y firma digital

A pesar que comúnmente se usan como conceptos sinónimos, técnicamente puede distinguirse entre la firma electrónica y la firma digital.

La primera es aquella que identifica a una persona con una clave o un password y le permite desde ingresar a una computadora o a un programa de software hasta acceder a un correo electrónico o a una página web.

En cambio en la firma digital, emisor y receptor crean cada uno su propia clave privada, que solo ellos conocen y guardan, a la vez que registran ante la autoridad certificante cada uno su clave pública. El receptor, al recibir el mensaje, identifica ante la autoridad certificante la clave pública del emisor mediante su clave privada.

La identidad de los interlocutores y la inalterabilidad del mensaje se asegura al ser éste encriptado en esa clave pública, mediante la clave privada que sólo el emisor posee, y, que es desencriptado por el receptor con su clave privada, también de su exclusivo conocimiento, asegurándose así la identidad de los interlocutores y la inalterabilidad del mensaje.

La correspondencia de la clave pública, tanto con la persona del emisor como con la del receptor es asegurada y garantizada por la autoridad certificante.

Ver cuadro comparativo en Anexo VIII

III. El camino recorrido hacia la Ley Argentina de Firma Digital

III.1. La situación a nivel internacional

Para comenzar haremos un breve desarrollo de cómo fue evolucionando la firma digital a nivel mundial; así podemos mencionar que en la actualidad existe consenso y acuerdo globalizado en que la firma digital basada en la criptografía de clave pública es un medio de autenticación a distancia que provee seguridad y desarrolla la confianza.

Entre los principales antecedentes, rescatamos los siguientes: en 1995, en Utah, Estados Unidos, se dicta la Utah Digital Signatures Act. Esta ley fue la primera en el mundo que sistematizó y le confirió validez jurídica a un mecanismo de autenticación como es la firma digital. Los objetivos de esta normativa fueron: a) facilitar las transacciones electrónicas comerciales a través de medios digitales más seguros y eficientes, b) reducir la incidencia de firmas digitales falsificadas y fraudes en el comercio electrónico, c) implementar en forma legal un estándar relevante de telecomunicaciones, d) establecer, en coordinación con múltiples estados, reglas uniformes relativas a la autenticación y validación de mensajes electrónicos y e) propiciar la implementación de la tecnología para reducir el uso del papel en el ámbito judicial. La ley establece un sistema de criptografía de clave pública o criptografía asimétrica, que consiste en una clave privada, que el usuario debe guardar en secreto, y una pública, que es conocida por todos los usuarios del sistema.

Posteriormente varios estados de Estados Unidos legislaron sobre el tema hasta que en el año 2000 se dictó una ley federal.

En 1996, Naciones Unidas, a través, de la UNCITRAL, dicta la Model Law on Electronic Commerce, atendiendo a que muchos países no contaban con legislación adecuada para receptar el comercio electrónico. Las exigencias de los documentos escritos, firmados y originales, constituían los principales obstáculos que esta ley modelo pretendía superar. La misma estipula procedimientos y los principios básicos para facilitar el empleo de las modernas tecnologías de comunicación.

En el 29º período de sesiones, celebrado en Nueva York, del veintiocho de mayo al catorce de junio de 1996, el modelo propuesto por la UNCITRAL fue aprobado por el plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, CNUDMI - UNCITRAL, en la que se analizó al documento electrónico y los lineamientos generales para el desarrollo del comercio electrónico.

La ley modelo en su artículo 7 establece que cuando la ley exija la firma de una persona, la misma se cumple en relación a un mensaje de dato.

La CNUDMI en su calidad de órgano jurídico central del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional, abordó el análisis sobre comercio electrónico, el estudio de las firmas electrónicas, entidades de certificación y la preparación de normas uniformes, con el propósito de establecer criterios comunes respecto del régimen legal y poder establecer una guía para introducir una ley de firmas electrónicas al régimen interior de cada país.

El 31º período de sesiones llevadas a cabo en Nueva York en febrero de 1997, centró su trabajo en las directrices sobre firmas electrónicas publicadas por la American Bar Association de donde se llega al consenso general en relación a la importancia y la necesidad de proceder a la elaboración de una legislación en esta materia. La finalidad era promover una eficaz comunicación digital estableciendo un marco de seguridad jurídica equivalente a los mensajes escritos en cuanto a los efectos jurídicos que producen, y llegar así a una seguridad en el desarrollo del comercio electrónico.

La American Bar Association desarrolló un modelo de directrices o líneas básicas sobre firmas digitales a través del Comité de ciencia y tecnología en su sección de seguridad, las directrices fueron publicadas el primero de agosto de 1996.

En 1997, Italia y luego Alemania regulan sobre esta materia. En 1999, España dicta el Real Decreto 14/1999 sobre Firma Electrónica y rompe en Europa la tendencia de no legislar sobre Firmas Digitales. En ese mismo año, el Parlamento Europeo y el Consejo de la Comunidad Europea adoptan la Directiva 1999/93/ CE por la que se establece un marco comunitario.

Francia comienza a incursionar a partir de 1997 y luego de un período de estudio por una Comisión, el veintinueve de febrero de 2000 la Cámara de Diputados transformó en ley el "Proyecto de adaptación del derecho de la prueba con las nuevas tecnologías de la información en relación con la firma electrónica", introduciendo una trascendente reforma a los principios sobre prueba escrita y firma en el Código Civil Francés, incorporando en estricto pie de igualdad con sus pares analógicos al documento electrónico y a la firma digital. Posteriormente el Gobierno dictó el decreto Nº 2001— 272 del treinta de marzo de 2001, de aplicación del nuevo artículo 1316-4 generando el sistema de firma digital en Francia.

De este modo, la mencionada ley modifica el Código Civil, incorporando en forma genérica el documento electrónico sin entrar en detalles sobre el mecanismo de firma a ser utilizado. Le reconoce al escrito en soporte electrónico la misma fuerza que tiene el escrito en soporte papel, en la medida que permita la identificación de la persona de quien emana y pueda ser conservado de forma tal que sea garantizada su integridad. La firma electrónica consiste,

en Francia, en la utilización de un procedimiento de identificación fiable que garantice su vinculación con el acto o documento para el que ha sido creada. Se presume la fiabilidad del procedimiento, salvo prueba en contrario, en la medida que la firma electrónica sea creada, la identidad del firmante asegurada y la seguridad del acto garantizada, según las condiciones establecidas por decreto por el Consejo de Estado.

En el año 2001, Naciones Unidas, a través, de UNCITRAL elabora un conjunto de nociones generales sobre firmas electrónicas complementando así, a la Ley Modelo sobre Comercio Electrónico.

Los países afrontan dudas al momento de legislar sobre la materia de firma digital, en punto a si hace falta una legislación especial sobre el tema o basta con modificar algunos artículos de los códigos de fondo referidos a firma, expresión escrita y documento, como hiciera Francia para luego sí concentrarse en legislar sobre temas específicos; o si convendrá dictar una ley sobre firma digital con reglas generales o será conveniente una legislación que regule en detalle lo referido al documento electrónico.

Una rápida mirada a la legislación y proyectos existentes sobre firmas electrónicas en el derecho comparado, revela que en donde existe consenso es en lo relativo a los fines declarados: aplicar la firma digital y facilitar el comercio electrónico.

Las legislaciones van desde las que sólo autorizan la utilización de este tipo de firmas en limitadas circunstancias, a reglamentos que establecen detalladamente la forma en que deben utilizarse las firmas digitales y regulan la operatoria de las autoridades certificantes.

En la legislación internacional podríamos hablar de tres modelos básicos sobre mecanismos de autenticación, de la firma electrónica y de la firma digital: (18)

a) Un modelo que procura facilitar el uso de firmas electrónicas en forma genérica. Esto significa que este tipo de acercamiento evita referirse a una tecnología determinada, de forma tal de no cerrar el camino a otro sistema que pueda desarrollarse en el futuro. Por lo tanto, a través de este modelo se procura solamente remover los obstáculos legales que impiden el reconocimiento de las firmas electrónicas y los documentos sustentados en un soporte distinto al papel.

b) El segundo modelo tiende a ser más específico. Se legisla sobre firmas digitales basadas en criptografía de clave pública, estableciendo los alcances de su utilización y los detalles de la infraestructura necesaria para su funcionamiento: certificados, autoridades certificantes, licenciamiento, etc.

---

(18) http://www.hfernandezdelpech.com

c) El tercer modelo representa una síntesis de los otros dos. Este modelo implica la sanción de leyes que determinan estándares para el funcionamiento de infraestructura de clave pública al mismo tiempo en que se refiere en forma genérica a lo que constituye una firma electrónica. Su ventaja radica en que asegura la neutralidad al reconocer distintos mecanismos de autenticación, mientras crea un entorno legal predecible y mejor definido al incorporar previsiones referidas a una tecnología en particular.

La adopción de alguno de estos modelos por los diferentes países estuvo relacionada con el sistema de derecho imperante en cada uno de ellos, así mientras los países de derecho común han tendido a adoptar el modelo de mínima, en los demás países, se advirtió inicialmente una tendencia a adoptar el criterio específico. En tanto en la Unión Europea, se produjo una inclinación hacia el tercero.

Con mayor o menor grado de avance la mayoría de los países en desarrollo tienen una normativa.

En el ámbito mundial, y siguiendo la mencionada cita, las tendencias de las legislaciones que se han ido dictando presentan las siguientes características:

a. Se produce una evolución desde las primeras legislaciones eminentemente reglamentarias y completas como la ley del estado de Utah en Estados Unidos, pasando por legislaciones técnicas como la ley de Alemania, hacia legislaciones más flexibles como el Real Decreto Español, la ley de Portugal, la ley de Colombia y la minimalista ley de Perú.

b. La tendencia mundial es el dictado de leyes de articulado breve, delegando en el reglamento de la ley, la tarea de establecer en firma exhaustiva los derechos, deberes y obligaciones de los sujetos que participan de la actividad.

c. La tendencia indica también, que las leyes se estructuran sobre cuatro conceptos fundamentales: firma electrónica o digital, documento electrónico, certificados digitales y prestadores de servicio de certificación.

d. Sobre esta materia, la Unión Europea promueve el libre acceso para quien quiera prestar servicios de certificación, estableciendo cada país en particular las normas mínimas que regirán la actividad. Además, en algunos países como España por ejemplo, se establece un sistema libre de acreditación frente al Estado, premiando esa adhesión voluntaria con el otorgamiento de mayor valor legal a los certificados emitidos por organismos acreditados.

e. La legislación sudamericana en cambio, se inclina por el sistema de autorización previa por el organismo estatal competente.

f. Las legislaciones más modernas, establecen requisitos de forma y fondo, llámense técnicos, financieros y de personal, relativamente importantes para el desarrollo de la actividad de certificación, ya sea estableciéndolos directamente en la ley o encomendado esa tarea al reglamento.

g. En cuanto a responsabilidades, la situación no es del todo clara. Legislaciones como la española y la doctrina en general, obligan al prestador de servicios de certificación a probar la diligencia con que actuó, y lo hacen responsable de los errores y consecuencialmente de los daños que su negligencia produzcan.

III.2. Algunas iniciativas en el mundo

III.2.a. Unión Europea (19)

Antes de comentar el avance en materia de legislación digital en particular en alguno de los países que conforman la Unión Europea, podemos mencionar, haciendo un poco de historia, que en un estudio comparativo de distintos países que la conforman realizado en 1992 reveló los siguientes datos sobre el valor probatorio de los documentos informáticos:

Respecto de la exigencia de la firma, solo Bélgica, Dinamarca, Luxemburgo y Alemania no preveían la posibilidad de una firma electrónica, pero ésta estaba aceptada en España, Francia, Grecia (si se la estampaba mecánicamente), Irlanda (para el derecho fiscal), Italia (si era posible identificar al emisor), Países Bajos y Portugal, donde se la equiparaba a un sello.

Respecto de la fuerza probatoria de los registros almacenados en soporte informático, cabe distinguir según el sistema probatorio que se aplique:

a) En los países donde regía la prueba libre, como en Dinamarca, se admitía su valor pero quedaba sujeto a la apreciación del juez en función de las garantías de autenticidad; no existía jurisprudencia al respecto.

b) En los países de prueba legal tampoco existía jurisprudencia, pero cabe aclarar que, en España, estos registros no tenían valor, a excepción de los datos que estaban contenidos en las bandas magnéticas; en Portugal si por ser supuestos admisibles a los documentos particulares y en Alemania se les otorgaba valor en virtud del art. 261 del Código de Comercio.

c) En los sistemas de prueba mixta la validez de estos sistemas también es admitida. En Francia y Bélgica, tenían valor en los casos de registraciones del derecho fiscal, contable o aduanero. En Grecia sólo si es autentificada por listings, equiparándose la memoria del computador a un documento escrito.

---

(19) Revista del Notariado, Nº 861, año 2000, pág. 90 y ss.

d) Por último, en los países del derecho común (Irlanda e Inglaterra) se admitía la fuerza probatoria de estos registros, sólo para ciertas transacciones bancarias (Irlanda) o bajo ciertas condiciones ya enunciadas (Civil Evidence Act, en Inglaterra), quedando en este último caso librado su valor a la apreciación del juez.

Es interesante destacar dada su exactitud y detallismo, la definición de firma digital incluida en la Directiva de Firma Digital de la Unión Europea, en cuyo art. 2 se establece que la "firma electrónica avanzada es la firma electrónica que cumple los requisitos siguientes: a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable.

Como los distintos enfoques legales que se puedan adoptar en países de la Unión pueden constituir un serio obstáculo para el mercado interno y podrían retrasar el desarrollo de nuevas actividades económicas relacionadas con el comercio electrónico, se sugiere establecer una legislación conjunta entre los países integrantes de la comunidad.

III.2.b. España

En septiembre de 1999, España se adelantaba a buena parte de los países europeos al aprobar un decreto ley para la puesta en marcha de la firma digital. (20)

En la sesión de Ministros de Telecomunicaciones de la Unión Europea, celebrada el veintidós de abril de 1999, se informó favorablemente la adopción de una posición común, respecto del Proyecto de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica.

En ese sentido, existen ya en España diversas normas sobre la presentación de la declaración del Impuesto sobre la Renta de las Personas Físicas por medios telemáticos, dictadas por la Administración Tributaria. La Comisión Nacional del Mercado de Valores, por su parte, aprobó y puso en marcha un sistema de cifrado y firma electrónica que se emplea para la recepción de información de las entidades supervisadas. Asimismo, el art. 81 de la Ley 66/1997, de Medidas Fiscales, Administrativas y de Orden Social anuncia la posibilidad de prestar, por la Fábrica Nacional de Moneda y Timbre Real Casa de la Moneda, los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones, a través de técnicas y medios electrónicos, informáticos y telemáticos. La Fábrica Nacional de la Moneda y Timbre Real Casa de la Moneda actuará en colaboración con Correos y Telégrafos.

---

(20) http://www.europa.eu.int

En el Proyecto de Directiva se incorpora, a solicitud del Estado español, una novedad entre los requisitos exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos, la cual consiste en permitir que la certificación pueda recoger la fecha y la hora en la que se produce la actuación certificante. El Real decreto-ley persigue, respetando el contenido de la posición común respecto de la Directiva sobre firma electrónica, establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación. De igual modo, este Real decreto-ley determina el registro en el que habrán de inscribirse los prestadores de servicios de certificación y el régimen de inspección administrativa de su actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento.

El Ministerio de Administraciones Públicas de España firmó en octubre del 2003 un convenio por el que los ciudadanos y las empresas podrán solicitar una dirección de correo electrónico única en la que recibirán notificaciones administrativas por parte de los organismos públicos con pleno valor jurídico.

El Consejo General de la Abogacía de España presentó su autoridad de certificación. El proyecto permitirá que más de 110.000 abogados puedan agilizar sus trámites y reducir costos hacia los ciudadanos, permitiendo la comunicación segura y con plena validez jurídica de los abogados con las diferentes Administraciones Públicas y con la Administración de Justicia. Asimismo, el gobierno español aprobó el proyecto de implementación del documento de identidad electrónico.

Según fuentes del gobierno español, el número de usuarios de certificados de firma electrónica se acerca al medio millón. Hasta el momento los certificados pueden utilizarse para numerosos trámites con la Administración Pública y se espera que en el futuro su uso se extienda al ámbito privado.

El Colegio de Registradores de la Propiedad, Bienes Muebles y Mercantiles de España y el Consejo General de la Abogacía Española (CGAE) firmaron un convenio para favorecer la utilización de certificados digitales en las comunicaciones entre los profesionales de ambas organizaciones.

Los efectos jurídicos que tiene la firma digital en este país son plenos y equiparables a la firma manuscrita siempre y cuando, a) se trate de una firma electrónica avanzada; b) esté respaldada por un certificado reconocido; c) el mismo haya sido expedido por un prestador certificado, y d) haya sido producida por un dispositivo seguro de creación de firma.

A efectos de facilitar el proceso de prueba, y a diferencia de la Directiva Europea, presume la validez plena de la firma siempre que se den los tres primeros requisitos y que el cuarto se realice mediante un dispositivo de acuerdo a determinadas normas técnicas especificadas en la ley.

III.2.c Estados Unidos (21)

Al tratar la situación internacional —en la introducción a esta sección tercera— expresaba que Estados Unidos fue el pionero en la materia, al sancionarse en Utah en 1995 la primera ley de firma digital (Utah Digital Signatures Act). Bajo el impulso del comercio, principalmente, los diversos estados sancionaron normas reguladoras del tema, hasta que se advierte la conveniencia de homogeneizar federalmente la cuestión.

Fruto de ello, en junio del año 2000, el presidente de ese país, Bill Clinton aprobó como ley el proyecto S.761, esta ley fue firmada digitalmente por el presidente mediante la inserción de una tarjeta inteligente (smart card) con su clave privada en un ordenador.

Antes y para facilitar la adopción de leyes similares, como dije, se había elaborado una directriz modelo conocida como "Directrices Modelo de Firma Digital de la Asociación de Abogados de Estados Unidos", pero tanto esta ley modelo como la pionera ley de Utah fueron criticadas resultando claramente necesaria la elaboración de una ley federal en la materia.

A nivel federal, las discusiones sobre leyes de firma digital comenzaron en febrero de 1997 en la Cámara de Diputados; a comienzos de julio de ese mismo año varios representantes del Congreso sostuvieron que era necesario tener leyes federales en la materia debido a la posibilidad de conflictos en la legislación estadual. Para esa fecha cerca de 30 estados habían aprobado o estaban considerando leyes de firma digital o firma electrónica.

El aspecto sobresaliente de esta ley es la escasa intervención que le corresponderá al estado en esta materia. Tal vez es demasiado escasa ya que la ley americana si bien señala los sistemas basados en criptografía de clave pública deja librado a la actividad privada el uso e implementación de estas actividades. Por contraposición, nuestra ley 25.506 crea varias instancias encargadas de regular la infraestructura de firma digital.

Podemos afirmar que la importancia de esta ley radica en la creación de un principio general de equivalencia entre las versiones electrónicas de contratos, firmas, notificaciones y otros documentos y sus símiles analógicos; también establece que un contrato no será inválido por el sólo hecho de que se usó una firma electrónica o un registro electrónico en su formación. En este aspecto es donde encontramos una diferencia muy importante con nuestra ley de firma digital, ya que mientras que en los Estados Unidos se diseñó a la firma digital como una forma más de suscribir los documentos, en Argentina se la diferenció desde un primer momento con la firma ológrafa, adjudicándole un régimen especial y mucho más estricto. La prueba de ello es que mientras que en los Estados Unidos suscribir digitalmente un documento es lo mismo que

---

(21) Revista de Derecho Comparado, Nº 5, año 2002, Santa Fe, Ed. Rubinzal-Culzoni Editores.

hacerlo manualmente, en Argentina se requiere la intervención obligatoria de una autoridad certificante como condición sine qua non.

Un tema interesante a analizar con respecto a esta ley es sobre las cuestiones de prioridad entre la legislación federal y la estatal. La finalidad del congreso de lograr uniformidad requirió que la ley federal tuviera una norma sobre prioridad de la legislación federal sobre la estatal, pero aun es un tema pendiente sujeto a interpretación judicial si la ley federal será aplicada en forma prioritaria a la ley estadual.

Con respecto a las excepciones contenidas en la ley, hay que mencionar que se exceptuaron muy pocas actividades, entre ellas del Derecho de Familia y Sucesiones, los documentos judiciales y una lista de notificaciones que se refieren a actos importantes en la vida del consumidor, tales como notificar la cancelación de un servicio público o una orden de desalojo. Sin embargo, estas excepciones están sujetas a una futura revisión del secretario de Comercio dentro de cierto período luego de la sanción de la ley.

Para finalizar es menester destacar que esta ley le atribuye una gran responsabilidad a aquel individuo que pierda o no cuide bien una clave privada. Un suscriptor de firmas digital deberá responder por una gran cantidad de responsabilidades compartidas por la falsificación de la firma causada por un descuido en la salvaguarda de la clave perdida.

III.2.d Uruguay

Uruguay optó por incorporar el tema a su Código Civil al legislar sobre firma digital, validez de los documentos electrónicos y eficacia probatoria de ambos instrumentos.

Este país, cabe destacar que fue el primero en Latinoamérica en legislar sobre la firma digital mediante la ley 16.736 en la cual entre otras cuestiones establece en el art. 695 que: “Los trámites y actuaciones que conforman el procedimiento administrativo así como los actos administrativos podrán realizarse por medios informáticos. Su validez jurídica y valor probatorio serán idénticos a los de las actuaciones administrativas que se tramiten por medios convencionales. La firma ológrafa podrá ser sustituida por contraseñas o signos informáticos adecuados”; en su art. 696 estipula además que: “La notificación personal de los trámites y actos administrativos podrá realizarse válidamente por correo electrónico u otros medios informáticos o telemáticos, los cuales tendrán plena validez a todos los efectos siempre que proporcionen seguridad en cuanto a la efectiva realización de la diligencia y a su fecha”; y, por último, en su art.697 aclara que: “La documentación emergente de la transmisión por medios informáticos o telemáticos constituirá de por si documentación autentica y hará plena fe, a todos sus efectos, en cuanto a la existencia del original transmitido”.

En Uruguay, si bien se consagró a la Administración Nacional de Correos como la autoridad certificante, la misma se limita a emitir los certificados.

III.2.e. Chile

Chile, con su Ley de Firma Electrónica se aparta del denominador común en cuanto a la denominación en las legislaciones de los demás países de la región, llamando *firma electrónica avanzada* a la firma digital.

Se observa un gran avance en la incorporación de las TICs,(22) ya sea a nivel de comercio electrónico como de apoyo a la gestión pública. Esta iniciativa dotó del marco jurídico necesario para dar estabilidad a las relaciones por medio de sistemas informáticos y telemáticos, otorgando mayores niveles de seguridad y certeza.

La ley chilena regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.

Además del gran avance que significó la determinación de la naturaleza de los documentos electrónicos, esta ley aborda el uso de la firma electrónica en la Administración del Estado, dando de esta forma sustento legal a las actuaciones efectuadas por estos medios, siempre y cuando cumplan con los requisitos establecidos por la misma.

Señala expresamente que "los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica" (Art. 6 Ley 19.799), exceptuándose sólo aquellas actuaciones para las cuales la Constitución Política o la ley exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas.

En el artículo 7 de la citada Ley 19.799 se establece el principio de equivalencia de soportes (en concordancia con los artículos 5, 18 y 19 de la Ley de Bases de Procedimiento Administrativo) señalando que los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel. Requiere para los instrumentos públicos, celebrados mediante esta metodología informática, para gozar de la calidad de tales y para que surtan los efectos propios de ellos, que deban suscribirse mediante firma electrónica avanzada.

Plantea la ley chilena el Proyecto de Modernización del Estado y Gobierno electrónico, que se define como "el uso de las TICs para mejorar los servicios e información ofrecidas a los ciudadanos, aumentar la eficiencia de la gestión pública e incrementar substantivamente la transparencia en el sector público y la participación ciudadana."

---

(22) Tecnologías de la Información y de la Comunicación.

Los ámbitos de acción sobre los cuales plantea que se promueva el gobierno electrónico tienen relación con tres esferas: atención al ciudadano, buen gobierno y desarrollo de la democracia.

Para fomentar el desarrollo del gobierno electrónico, se contemplaron también distintos tipos de instrumentos, tanto legales como administrativos, como son, por ejemplo: la Ley de Firma Digital, la Ley de Dirección de Compras Públicas; el Decreto Supremo Nº 81 de 1999, que reguló el uso de la firma digital Intraestado; el Decreto Supremo Nº 1312-1999; que establece el uso del sitio chilecompras.cl; el Decreto Supremo Nº 54-2001, que permite el establecimiento de acuerdos marcos para los procesos de compra; el Instructivo Presidencial Nº 5 del 11 de Mayo de 2001, que da instrucciones para el gobierno electrónico; y el PMG 2001, que establece la obligatoriedad del uso de chilecompras.cl a 95 servicios públicos.

Es necesario resaltar, por su importancia, la Ley 19.628 sobre protección a la vida privada, que regula el tratamiento de datos personales por medios automatizados, estableciendo los requisitos para la obtención, tratamiento y registro de datos personales por parte de los Organismos Públicos.

III.3. Antecedentes nacionales

En nuestro país la iniciativa nace en el seno del Estado Nacional, aproximadamente en 1996.

A partir de entonces se ha sucedido un intenso trabajo desde la Secretaría de la Función Pública, reflejado en las numerosas disposiciones que permitieron que en el ámbito de la administración pública nacional desde hace tiempo se utilice la firma digital.

Debe destacarse el esfuerzo realizado por el Ministerio de Justicia, la Jefatura de Gabinete y, en el ámbito privado, la colaboración del Consejo Federal de Notariado Argentino y del Colegio de Escribanos de la Capital Federal.

La Comisión Nacional de Valores (CNV), desde hace tiempo está aplicando tanto las disposiciones de la firma digital como la presentación de documentación en forma digital.

Párrafo aparte merece la labor desarrollada por la Junta Federal de Cortes y Superiores Tribunales de Justicia de la Provincias de la República Argentina. Del seno de sus deliberaciones surgieron las matrices que servirían como antecedentes para las ulteriores elaboraciones legislativas en la materia: el Acta-Acuerdo de Termas de Río Hondo —Santiago del Estero—, la constitución del Foro Permanente de Técnicos Informáticos; que trabajó en forma conjunta con el Foro de Ministros, el Convenio de Comunicaciones Electrónicas Interjurisdiccionales celebrado en Ciudad Autónoma de Buenos Aires, entre otros.

El Anteproyecto de Código Civil y Comercial Unificado de 1998, preveía modificaciones referentes al documento electrónico y a la firma digital. Ex-

presamente el proyecto dice: "se amplía la noción de escrito, de modo que puede considerarse expresión escrita, la que se produce, consta ó lee a través de medios electrónicos". También se define la firma, y se considera satisfecho el requisito de la firma cuando en los documentos electrónicos se sigue un método que asegure razonablemente la autoría e inalterabilidad del documento. Se prevé expresamente que existan instrumentos públicos digitales.

En su art. 226, establece que, la firma prueba la declaración de la voluntad expresada en el texto al cual corresponde. Debe ser manuscrita y consistir en el nombre del firmante, o en un signo, escritos del modo que habitualmente lo hace a tal efecto. En los instrumentos generados por medios electrónicos, el requisito de firma de una persona, queda satisfecho si se utiliza un método para identificarla; y ese método asegure razonablemente la autoría e inalterabilidad del instrumento.

Como se observa, los recaudos requeridos por este proyecto para la validez de una firma digital, son los mismos que prevén para la firma ológrafa. Según el análisis del texto, diríamos que los recaudos a observarse son: a) la existencia de un método para asegurarla: un método es un modo de hacer con orden una cosa, por esto se requiere un conjunto ordenado de reglas preestablecidas, que ordenen la forma en que se identifica la persona en relación con la firma digital que se incluya en un documento; b) además que dicho método asegure razonablemente: la autoría, es decir, la posibilidad de identificar a la persona que firmó el documento; y la inalterabilidad del instrumento, o sea, la imposibilidad de que sea alterado físicamente el contenido del documento, o, en caso de ser modificado, el sistema debe tener un resguardo que permita detectar dicha alteración.

El Anteproyecto del Código Civil y Comercial del año 1998, dispone importantes modificaciones en el tratamiento de los instrumentos; equiparando a los documentos digitales con el documento tradicional.

Lo relevante es que:

Se amplía la noción de escrito, de modo que puede considerarse expresión escrita la que se produce, consta o lee a través de medios electrónicos.

Se define la firma y se considera satisfecho el requisito de la firma cuando en los documentos electrónicos se sigue un método que asegure razonablemente la autoría e inalterabilidad del documento.

Se prevé expresamente la posibilidad de que existan instrumentos públicos digitales. En este sentido el proyecto de Código recepta los documentos electrónicos, aunque con fórmulas abiertas y flexibles y sin vinculación a la tecnología. De ese modo intentaba evitar su rápido envejecimiento que se produciría por el vértigo de la permanente superación de la tecnología.

Se regula expresamente el valor probatorio del documento electrónico, que se vincula a los usos, a las relaciones preexistentes de las partes y a la confiabilidad de los métodos usados para asegurar la inalterabilidad del texto.

Para ello se han tenido especialmente en consideración la ley modelo de comercio electrónico elaborada por UNCITRAL, el Código de Québec y las tentativas de reforma del Código Civil francés en materia de prueba.

Sus artículos más destacados sobre el tema en análisis son los art. 262, 263, 264, 264, 266, 267 y 268.

Otros antecedentes que deben citarse los encontramos en el ámbito comercial. En efecto el art. 53 del C. de Comercio, fue modificado por el art.61 de la Ley 19.550 que permitió a las sociedades la sustitución de las anteriores formalidades en materia de documentación contable y libros de comercio, habilitando los usos informáticos.

La ley 24.624, complementaria del presupuesto general, habilitó la posibilidad de de archivar documentación de la Administración Pública nacional en soporte electrónico.

El 16 de abril de 1998 el Poder Ejecutivo dictó el decreto 427 mediante el cual dispuso la creación de la Infraestructura de firma Digital (IFDAPN), y habilita el uso de la firma digital en actos internos de la administración.

En el año 2001 el decreto 677 vinculado al régimen de Transparencia de Oferta Pública, establece pautas para la gestión de la Comisión Nacional de Valores, como autoridad de aplicación instituida. En la norma se acepta la posibilidad de celebrar reuniones de directorio y asambleas por medios no presenciales

La ley 25.506:

Al final del camino encontramos nuestra ley de firma digital. Como se dijo, lleva el número 25.506, fue sancionada el catorce de noviembre de 2001 y promulgada de hecho el once de diciembre de ese mismo año. A título de síntesis hago referencia a la misma, dado que es la materia desarrollada en mayor extensión al capítulo siguiente.

Dicha ley incorpora el reconocimiento con fuerza legal de los distintos modos de expresión de consentimiento o declaraciones de conocimiento que puedan realizarse sobre soporte electrónico.

La citada ley 25.506 regula una nueva forma de interactuar, al reconocer validez y valor probatorio al documento digital y autorizar el uso de la firma digital, al tiempo que, bajo ciertas condiciones, reconoce la firma digital y certificado digital extranjeros. Regula también el uso de la firma electrónica, con una acepción más amplia que la digital.

Esta norma no sustituye las formas tradicionales, por el contrario, se proclama un respeto a las formas documentales existentes, agregando en nuestro sistema legal, a las formas tradicionales, el documento digital, y a la firma, la firma electrónica y la firma digital.

Un alto porcentaje de la ley está dedicado a la organización del soporte necesario para el funcionamiento de la firma digital.

Es fundamental para el desarrollo del comercio electrónico, el reconocimiento legal del documento así emitido, en equivalencia con el documento impreso en papel y su admisibilidad como prueba en juicio.

Hoy podemos hablar de tal equivalencia entre el documento en soporte papel y electrónico, dejando a salvo los requisitos solemnes de la intervención y actuación notarial.

III.4. El documento digital y la prueba en los regímenes procesales.

En materia procesal debe tenerse en cuenta lo prescripto en nuestro régimen nacional en cuanto a que "... la prueba deberá producirse por los medios previstos expresamente por la ley y por los que el juez disponga, a pedido de parte o de oficio, siempre que no afecten la moral, la libertad personal de los litigantes o de terceros, o no estén expresamente prohibidos para el caso. Principio general contemplado en modo análogo en casi todos los regímenes provinciales.

Los medios de prueba no previstos se diligenciarán aplicando por analogía las disposiciones de los que sean semejantes o, en su defecto, en la forma que establezca el juez" (art. 378 C.P.C.C. de la Nación; y art. 376 C.P.C.C. de la Provincia de Bs. As.).

Las normas en general en nuestros sistemas procesales provinciales y nacionales, no son taxativas, al admitir los medios de prueba. No se alude en forma expresa al medio probatorio en tratamiento, pero puede admitirse tácitamente. Debe agregarse para arribar a esta conclusión, la aplicación esencial de la sana crítica judicial prevista en los códigos citados que expresamente prescriben que "... salvo disposición legal en contrario, los jueces formarán su convicción respecto de la prueba, de conformidad con las reglas de la sana crítica..." (art. 386 C.P.C.C. de la Nación; art. 384 C.P.C.C. de la Pcia. de Bs. As.), es por ello que los jueces están dotados de suficientes facultades para llegar a la verdad valorando críticamente los elementos aportados por los litigantes, pudiendo incluirse entre ellos al documento electrónico, evaluando adecuadamente la autenticidad, seguridad e inalterabilidad de los soportes utilizados. (23)

IV. La firma digital en la ley 25.506

IV.1. Aspectos generales

Recordemos algunas definiciones de firma. Una dice: "nombre y apellido, o título de una persona, que ésta pone con rúbrica al pie de un documento

---

(23) VALCARCE, A., "Valor probatorio del documento electrónico", en Revista de Jurisprudencia Provincial, Buenos Aires, año 5, Nº 9, págs. 741/747, año 1994.

escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido, o para obligarse a lo que en él se dice.". Otra, comentando la nueva ley de Francia, habla de un grafismo, por el cual una persona se identifica en un acto y asiente sobre el contenido del documento, acordándole fuerza probatoria. Estas definiciones incorporan dos cuestiones, la intención y la fuerza probatoria.

En su artículo1 referido al Objeto, nuestra ley 25.506 dice que: "Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley."

Se advierte que comienza hablando de firma electrónica, antes que de la firma digital. Aunque la firma electrónica es el género, y la firma digital es la especie, tratándose de una Ley de Firma Digital no parece razonable comenzar con una referencia a aquélla, firma electrónica, máxime, cuando más adelante la habrá de considerar en especial.

La firma digital específicamente está definida en el artículo 2: "Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar cualquier alteración del documento digital posterior a su firma."

Vemos así que la firma digital requiere determinadas condiciones, que luego complementa con otras disposiciones.

a. Aplicar a un documento digital: de acuerdo con esta definición la firma digital no existe, no tiene vida, sin un documento digital.

b. Un procedimiento matemático: la firma digital es un procedimiento matemático realizado automáticamente por un computador, generando un par de claves.

c. Información de exclusivo conocimiento del firmante. Se aclara que la ley debió decir más correctamente "que debe ser susceptible de conocimiento exclusivo", pero no obsta al hecho de que el firmante permita que un tercero conozca esa información.

d. Encontrándose ésta bajo su absoluto control: aquí cabe la misma observación del anterior. Debe ser de conocimiento exclusivo y estar bajo su absoluto control. Esto supone tener en todo momento la posibilidad de su utilización, sin depender de terceras personas.

e. Susceptible de verificación: ésta es una condición esencial dado que, en el esquema de la ley, si ello no se verifica no estamos ante una firma digital, aunque podría ser una firma electrónica.

f. Posibilidad de identificar al firmante: la firma digital debe permitir la identificación del firmante en forma indubitable. En verdad, estamos aquí ante una ventaja sobre la simple firma la cual, prima facie, no identifica necesariamente al firmante. Ante una firma escrita o manuscrita, podemos decir que presumiblemente es de tal persona y se la atribuimos, pero no con el grado de certeza que lo hace la firma digital.

g. No alteración del documento digital: finalmente la firma digital debe proteger la inalterabilidad del documento digital con lo cual, asegurada la identidad de quien la firma y la autenticidad del documento digital, sería imposible que el firmante niegue o repudie el documento digital. En otras palabras, está introduciendo el concepto del no repudio que requieren otras legislaciones. También en esto su efecto es superior a la simple firma.

El artículo 7 de la ley trata sobre la presunción de autoría; se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma. Este artículo introduce el concepto del certificado digital de donde resulta que no hay firma digital sin un certificado digital.

El artículo 8 introduce otra presunción esencial, esto es, que el documento digital no ha sido modificado. "Presunción de integridad: si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma."

Concluimos que estos artículos 7 y 8 otorgan a la firma digital presunción de autoría y de integridad, es decir que la carga de la prueba, el onus probandi, recaerá sobre la persona que alega la falsedad de un documento firmado digitalmente, o que el mismo ha sido firmado por otra persona.

Y el artículo 10 suma otra presunción importante: "Remitente. Presunción: cuando un documento digital sea enviado en forma automática por un procedimiento programado y lleve la firma digital del remitente, se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente."

Los recaudos de validez están expuestos en el art. 9:

"Validez: una firma digital es válida si cumple con los siguientes requisitos:

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 artículo 16 de la presente, por un certificador licenciado."

No sólo tiene que haber un certificado digital, sino que la firma digital que haya sido estampada durante su período de vigencia pues en caso contrario no vale como tal. El inciso c) requiere, además, que dicho certificado digital haya sido emitido o reconocido por un certificador licenciado. Al terminar esta disposición se consigna que una autoridad de aplicación regulará todo lo referido a cuestiones tecnológicas. No puede haber firma digital sin un certificado digital y éste sólo puede ser válido si ha intervenido un certificador licenciado y los procedimientos sólo podrán ser los determinados por la autoridad de aplicación. Todo ello es lo que se conoce como infraestructura de firma digital.

En tal sentido el artículo 23 señala los casos de invalidez del certificado: "Desconocimiento de la validez de un certificado digital: un certificado digital no es válido si es utilizado:

a) para alguna finalidad diferente a los fines para los cuales fue extendido;

b) para operaciones que superen el valor máximo autorizado cuando corresponda;

c) una vez revocado."

IV.2. Ambito de validez de la ley

El campo de validez de la firma digital, de la firma electrónica y del documento digital, está delimitado por vía de las exclusiones y excepciones, esto es por las esferas que les son vedadas. El artículo 4 que las establece dice que sólo no son válidas en las situaciones taxativamente enumeradas.

"Exclusiones: las disposiciones de esta ley no son aplicables:

a) a las disposiciones por causa de muerte;

b) a los actos jurídicos del derecho de familia;

c) a los actos personalísimos en general;

d) a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdos de partes."

IV.3. Relaciones entre la normativa sobre firma digital y el derecho de fondo

La ley de firma digital incorpora algunas disposiciones al derecho de fondo. Así en el artículo 3 se establece: "Del requerimiento de firma: cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por

una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencia para su ausencia."

A partir de esta ley, cada vez que en los códigos y leyes de fondo se lea la palabra firma y documento o instrumento puede ser reemplazado por firma digital o documento digital.

En general las disposiciones de la legislación argentina y el código no registran contradicciones y son compatibles con la utilización de la firma digital.

Vale alguna aclaración con relación a la firma en blanco (art.1016 C.C.: recordemos que se otorga antes de la redacción del escrito y hace fe después de llenado el acto por la parte a la cual se le ha confiado, siempre que el firmante haya reconocido la firma). Implica una autorización por parte del firmante a otra persona para llenar el documento firmado en blanco.

La firma digital es práctica y técnicamente imposible de otorgar en blanco, dado que como dijimos es vinculada, ligada de modo inseparable, inescindible al documento digital.

IV.4. La firma electrónica

Se mencionó ya que la firma electrónica sería el nombre genérico de una forma de expresar en el mundo digital todo lo que implica la firma en el mundo real. La firma digital sería una variedad, la más conocida, segura y recomendable, de la firma electrónica. En el artículo 5 se define a la firma electrónica: "Se entiende por firma electrónica el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quién la invoca acreditar su validez."

Hay diferencias notables entre la firma electrónica y la firma digital, lo sustancial son las presunciones, pues en tanto en el caso de firma digital se presume que, cumplidas ciertas condiciones, el firmante no puede desconocerlo y se invierte la carga de la prueba, iuris et de iure, en el caso de la firma electrónica, corresponde a quién la invoca acreditar su validez.

El legislador hacia el final marca el elemento diferenciante más importante "que carezca de alguno de los requisitos legales para ser considerada firma digital". Todos los sistemas de identificación digital que expresen asentimiento e identificación y que carezcan de alguna de las características de la firma digital serán firma electrónica.

electrónicos, utilizado por el signatario como su medio de identificación". Deja de lado aquí los conceptos de reserva y exclusivo control, para ir hacia algo más simple.

In fine marca el elemento diferenciante más importante "que carezca de alguno de los requisitos legales para ser considerada firma digital". Todos los

sistemas de identificación informática que carezcan de alguna de las características de la firma digital serán firma electrónica.

IV.5. Documento digital y firma digital

La ley define al documento digital en su artículo 6: "Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.".

En el ámbito digital un documento es exactamente igual a otro, no se trata de algo muy parecido, sino lo mismo, no es una copia en nuestra concepción común y habitual. La ley resuelve el tema de esta forma en el artículo 11: "Original: los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación."

En cuanto a la obligación de conservar los documentos existente en alguna legislación dice el artículo 12: "Conservación: la exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción."

Este artículo posibilita cumplir con las exigencias legales de conservación de documentos, registros o datos, como por ejemplo: notificaciones, balances de empresas, libros de actas de asambleas societarias, libros de accionistas, etc., en soporte digital y firmados digitalmente de forma tal que puedan ser accedidos para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

IV.6. Firma manuscrita y firma digital

Consideraciones de la Comisión Redactora del Anteproyecto: La misma sostiene la validez de la firma manuscrita cuando se cumplen las siguientes condiciones:

a) el documento está escrito con tinta indeleble y en soporte papel absorbente, tal que una enmienda o raspadura que altere la información escrita sea visible y evidente.

b) el documento posee márgenes razonables que contienen los renglones escritos, tal que cualquier escritura adicional sea visible y evidente.

c) la firma manuscrita se coloque delimitando la información escrita, tal que no sea posible agregar texto escrito a continuación de la firma manuscrita.

d) el firmante utiliza siempre la misma o similar firma manuscrita para firmar los documentos de su autoría.

e) la firma manuscrita es suficientemente compleja tal que su falsificación deviene no trivial.

f) existen peritos calígrafos que pueden detectarlas falsificaciones con un razonable grado de certeza.

Es importante destacar, agrega, que la falla de cualquiera de los seis puntos especificados tornaría inseguro el mecanismo de firma manuscrita para documentos en soporte papel permitiendo así a su autor repudiar la autoría de los documentos que le son atribuidos.

En el régimen de la ley de firma digital, dentro de su mecanismo propuesto, estos puntos se implementan generando un digesto o resumen criptográfico del mensaje, creado por una función de digesto de mensaje, el cual a su vez es encriptado con la clave privada del firmante, que solo el firmante conoce, y un certificador de clave pública que certifica cuál es la clave pública utilizada por el firmante.

También el informe compara la seguridad entre la firma ológrafa y de la firma digital.

La tecnología propuesta de firma digital no es perfecta ni infalible. Los dispositivos de hardware y software de creación y verificación de firmas digitales deben ser homologados previa auditoría de su funcionamiento para poder ser utilizados para crear firmas y verificar firmas digitales con plena eficacia jurídica. Por otro lado, es importante destacar que la firma manuscrita tampoco es perfecta e infalible, puesto que es decididamente posible en ciertos casos alterar de forma indetectable el contenido de un documento en soporte papel o falsificar una firma manuscrita.

IV.7. Protección penal

La ley en su artículo 51 ha equiparado los términos de firma con firma digital y de documento o instrumento con el de documento digital. Reza el texto de dicho artículo:

"Equiparación a los efectos del derecho penal. Incorporase el siguiente texto como artículo 78 (bis) del Código Penal: los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente."

Pero debe señalarse que se omite el instrumento público cuando, como se ha visto, la firma digital se aplica hoy a instrumentos públicos en el ámbito de la administración nacional.

IV.8. Despapelización del Estado

La ley incentiva a la despapelización del Estado. Así, dice, por ejemplo, que "el Estado Nacional utilizará las tecnologías y previsiones de la presente ley en el ámbito interno y en relación con los administrados", en el artículo 47, y también que "... promoverá el uso masivo de la firma digital que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización. En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley (esto es, a partir del año 2001), se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones, sentencias", en el artículo 48.

IV.9. La situación en la Justicia

Tanto el documento digital como la firma digital han tenido un gran impacto en la actividad judicial y en los propósitos declarados de despapelización. Pese a ello estamos a mitad de camino y falta el impulso final, que sin dudas y amagues, haga plenamente operativa la digitalización en el seno de la Justicia.

Una vez que se lleve a cabo la plena operatividad de la digitalización habilitada por la ley 25.506, en especial su firma, servirá para concretar la anhelada informatización de la Justicia, objeto de reclamo permanente, por mayor agilidad, eficacia y eficiencia, acorde con los tiempos que corren.

Los anhelos expresados por los hombres de las justicias provinciales argentinas desde el Acta Acuerdo de Termas de Río Hondo del dieciocho de junio de 1999 y en el Convenio de Comunicación Electrónica Interjurisdiccional del seis de septiembre de 2001, pueden hacerse realidad en el marco de esta legislación y su operatividad.

El primer documento (Acta Acuerdo de Termas de Río Hondo 1999), se constituyó en el punto de partida necesario del posterior desarrollo en la materia. Tal Acta Acuerdo referida fue fruto de la primera reunión convocada a tal efecto por la Junta Federal de Cortes y Superiores Tribunales Provinciales (JU. FE.JUS.). Al suscribirla, los poderes judiciales provinciales asumieron coordinadamente el compromiso de colaboración recíproca para la implementación de nuevas tecnologías aplicadas al servicio de Justicia.

Se sentaron así, las bases consensuadas del trabajo interdisciplinario a realizar, y, simultáneamente, se constituyó el Foro de Técnicos Informáticos que comienza a desempeñar sus labores junto a los Ministros de las Cortes provinciales.

Consecuencia directa de esos compromisos asumidos fue el Convenio de Comunicación Electrónica Interjurisdiccional en el que se establecieron los principios rectores en la materia y se fijaron una serie de objetivos a alcanzar en forma coordinada entre, los poderes judiciales de las provincias, sus ministerios públicos, el Ministerio Público nacional, el Ministerio de Justicia y Derechos Humanos de la Nación y la Jefatura de Gabinete de Ministros. Se sentaron así, las bases consensuadas del trabajo interdisciplinario a realizar, y, simultáneamente, se constituyó el Foro de Técnicos Informáticos que comienza a desempeñar sus labores junto a los Ministros de las Cortes provinciales.

IV.10. Ventajas de la firma digital: reconocimiento de aspectos negativos

La primera ventaja que podemos mencionar de la firma digital en comparación de la firma ológrafa, es que el procedimiento de verificación es exacto y que, si bien no es imposible en la práctica su falsificación, a diferencia de la firma manuscrita, en el caso de la firma digital la alteración es fácilmente detectable.

Otra ventaja es que puede ser realizada en diferentes puntos del mundo, de forma simultánea y sin necesidad de testigos. En un contexto electrónico, en el que no existe contacto directo entre las partes, resulta posible que se trabaje con un documento digital que ofrezca la misma eficacia que los documentos físicos, pero con plena seguridad, en especial en cuanto a: a) integridad de la información, b) autenticidad del origen del mensaje, c) no repudio del origen, d) imposibilidad de suplantación, y e) auditabilidad.

En lo específico en la órbita del Poder Judicial, la puesta en funcionamiento de esta tecnología aporta la seguridad que le faltaba a la celeridad procesal, con muchas expectativas, en todos los ordenes como el que nos ocupa de las comunicaciones entre jueces de la propia y de distinta jurisdicción y en otras esferas como por ejemplo en materia de presentaciones judiciales. Se hacen virtuales las actividades las mesas de entradas (muchas justicias provinciales ya lo tienen implementado) trayendo como consecuencia diversos tipos de efectos:

a) se descongestionan las mesas de entradas;

b) se aprovecharían los recursos humanos existentes en tareas de mayor elaboración intelectual;

c) se avanza en la digitalización del expediente (despapelización).

La aplicación de la firma digital, puede abrir campos inimaginables, y de hecho ya nos ha sorprendido, como realizar transacciones bancarias y de comercio electrónico seguras y relacionarse con la Administración.

En cuanto a los aspectos negativos, quizás, lo más notable provenga de la eventual aplicación de criterios legales diferentes en distintos países en cuanto

a los efectos jurídicos de la firma digital, y cualquier diferencia en los aspectos técnicos en virtud de los cuales las firmas digitales son consideradas seguras, resultará perjudicial para su aplicación.

Todas las etapas de transición generan una resistencia en su aceptación a pesar de los grandes beneficios que proporcione.

Otro aspecto a resolver es que no todos los ciudadanos del país tienen acceso a tal tecnología y su lenguaje técnico no es de fácil comprensión para el común denominador de los ciudadanos. Hay una evolución constante de la tecnología en los últimos años, en especial en el campo electrónico y digital. Los cambios operados en el ámbito de la información y de la comunicación han contribuido a la modernización de los instrumentos utilizados para el caso.

Lo que es importante remarcar es la conveniencia de gradualismo y proporcionalidad en la especificación de los sistemas y parámetros, a la hora de aplicar la firma digital en relación con el tipo de acto en particular, teniendo en consideración las consecuencias jurídicas del acto o el valor económico involucrado.

La intervención de un notario y la protocolización del acto, cuando tratamos la venta de un inmueble, no mengua ni lo ha hecho en la historia el valor de la firma ológrafa. Es una forma y una solemnidad que se adiciona sin que merezca discusión. A nadie se le ocurre exigirlo en la compra de un electrodoméstico, o de un pasaje aéreo, con tarjeta de crédito. De igual forma habrá ciertos requisitos para otorgar validez jurídica a los documentos firmados digitalmente, dependiendo de la naturaleza del acto o de la transacción subyacente.

Ese gradualismo y proporcionalidad, no deben ser una guarida de temor y resistencia al cambio con la consiguiente renuencia a aplicar las nuevas herramientas tecnológicas; en este caso la firma digital. Los riesgos están en igual entidad en uso de la firma manuscrita, y en algunos casos, como cuando se refiere a detectar que ha habido alguna alteración, con mayor protección en el ámbito digital.

Cito como ejemplo el caso ocurrido en el Juzgado Federal a cargo del Dr. Ricardo Bustos Fierro de la ciudad de Córdoba, y que originara una causa penal en la que al imputado (cuyo nombre y carátula de la causa preservo hasta tanto no cuente con sentencia firme) se le atribuye haber hecho la firma manuscrita del Juez, secretario y respectos sellos, incluidos los del Tribunal, en oficios que tenían por finalidad ordenar a diversos bancos la entrega de importantes sumas de dinero en dólares (casos denominados comúnmente amparos por el corralito)...y las adulteradas firmas cumplieron su cometido...se logró retirar el dinero. Seguramente si se hubiera encontrado en uso la firma digital el supuesto iter criminis hubiera sido truncado.

V. Precisiones y nomenclatura en el marco normativo vigente

El marco normativo de 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 (B.O. 20/12/2002), el decreto Nº 724/06 modificatorio del anterior (B.O. 13/06/06), la Decisión Administrativa Nº 6/07 y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

Precisión terminológica:

Es conveniente precisar el uso de la terminología adecuada a las opciones de nuestro marco normativo

Firma Digital y Electrónica: como se anticipó, para la legislación argentina los términos firma digital y firma electrónica no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada uno de ellos, dado que en el caso de la firma digital existe una presunción iuris tantum en su favor; esto significa que si un documento firmado digitalmente es verificado correctamente, se presume salvo prueba en contrario que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la firma electrónica, en caso de ser desconocida la firma por su titular corresponde a quien la invoca acreditar su validez.

La legislación argentina emplea el término firma digital en equivalencia al término firma electrónica avanzada o firma electrónica reconocida utilizado por la Unión Europea o firma electrónica utilizado en otros países como Brasil o Chile.

El conjunto normativo que regula la materia conforma una infraestructura de firma digital de alcance federal integrada por:

Autoridad de Aplicación: según el decreto Nº 409/2005, la Subsecretaría de la Gestión Pública actuará como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital establecida en la ley Nº 25.506 y en las funciones de entidad licenciante de certificadores, supervisando su accionar.

Comisión Asesora para la Infraestructura de Firma Digital: funciona en el ámbito de la Subsecretaría de la Gestión Pública, emitiendo recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la infraestructura de firma digital.

A través del decreto Nº 160/2004, el Poder Ejecutivo Nacional ha designado a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la ley Nº 25.506.

Ente Licenciante: es el órgano técnico- administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad.

Certificadores licenciados: son aquellas personas de existencia ideal, registro público de contratos u organismo público que obtengan una licencia emitida por el ente licenciante para actuar como proveedores de servicios de certificación en los términos de la ley Nº 25.506 y su normativa complementaria.

Autoridades de Registro: son 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 el certificador licenciado.

Sistema de Auditoría: será establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.

VI. Régimen normativo vigente

A continuación se detallan las normas que constituyen el régimen normativo vigente en materia de Firma Digital en la República Argentina:

Ley Nº 25506

Ley de Firma Digital - Boletín Oficial 14/12/2001

Decisión Administrativa JGM Nº 6/2007:

Establece el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten.

Decreto Nº 724/2006:

Modifica el Decreto Nº 2628/02 reglamentario de la Ley de Firma Digital.

Decreto Nº 409/2005:

Establece que la Subsecretaría de la Gestión Pública actuará como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital establecida en la Ley Nº 25.506 y en las funciones de entidad licenciante de certificadores, supervisando su accionar.

Resolución JGM Nº 435/2004:

Aprueba el Reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital, que fuera creada por la Ley Nº 25.506 y cuyos miembros fueran designados por Decreto Nº 160/04 del Poder Ejecutivo Nacional.

Decreto Nº 160/2004:

Designa a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la Ley Nº 25.506.

Decreto Nº 1028/2003:

Disuelve el Ente Administrador de Firma Digital, creado por el artículo 11 del Decreto Nº 2628/02, cuyo accionar será llevado a cabo por la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública.

Decreto Nº 152/2003:

Otorga competencia a la Subsecretaría de la Gestión Pública para licenciar a los certificadores, supervisar su actividad y dictar normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de firma digital.

Decreto Nº 283/2003:

Autoriza con carácter transitorio a la Oficina Nacional de Tecnologías de Información a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la Política de Certificación vigente.

Decreto Nº 2628/2002:

Reglamenta la Ley Nº 25.506 de firma digital. Crea el Ente Administrador de Firmas Digitales.

Decreto Nº 1023/2001:

En su artículo 21 permite la realización de las contrataciones comprendidas en el Régimen en formato digital firmado digitalmente.

Resolución SFP Nº 194/98:

Establece los estándares sobre tecnología de firma digital para la Administración Pública Nacional

TERCERA PARTE

LEY DE COMUNICACION INTERJURISDICCIONAL ELECTRONICA

I. Introducción

I.1. Algunas palabras para destacar

- "Cambiar leyes o funcionarios no es el único camino necesario para que el ciudadano vuelva a confiar en la transparencia y eficiencia de la Justicia. Informatizar el Poder Judicial, una tarea mayúscula pero posible, es un paso importantísimo para mejorar la gestión"

- "Solamente en provincia de Buenos Aires se emiten 12 millones de cédulas anuales. En el fuero Penal son 3 millones por vía judicial y 3.700.000 por Policía. Sería significativo el aumento de eficiencia y celeridad en la Justicia de aplicarse en todo el país la notificación digital."

— "La Reglamentación ahora dictada por el Poder Ejecutivo Nacional, al fijar los alcances para otorgar y revocar licencias y obligaciones de los certificadores licenciados es un gran aporte, pues permite que la firma digital surta plenos efectos jurídicos y facilita así su adopción por el Poder Judicial. De esta manera, ya no hay excusas para usar las tecnologías de la información que brindarán mayor transparencia, seguridad y celeridad a los procesos"

Dr. Héctor Chayer, Director de Fores (24)

I.2. Los procesos judiciales y el uso de las nuevas tecnologías de la información y de la comunicación: breve repaso del panorama internacional en la materia

Hemos visto en las páginas precedentes un panorama de la legislación sobre firma digital en el ámbito internacional, veamos ahora la recepción en el ámbito judicial internacional de esta herramienta y en general de la informática

---

(24) Fragmento extraído de la página web del Foro de Estudios sobre la Administración de Justicia, publicado con fecha 16/02/2007, para mayor información ver: www.foresjusticia.org.ar

I.2.a. España: (25)

El servicio que el Ministerio de Justicia (Lex NET) desarrolló y puso en marcha en estrecha colaboración con otras administraciones con competencia en materia de dotación de medios informáticos para la administración de justicia, se puede definir como: "Una plataforma de intercambio seguro de información entre una gran diversidad de agentes que en su trabajo diario o por cualquier circunstancia necesitan operar con la Justicia." Por tanto, en la evolución del sistema no sólo cuenta con las administraciones implicadas, sino también con los colectivos profesionales afectados, en concreto con todos los operadores jurídicos y aquellos agentes externos que aunque no tienen interlocución directa con la Justicia, aportan documentos necesarios para el desarrollo del proceso.

Todo esto en un entorno tecnológico que garantiza la seguridad del intercambio de comunicaciones. El núcleo básico del sistema comprende la utilización de la firma digital que garantiza la autenticidad e integridad de los documentos intercambiados, pero se han añadido también a LexNET los servicios de sellado de tiempo y de custodia de documentos, lo que determina la imposibilidad del repudio de la comunicación tanto en su contenido como en el tiempo de la recepción. Por otra parte la arquitectura se ha asegurado para que el servicio se preste en unas condiciones de alta disponibilidad, cerrando con ello el ciclo de la seguridad.

El sistema opera en los dos sentidos:

a) Notificación telemática. Incluyendo características específicas de la problemática de justicia: por ejemplo la gestión del "salón virtual de procuradores" y exigencias legales como la elaboración de la diligencia de presentación firmada electrónicamente por el secretario judicial del juzgado.

b) Presentación de demandas y escritos de trámite. Incluyendo también algunas características específicas: El traslado de copias para procuradores: Procedimiento muy agilizado y simplificado, al eliminar el papel circulante y la necesidad de cotejo, gracias a la utilización de los medios telemáticos y la firma electrónica.

Se enfrenta la problemática específica de la Justicia desde la electrónica a través de un abanico de acciones simultáneas que, mediante una estrategia de aproximación sucesiva, permiten minimizar el impacto organizativo a la vez que se consigue el objetivo buscado:

a. La firma digital con que se dota a los secretarios judiciales, con la que se incorpora la característica de la fe pública judicial a la comunicación telemática de las actuaciones de los tribunales.

---

(25) Ver: http://www.eiusabogados.com/portadas/File/Temasdehoy52007.

b. Un proceso interactivo de construcción del sistema gracias al cual se ha incorporado en un primer momento la notificación, luego la presentación de escritos y finalmente la presentación de demandas, para a continuación abordar el problema de los documentos originales electrónicos que se aportan al proceso. Se avanza así en el proyecto mientras los implicados se familiarizan con el funcionamiento del sistema sin impactar en su propia organización. Se es sensible de esta forma a las necesidades particulares.

c. La incorporación gradual de colectivos al proceso mediante el establecimiento de convenios con los mismos para sincronizar el sistema con la casuística de cada uno, a la vez que les anima a esforzarse y avanzar en la misma línea en tanto que es beneficiosa para todos ellos. En esta línea por el lado de la Justicia se han incorporado Secretarios Judiciales y el Cuerpo de Gestión Procesal, para más adelante contar con el resto de los cuerpos de funcionarios afectados. Por el lado de los profesionales se trabaja con procuradores y abogados y se han iniciado contactos con otros colectivos como cuerpo de letrados de la Seguridad Social.

d. La aproximación tecnológica al problema. Cada interlocutor se incorpora al servicio con una funcionalidad completa pero con la tecnología de que dispone en ese momento aunque ésta sea muy básica, tales como una PC con navegador, una conexión a internet tipo ADSL o similar y una tarjeta criptográfica. Incluso en el caso en que el colectivo en cuestión no disponga de la capacidad de emitir certificados, le serán otorgados por el propio Ministerio en virtud del convenio que tiene suscrito con la FNMT junto con las facilidades de gestión de los mismos en su "rama" correspondiente del "directorio LDAP de Justicia". Posteriormente el interlocutor podrá evolucionar hacia un escenario en que sus aplicaciones de gestión de despacho "hablen" directamente con LexNET mediante web-services, beneficiándose de la sinergia que proporcionará este mecanismo del mismo modo que ya lo hace en la integración de LexNET con las distintas aplicaciones de gestión procesal de los juzgados.

I.2.b. Estados Unidos — El caso Virginia: (26)

En el caso de los Estados Unidos se ha tomado emblemáticamente la situación de los Tribunales estaduales de Virginia, paradigmáticos en lo que respecta a la informatización del Poder Judicial.

Partiendo de la base que la tecnología mejorará las posibilidades de acceso y facilidad del sistema judicial, lo que optimizará su calidad, se concluyó en

(26) Ver: http://www.reformajudicial.jus.gov.ar/materiales/documentos/VIRGINIA.
ERG.doc

la conveniencia de implementar un plan de informatización de largo alcance para el Poder Judicial, en el que se propusieron las siguientes metas:

a) Desarrollar un subsistema de gestión judicial para: 1) expandir el número de tribunales en el Sistema de Información Automatizada de Cortes (Courts Automated Information System, CAIS); 2) proveer la automatización de las oficinas judiciales,, mediante el uso de computadoras personales y redes locales de trabajo; 3) agregar otras dieciséis cortes de circuito en el sistema de registros informáticos con índices; y, 4) desarrollar mejoras de este sistema para obtener la capacidad de reproducción de imágenes.

b) Expandir la apertura y facilidades de los tribunales, mediante un continuo mejoramiento del Sistema de Acceso Público a la Jurisprudencia (Law Office Public Access System, LOPAS).

c) Realizar una evaluación de los medios más apropiados para minimizar la cantidad de tiempo de archivo de los registros públicos en los tribunales.

d) Estudiar una legislación que contemple la posibilidad de obtener copias electrónicas autenticadas como si fueran originales.

e) Fomentar la decisión de reducir los requerimientos para el ingreso de información en los tribunales y otras oficinas, estableciendo un sistema efectivo de interfases para que contenga datos uniformes que puedan ser transmitidos mediante sistemas automatizados.

f) Proveer un intercambio de información electrónica de bajo costo entre los tribunales y otras oficinas vinculadas con el sistema judicial, para fortalecer y expandir las comunicaciones con el Registro de la Propiedad Automotor, el Registro de Reincidencia y Estadística, la Policía del Estado y los Consejos del Menor y la Familia y un Bureau de Apoyo Reforzado, de tal forma que los resúmenes de las resoluciones de los tribunales puedan ser transmitidos de una manera precisa y eficiente.

g) Desarrollar mecanismos por los cuales los tribunales, de juicio y de apelación, estén conectados por un intercambio electrónico y puedan disponer de la información necesaria.

h) Expandir el empleo de grabaciones de video como un medio de registro de lo que sucede en los tribunales, como pruebas piloto para la evaluación del Consejo Judicial.

i) Estudiar la factibilidad de desarrollar un proyecto piloto para adoptar un sistema de video que conecte la sede del tribunal y una prisión.

j) Extender la automatización de la oficina judicial para posibilitar las investigaciones de los jueces y sus funcionarios, mediante el uso de computadoras personales y redes locales.

k) Asegurar que exista un sistema adecuado de respaldo de los registros para todos los sistemas informáticos, en caso de emergencia.

l) Ampliar el sistema informático para permitir: 1) la promoción de demandas por medios electrónicos desde lugares lejanos; 2) una colección de archivos sobre litigios; y, 3) proporcionar noticias, resúmenes y otros documentos que se generan automáticamente sobre la base de la información con la que se inicia la causa.

m) Determinar la factibilidad de desarrollar un sistema automático de monitoreo, que haga un seguimiento de la conducta de las partes que intervienen en los tribunales en casos de abuso de menores y maltrato familiar.

I.2.c. Brasil: (27)

Respecto a la informatización de la justicia brasileña, deben tenerse en cuenta factores específicos, como la dimensión territorial del país, verdaderamente continental.

Tomaremos como punto de referencia al Supremo Tribunal de Justicia (en adelante STJ), que más o menos refleja el grado de informatización alcanzado.

a. Tecnología de la información - Estructura:

Actualmente el STJ cuenta con una red de teleinformática que interconecta las seis unidades de su complejo de edificios, alcanzando aproximadamente 5 km de cables de fibra óptica. En esa red están conectadas más o menos 2.200 microcomputadores (estaciones de trabajo), todos ellos con acceso a los computadores centrales (servidores) que suministran los diversos servicios para el área fin y también el área administrativa del Tribunal. En el segmento del área fin se destaca el concepto de oficina virtual que es una facilidad ofertada a los ministros del Tribunal, los cuales realizan muchos de sus trabajos aún cuando de encuentren distantes del Tribunal.

b. Sistema para seguir el curso del proceso:

Ese sistema abarca todo el movimiento del proceso del tribunal, desde el momento en que se da entrada al proceso o causa, hasta el momento en que se archiva o se devuelve a su origen. Por medio de este sistema disponible para uso interno y para consulta vía Internet por los interesados, se puede seguir toda la marcha y situación instantánea de cada proceso en el STJ.

c. Sistema Push:

Es una facilidad disponible a cualquier ciudadano que tenga interés acreditado en un proceso catastrado en la base de datos del sistema para seguir el

(27) Ver: http://www.stj.gov.br/Discursos/0001119/LA%20INFORMATIZACI%C3%93N%20EM%20EL%20PODER%20JUDICIAL%20BRASILE%C3%91O.doc

curso del proceso. A partir del catastro del e-mail, y de los números de procesos, de su interés, la persona pasará a recibir, automáticamente, en la dirección electrónica catastrada, cualquier movimentación que haya sido dada al proceso, posibilitando que pueda ser seguido paso a paso, por el interesado.

d. Sistema Push OAB:

Pone a disposición de la Orden de Abogados el mismo servicio que el Sistema Push convencional, con una ventaja adicional para los abogados a partir de la vinculación automática de su número de inscripción en la Orden, con los respectivos procesos en que su número esté catastrado. De esa forma, automáticamente, el abogado pasa a recibir informaciones en su e-mail sobre el curso de los procesos en los cuales tenga participación, sin necesidad de catastrarse individualmente cada uno.

e. Sistema Push corporativo:

Es una facilidad implementada a través de convenio con determinados órganos que poseen un cuantitativo muy grande de procesos en el STJ y actualmente está en funcionamiento para la Caixa Económica Federal, la Abogacía General de la Unión y el Instituto Nacional de Seguridad Social. De forma similar a los servicios Push ya citados, tiene por finalidad encaminar o dirigir, al final de cada día la marcha de todos los procesos que están en el STJ y en los cuales la entidad convenida es parte interesada.

f. Revista electrónica:

Permite consultar por entero el tenor de los acuerdos publicados, en formato texto, lo que posibilita la manipulación del contenido de las decisiones colegiadas en fundamentaciones, libros, citas etc. Facilita al ciudadano la recolección de datos, dispensándolo de obtener en las dependencias del Tribunal, las copias registradas de las sentencias registradas que se desea, pues la página Internet que exhibe el contenido de la sentencia es certificada digitalmente.

La página de Jurisprudencia del STJ brinda a los consultantes el resumen de las decisiones colegiadas, cuyo contenido constituye un facilitador de investigación y consulta para los interesados. El contenido del resumen, lo prepara una secretaria especializada, tratando de facilitar la búsqueda a los abogados, con el fin de poder abarcar las decisiones, ampliando su alcance más allá de su propio contenido textual, pero sin ampliación de lo que abarca.

Además de eso, cuenta con una página sobre la Jurisprudencia Comparada del STJ, es un servicio agregado, ofertando a la investigación y consulta de temas objeto de decisiones diferenciadas.

g. Informativo de jurisprudencia:

Es una publicación semanal de las principales decisiones tomadas por los órganos juzgadores del STJ, con la finalidad de dar publicidad inmediata a los

asuntos relevantes, antes aún de la publicación de las sentencias, sin embargo ya sirve como punto orientador para el futuro.

h. Valija digital:

Es un servicio de intercambio de informaciones, complementado, a partir de una idea victoriosa presentada por un técnico del tribunal, en concurso interno para descubrir talentos e ideas innovadoras. El propósito es promover el intercambio de informaciones entre tribunales de diversos niveles, que tienen trámite de procesos entre si a partir de la transferencia de informaciones a través de recursos de teleinformática, se abrevia el tiempo de transferencia de datos que ya se encuentran en determinado tribunal y que deberían volverse a tipear nuevamente en el otro, cuando hay transferencia de proceso entre ellos. De este modo se evita volver a tipear las informaciones que ya han sido catastradas en el tribunal de origen, que está enviando una causa o proceso para otro tribunal.

i. Indice del abogado en el Diario de Justicia:

Es una publicación impresa de las decisiones del STJ en el Diario de la Justicia. Este índice permite que los abogados tengan una referencia cruzada en las publicaciones del Tribunal, indicando, en un único lugar, la página del Diario en que determinado abogado figura en aquella publicación, facilitando de este modo la búsqueda de los asuntos de su interés en las páginas del diario oficial.

j. Informatización en el 1º y 2º grados:

Se está desarrollando más lentamente que en los tribunales superiores. Los tribunales regionales superiores. Los tribunales regionales federales ya están interconectados mediante una red privada de comunicación de datos al STJ. Algunos tribunales de los estados brevemente también estarán conectados, inclusive al Supremo. Los tribunales de 2º grado ya cuentan con Internet, así como los superiores, y algunos de ellos ya están conectados a diversas comarcas.

Casi todos tienen su sitio en la Internet, de los cuales se valen los abogados y otros interesados para recoger información sobre el trámite del proceso.

k. Futuro próximo:

Documentos electrónicos:

Actualmente los tribunales aceptan peticiones que le solicitan vía fax, desde que le original llegue hasta, cinco días después. En un futuro próximo, se espera adoptar el uso de medios completamente digitales, para la transferencia de esos datos, dispensándose el uso casi por completo del papel.

Proceso digital (o electrónico):

Se está tramitando en el Congreso Nacional un Proyecto de Ley que permita la utilización de los avances tecnológicos ya disponibles a los jueces de

diversas instancias y también a la sociedad en general, para instrucción y tramitación de procesos judiciales. Con esto, al lado de mayor agilidad, habrá disminución de costos de los procesos. El STJ se está preparando para esto, está adquiriendo equipamientos y está dotándose de tecnología que asegure la privacidad, seguridad y autenticidad de las informaciones transferidas para ese proceso.

I.2.d. Uruguay: (28)

Los aspectos negativos más mencionados en los diagnósticos de los sistemas de administración de justicia en la República Oriental del Uruguay y Latinoamérica han sido: lentitud, incertidumbre, la excesiva complejidad, inaccesibilidad y una relación muy alta costo-beneficio.

Por otra parte, las soluciones propuestas pasan casi siempre por aumentar el número de jueces y funcionarios, equipamiento y nuevos códigos. Frecuentemente, se piensa que estas medidas producirán automáticamente los resultados esperados. Mientras tanto el tamaño y la estructura del Poder Judicial crece irracionalmente, creándose nuevos conflictos y nuevas dificultades.

Sin embargo, gran parte de los problemas tienen su raíz en los modelos existentes sobre la gestión y el manejo de casos. Muchos de los cambios que pueden resolver estos problemas podrían ser generados desde el interior del Poder Judicial sin aumentar sustancialmente el presupuesto ni recurrir a reformas legislativas. Para poder diseñar cambios desde el interior resulta necesario disponer de información básica y estadística que pueda ser analizada conjuntamente con jueces y funcionarios y contrastada con las experiencias realizadas en otras jurisdicciones.

El Poder Judicial debería idear medios para analizar constantemente su funcionamiento y buscar la manera de perfeccionarlo, al mismo tiempo que imparte justicia.

Aumentar la productividad y la eficiencia supone la redefinición de cada una de las tareas, eliminar pasos innecesarios y poner a disposición de la administración de justicia tecnologías que son cada día más accesibles.

También resulta necesario mejorar los mecanismos de control, agilizar los trámites y facilitar las comunicaciones.

La reforma de la administración de justicia supone, en muchas ocasiones, cambiar el rol del juez en el proceso. Estos cambios surgen por lo general de las

---

(28) En este análisis se sigue el informe "Gestión judicial y reforma de la administración de justicia en América Latina" elaborado por Carlos G. Gregorio, publicado por el Banco Interamericano de Desarrollo, Washington, D.C., Departamento de Desarrollo Sostenible, División de Estado, Gobernabilidad y Sociedad Civil, Mayo 19-22 de 1966. En el mismo se formula un relevamiento y diagnóstico no sólo de Uruguay, sino de Latinoamérica en general más allá del énfasis puesto en la propuesta uruguaya .Ver: http://www.iadb.org

nuevas normas procesales, pero en algunos casos es posible también cambiar la frecuencia, intensidad, impacto y forma de intervención de los jueces, modificando algunas pautas sobre el manejo de los casos y el flujo de la información en la oficina judicial, y lograr con ello un mayor control del proceso.

En este campo, los propósitos concretos de la reforma judicial en la República Oriental del Uruguay apuntan a reducir el retraso y el congestionamiento; mejorar la gestión y seguimiento de casos; identificar los problemas o tipos de casos que se presentan con mayor frecuencia para lograr procedimientos especiales o automatizados para ellos.

Para atender a estos problemas y en lo que hace a la gestión y seguimiento de casos, los proyectos de reforma se concentraron en la informatización de los juzgados además de atender a los siguientes ítems:

a) Congestionamiento

Las soluciones a los problemas del congestionamiento del sistema judicial pasan en general por un conjunto coordinado de medidas tendientes a: 1) favorecer la resolución alternativa de conflictos, alejando así del sistema los casos que pueden ser resueltos sin la intervención de un juez; 2) reformas procesales, atendiendo así a buscar procedimientos más rápidos y transparentes, 3) reformas administrativas, y; 4) implementación de nuevas tecnologías aplicadas a los procesos judiciales.

b) Reducción de los retrasos

La duración del proceso es únicamente vista como un indicador de la eficiencia del sistema de administración de justicia. Sin embargo en muchos casos los retrasos se tornan inadmisibles y pueden llegar a impedir la obtención de una solución justa al conflicto.

La mayoría de las acciones en la región para reducir retrasos se han dirigido a la modificación de las normas procesales y a la utilización de servicios digitales tales como las notificaciones electrónicas entre jueces de grado.

c) Accesibilidad de la información judicial

Los sistemas de información deberían permitir a los abogados patrocinantes, defensores oficiales, fiscales, etc., consultar la información correspondiente a sus causas, para tomar conocimiento en forma directa de la etapa en la que se encuentran, conectándose ellos mismos con la base de datos que contiene la información.

Una gran cantidad de necesidades de información será satisfecha así sin la intervención de personal, optimizando el uso de tiempo y espacio.

Los sistemas actualmente en funcionamiento en Uruguay, tienden a que los abogados realicen la consulta de sus causas desde sus propios estudios, mediante un sistema de comunicaciones externas al sistema de información judicial, para tener así acceso “en forma parcial” a la información requerida.

d) Mejoras en las estadísticas judiciales

Las estadísticas judiciales revisten un papel fundamental para el diseño y optimización de los sistemas de gestión y seguimiento de casos. En los últimos años la calidad de la información estadística sobre la administración de justicia ha mejorado significativamente en América Latina.

Sin embargo no parece haberse tomado ventaja del proceso de informatización para incrementar la calidad de los datos y su uso en la toma de decisiones. La mayoría de los datos que se obtienen, y en particular los que se publican, son descriptivos de la carga de casos. En este sentido parece necesario darle un nuevo impulso a los sistemas de gestión y seguimiento de casos para obtener información básica global, que quizás no sea relevante para las tareas del juzgado, pero que resultará de fundamental importancia para realizar estudios tendientes a optimizar los procedimientos administrativos.

El nivel actual alcanzado por las estadísticas sobre administración de justicia en Costa Rica parece ser uno de los buenos ejemplos sobre la forma en que el Poder Judicial debe informar a la comunidad sobre su funcionamiento.

e) Características de los sistemas de información

Uno de los procesos de reforma de la administración de justicia consiste en el reemplazo de los sistemas de registro manuales por sistemas computarizados de manejo de la información. En casi todos los países de la región este proceso ha sido gradual.

Los procesos de informatización de la administración de justicia han comenzado por la producción de sentencias (procesador de texto), seguido por los mecanismos de registro y seguimiento de casos que reemplazaron las fichas y los libros del juzgado.

En casi todos los países de la región existen procesos de informatización.

Hoy, como corolario de estas experiencias, los objetivos primarios de estos sistemas apuntan a proporcionar información para facilitar la toma de decisiones, tanto por parte del juez y sus colaboradores, como por las partes, sus abogados o cualquier otra persona que intervenga en un proceso, permitir la generación de información básica para el análisis estadístico, evaluación, racionalización, optimización del sistema y para la toma de decisiones por parte de quienes dirigen el sistema de administración de justicia y definen la política judicial.

f) Finalidad y calidad de la información

La información que se origina o procesa judicialmente puede tener diferente entidad y valor. Sin embargo la información que normalmente es incluida en los sistemas de información podría clasificarse en los siguientes niveles:

1) Estadístico: cuando los datos se incluyen en un sistema de información para ser utilizados en la realización de estadísticas, investigación o monitoreo; entonces no es necesario identificar el nombre de las partes (quizás con la excepción del propio Estado o partes que mantienen múltiples casos). La consecuencia más importante es que la información que sólo se incluye a estos fines puede ampararse en el secreto estadístico.

2) Referencial: la información contenida en el sistema facilita el acceso a los datos o el proceso de identificación de documentos a personas autorizadas para la gestión.

3) Documental: la información que tiene valor documental habilita para la toma racional de decisiones. Si las partes, por ejemplo, pueden informarse sobre una decisión del juez o una notificación por medio de una consulta al sistema de información, ese dato debe tener valor documental. En todos los datos clasificados como documentales debe garantizarse que la información no pueda ser modificada o, en su caso, deberá dejar rastros sobre cual era el contenido anterior, quién los modificó y cuándo.

4) Registral: la característica más importante es que la inclusión de un dato en el registro produce efectos legales.

En el proceso de planificación resulta necesario establecer qué alcance (estadístico, referencial, documental, registral) tendrá cada unidad de información o dato en cada sistema de información, cuál será su evolución en el futuro y qué flujos de información se definen con otros sistemas de información, ahora y en el futuro.

Este aspecto, quizás será relevante en los futuros desarrollos o en la revisión de las versiones actuales de los sistemas de información. Probablemente deberá insistirse en realizar "o profundizarla, si ya se realizó" una cuidadosa evaluación de necesidades de información.

En muchos sistemas desarrollados en la región, en particular durante las etapas iniciales, es posible señalar que la inclusión o no de la información no surgió de un proceso de identificación de necesidades y que no se establecieron la finalidad ni los estándares mínimos de calidad para cada dato.

También se ha generalizado el uso de campos literales en detrimento de los codificados y, en algunos casos, se ha dejado libertad a cada juzgado para establecer sus propias tablas de códigos. No tomar precauciones en este sentido se traduce en una menor calidad de la información que, si bien no afecta en principio la labor del juzgado, se toma relevante cuando en etapas futuras, los datos informatizados son utilizados para elaborar estudios globales y analizar el funcionamiento del sistema judicial en su totalidad.

La información de fuente judicial interviene en las pautas decisorias de muchas personas, pudiendo los incrementos de su calidad y accesibilidad modificarlas radicalmente. Por otra parte algunos sistemas de información

pueden tener por finalidad optimizar o apoyar algún tipo particular de casos ya sea para la gestión diferencial o aportando información de contexto.

g) Distribución de casos

En muchos casos la instalación de sistemas computarizados de información permite administrar la distribución y asignación de causas entre los juzgados en forma aleatoria y equitativa, de acuerdo con la dificultad y urgencia con que deben resolverse (v.gr. acción de amparo).

Un hecho importante asociado a los sistemas automatizados de distribución de causas es el contar con tablas de codificación de objetos de litigio, materias, tipo de caso, objeto del proceso (recogiendo la sinonimia utilizada en algunos países de la región). La clasificación preliminar del caso es propuesta por el abogado que presenta la demanda, lo que permite un control más eficiente de los casos iniciados e intentar una distribución más homogénea de las causas.

Es necesario revisar periódicamente estas tablas de opciones, teniendo en cuenta los requerimientos de los estudios estadísticos y de los sistemas de información. Es conveniente calcular las frecuencias de aparición en los últimos años de cada una de las opciones para analizar las ventajas de suprimir, agregar o distinguir nuevas opciones, con criterios estadísticos o jurídicos.

Los sistemas de distribución permiten generar archivos comunes a todos los juzgados o tribunales de apelaciones de una misma materia. Sólo en algunos casos están conectados en red con los sistemas de gestión de los juzgados, lo que permite un control más efectivo y hace posible identificar los casos relacionados.

h) Gestión y seguimiento de casos

Existen en la región varios sistemas en uso, algunos fueron desarrollados por los equipos técnicos del Poder Judicial y otros por empresas o consultores externos. En todos los casos se presentó como favorable un control y seguimiento directo de los proyectos por parte de las autoridades del Poder Judicial.

En el Uruguay se usa un sistema desarrollado por el Centro de Cómputos del Poder Judicial. Actualmente está en uso en los juzgados civiles, laborales, de familia y contencioso administrativo de Montevideo, y en los juzgados de jurisdicción múltiple (no penal) de las ciudades de Las Piedras, Maldonado, Pando, Paysandú y Salto.

Los primeros sistemas de gestión que se desarrollaron en la región para funcionar con códigos procesales con procedimientos escritos estuvieron dirigidos a saber dónde estaba el expediente ya facilitar la redacción de la sentencia (procesadores de textos).

Por su parte, si la actividad procesal se concentra en las audiencias orales, los sistemas de gestión apuntarán más al manejo del calendario y de la agenda.

Si bien estas fueron las primeras necesidades identificadas, hoy la experiencia acumulada en el uso de la tecnología informática indica que el sistema de gestión es una herramienta fundamental para mejorar el control efectivo de la marcha del proceso por parte del juez y sus colaboradores.

De acuerdo con las experiencias desarrolladas, el sistema de gestión puede implementarse con diferentes niveles de compromiso con las normas de procedimientos. En algunos casos, se ha intentado producir un sistema de gestión que pueda adaptarse prácticamente a un cualquier tipo de código de procedimientos; en otros casos, el sistema se ha desarrollado ad hoc para un código en particular.

La búsqueda de una alternativa intermedia deja librado al usuario la inclusión de información vinculada con las normas procesales; en esta modalidad, por ejemplo, los pasos o etapas procesales son incluidos como tablas modificables por el usuario. Sin una adecuada coordinación, esta forma de trabajo tiende a generar información no comparable.

Se ha observado que el sistema de gestión puede tener cierta inercia o podría introducir procedimientos por vía no legislativa que, en algunos casos, ha mantenido vivos institutos o procedimientos derogados cuando se reforma un código procesal. Es conveniente diferenciar claramente, cuando se planifica la inclusión de cada dato, tabla o calificación, si se adecua fielmente a las normas procesales en vigencia. No todas las normas procesales deben ser motivo de referencia o registro en el sistema, sino sólo aquéllas identificadas como necesarias. El desarrollo de esta actividad requiere la participación de un grupo de especialistas en procedimientos judiciales, en administración de justicia e informática.

Tanto el diseño como las modificaciones al sistema de gestión y seguimiento de casos deberían responder a necesidades identificadas previamente.

Si se toma como referencia la estructura de los sistemas de gestión existentes en la región, en principio, el sistema las características básicas incluyen:

a. un sistema de identificación del caso, único para todo el Poder Judicial;

b. mantener en lo posible una interfase visual y lenguaje uniforme para todos los tipos de juzgado, procesos y casos, las distintas versiones deberían tener un mismo patrón lógico.

c. ser flexible, para ser adaptable a nuevas modalidades;

d. funcionar con adecuada vinculación al código procesal en vigencia.

e. reemplazar los sistemas de registro (libros o fichas) del movimiento de las causas;

f. incluir sub-sistemas para la gestión diferencial para algunos tipos de caso;

g. disponer de índices que faciliten el acceso, a parte o a toda la información sobre el caso, por diferentes entradas (el procedimiento debería incluir búsquedas alfafonéticas). La información recuperada debería ser accesible para su modificación;

h. incluir aplicaciones para realizar las funciones de registro de pasos y etapas procesales, citaciones, fianzas, detenciones, cambios en las partes intervinientes, efectos incautados, cálculo de tasas judiciales, honorarios, etc.;

i. registrar fechas y tiempos de todas las intervenciones;

j. incluir aplicaciones específicas para los procedimientos orales, en particular para el manejo de la agenda del juzgado. El sistema debe incluir un calendario y la posibilidad de conocer, registrar los eventos programados para cada día y la duración estimada de cada uno de ellos;

k. cuando sea posible, incluir elementos de automatización;

l. contener un procesador específico de textos y utilitarios para generar documentos-tipo, correspondencia de rutina, insertar citas de jurisprudencia o los nombres de las personas involucradas accediendo a las bases de datos, usar diccionarios, proteger los nombres de los menores, etc.;

m. alertar automáticamente al asesor de menores sobre la presencia de menores en un caso, para la defensa de sus intereses;

n. asistir al juez y sus colaboradores, integrantes de la oficina judicial, en la programación de audiencias durante un determinado período;

o. utilizar tablas de referencias internas y tablas de opciones modificables;

p. contener información sobre calendarios (feriados), disponibilidad y reserva salas de audiencias;

q. utilitarios para ordenar los datos por fecha, alfabéticamente o numéricamente;

r. seleccionar datos mediante operadores boleanos;

s. realizar operaciones aritméticas, etc.;

t. producir varios tipos de informes estadísticos internos del juzgado (casos en trámite e iniciados, en el juzgado, en el fuero, el año anterior, retrasos, mes por mes, casos más antiguos, etc.), y presentarlos conjuntamente con los indicadores globales del mismo tipo de juzgado.

i) Privacidad e información judicial

Los procesos de informatización de la administración de justicia han comenzado por el apoyo en la producción de sentencias (procesadores de texto), seguido por mecanismos de seguimiento de casos que reemplazaron las fichas o libros del juzgado.

En la medida que los sistemas de información crecen y se perfeccionan, se generan bases de datos centrales para todos los juzgados de un mismo tipo en una jurisdicción.

Por otra parte la administración de justicia debe ser transparente, la publicidad de las actuaciones y de las decisiones es uno de los pilares del sistema y el conocimiento de los precedentes es lo que permite el respeto del principio de igualdad ante la justicia.

Los incrementos en la accesibilidad, consecuencia de los sistemas centralizados de información judicial, han dado lugar a nuevos requerimientos. Por ejemplo en la justicia laboral se reciben pedidos de empresas que seleccionan personal interesadas en conocer la existencia de demandas laborales iniciadas por un potencial candidato a cubrir un puesto.

Ciertamente se intenta predecir la conducta futura, pensando que quien ejerció sus derechos en el pasado no temerá iniciar nuevas acciones en el futuro.

Atento, pues, a la disparidad de criterios existentes con respecto publicidad de la información recogida en las actuaciones judiciales y ante la certeza de que tanto el volumen como las facilidades de acceso seguirán creciendo, mientras, que la demanda de información, con o sin interés legítimo, irá también en aumento, se considera altamente recomendable preparar legislación que contemple las situaciones anotadas y, fundamentalmente, defina principios generales aplicables durante el proceso de desarrollo de los sistemas informáticos del Poder Judicial.

Esta legislación debería ser compatible y complementarse con las normas que determine los alcances del habeas data, puesto que, en principio, la publicidad rige toda información que maneja la administración pública. Con todo, deberían establecerse lineamientos que atiendan al ciudadano en su situación de indefensión frente al uso que de esa información pueda hacerse. Será necesario, pues, establecer límites en los procesos de recolección de datos mediante normas sustantivas que exijan la identificación previa de la necesidad de contar con el dato y su finalidad de uso, así como quiénes podrán requerir tal información.

La creación de sistemas de procesamiento de datos debería ser transparente y accesible a todos los usuarios. Es necesario que las agencias gubernamentales que trabajen con bancos de datos tengan contactos con instituciones independientes y organizaciones no gubernamentales que ofrezcan el servicio de sus expertos y representen la opinión de sectores específicos. Se debería estudiar, como análisis de riesgo, los efectos y consecuencias que los sistemas de procesamiento de datos puedan producir en la sociedad.

La legislación debería evitar que la información almacenada genere o permita cualquier forma de discriminación o preconcepto, por ejemplo mediante la recopilación y conservación de datos sobre creencias religiosas, opiniones políticas, actitudes sexuales, origen étnico, discapacidad, etc.

A su vez, se deberían identificar y estipular los plazos en que el mantenimiento de los datos fuera necesario, definiendo los procedimientos mediante los cuales serán eliminados. La publicidad no protege la indiscriminada divulgación de los datos, ni significa convertir a la administración pública en un servicio de informes. La legislación debería establecer en qué casos la información referente a un individuo puede ser proporcionada a terceros.

Resultan necesarias, pues, decisiones adecuadas este área, sea abriendo la información del Poder Judicial a cualquier usuario y admitiendo el recurso individual de reserva de la información, o, por el contrario, restringiendo el acceso solamente a quienes ostenten un interés legítimo debidamente acreditado.

Las definiciones en este campo son un requerimiento sustancial para el desarrollo y la eficacia de los sistemas de información judicial, así como de los servicios públicos de información y de los registros nacionales, y, en especial, de los sistemas de información estadística.

De acuerdo con los antecedentes expuestos, el diseño de los sistemas de información del Poder Judicial debería "mientras no existan normas o políticas explícitas" buscar de no romper el equilibrio entre él:

1) principio de publicidad de las actuaciones y decisiones de la justicia; y las más recientes tendencias sobre la protección de datos personales

2) principio de finalidad (los datos se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades);

3) principio de proporcionalidad (los datos deben ser adecuados, pertinentes y no excesivos);

4) los datos se obtendrán y tratarán leal y legítimamente;

5) derecho de acceso a la información (antes de iniciarse cualquier tratamiento informático, y definir qué datos personales y cómo dichos datos van a ser tratados, transmitidos y transferidos a otras personas);

6) derecho a saber a quien se han transferido sus datos personales;

7) derecho de oponerse por motivos legítimos a que los datos sean objeto de tratamiento informático; derecho de rectificación;

8) acciones específicas para la garantía del habeas data;

9) cancelación de los registros cuando hayan dejado de ser necesarios o pertinentes para su finalidad(secreto estadístico)

10) existencia de una autoridad de protección de datos personales.

II. El aporte de la ley 22.172 sobre comunicaciones entre jueces de distinta jurisdicción

El tratamiento del tema nos exige una primera precisión. Con frecuencia se invocan los artículos del convenio que aprueba la citada ley, como correspondientes a la misma. Así se los cita en sentencias y en doctrina.

En rigor la Ley 22.172 cuenta con seis artículos destinados a aprobar el convenio celebrado entre la Nación y las Provincias que sucesivamente adhieran.

La normativa procesal importante está contenida en ese convenio que se denomina de Comunicación entre Tribunales de la República con su articulado del primero al catorce.

Su aporte fue valioso. Hoy me toca reprocharle morosidad al trámite previsto en la norma. Pero debo reconocer, que, ayer, como litigante, usé con alivio el benéfico efecto que creara, al despejar formalismos anteriores, y dando agilidad a la tramitación, tanto en el diligenciamiento de oficios entre jueces de distinta jurisdicción, como el cumplimiento directo en otra jurisdicción de medidas ordenadas por un juez extraño a aquella.

La homogeneidad que aportó despejó el cuello de botella que generaba el debido respeto a la diversidad procesal propia de nuestro sistema, y sus innovaciones derivaron en una agilidad destacable para su tiempo.

La mayoría de sus exigencias se mantienen vigorosas, desde que, su práctica ha sido en general pacífica en sus ámbitos de aplicación. Sin perjuicio de las mejoras que pudieran proponerse desde el ámbito procesal

Pero al legislador, al tiempo de su génesis, no le era posible barruntar el aluvión tecnológico que se avecinaba. Sus previsiones fueron para el soporte papel, que debidamente foliado y sellado debe trasladarse materialmente desde la sede física de su emisor hasta su destinatario.

A veces largas distancias con las consecuentes dilaciones. Aún en las cortas se pone en evidencia la declinación de aquella forma. Me ha tocado conocer la demora de dos días en restituir la libertad de un ser humano, como consecuencia de la necesidad de confección de un oficio en soporte papel por parte de un Tribunal. El destinatario se encontraba pasillo de por medio.

Esta propuesta no modifica los aspectos procesales del Convenio de Comunicación entre Tribunales de la República que aprobara la Ley 22.172, aunque, como dije, sin duda habrá muchas mejoras que podrán sugerirse a su andamiaje. Tan sólo en su contexto, se habilita que esa comunicación en-

tre jueces de la República, o disposiciones de alguno de ellos a cumplirse en extraña jurisdicción, pueda llevarse a cabo con la celeridad e inmediatez que la evolución tecnológica habida en el mundo ha puesto a nuestro alcance, y que de hecho usamos cotidianamente en nuestras vidas.

III. Anteproyecto de ley de comunicación interjurisdiccional electrónica

Preliminar

Es sobreabundante diagnosticar genéricamente, sobre tantas falencias que se imputan a la Justicia Argentina, que por otro lado, en algunos aspectos tienen analogía con muchos de los países del mundo, aunque, lamentablemente para nosotros, en forma paralela, vemos la distancia con casos puntuales —y algunos muy cercanos— de países en los que se observa una planificación y estrategia destinada a enfrentar tales déficit. A título de ejemplo en la materia específica: en el año 1997, cuando me tocaba presidir la Justicia santiagueña, diseñamos una visita de los magistrados del poder judicial santiagueño a la hermana República de Brasil, y en la misma tuvieron oportunidad de participar en jornadas de capacitación en Porto Alegre; ya entonces (reitero que hablamos de 1997) pudieron presenciar la recepción de audiencias a distancia mediante video conferencias.

Como dije antes, ha sido mucho y muy valioso el esfuerzo realizado por los integrantes de la Junta Federal de Cortes y Superiores Tribunales de la República Argentina (JU.FE.JUS.), en la tarea de capacitación, sembrando centros o ayudando a hacerlo en cada provincia, y en lo específico, coordinando la labor y emprendimientos informáticos, encarados por cada Poder Judicial, muchas veces con magros recursos.

Es gracias a ese organismo que se celebran como se dijo las Primeras y Segundas Jornadas Informáticas de Ministros y de Técnicos del área. La primera de ellas en Termas de Río Hondo y la segunda en Santiago del Estero. Parece indudable el embrión federal, cuyo espíritu, está ínsito en la mencionada Junta.

Desde allí nace el Foro Permanente de los Técnicos Informáticos, que continuaron trabajando en coordinación, y que gracias al valioso aporte del equipo de funcionarios y colaboradores del Ministerio de Justicia de la Nación, sentaran las bases para la celebración del Convenio de Comunicación Interjurisdiccional Electrónica que antes he reseñado, y al que se glosara el Protocolo Técnico respectivo (sus textos obran completos en anexos).

En el mismo se insinúa la necesidad de complementar la Ley 22.172. Tal la terminología usada, quizás imbuidos del principio de operatividad de las normas (en este caso la Ley de Firma Digital), y ansiosos de buscar el plausible objetivo de celeridad mediante el uso de las nuevas herramientas tecnológicas, se esbozó en el convenio la posibilidad de que los jueces se comunicaran formal y procesalmente, con salvedades obviamente, mediante la vía electrónica y el uso de la firma digital.

Las excepciones hablaban, ya entonces, de modo elocuente, de la necesidad de abordar el tema desde la legislación, y para ello modificar la Ley 22.172, que regula el sistema de comunicación entre los jueces argentinos. Es el camino adecuado, más allá del elevado espíritu, en el que cabalgáramos a quienes nos tocó suscribir el referido convenio. Lo correcto jurídicamente para habilitar procesalmente la cuestión, despejando las posibilidades de nulidades y planteos de inconstitucionalidad, es a mí entender, abordarla desde lo legislativo, sancionando la pertinente incorporación y modificación de las normas pertinentes en el contexto del régimen vigente por la Ley 22.172.

Lo cierto, es que, lamentablemente, pese a la suscripción del Convenio y las intenciones tenidas al celebrarlo, no ha sido una realidad y uso común, desde aquel entonces a la fecha, la comunicación formal y procesal entre los jueces argentinos de distinta jurisdicción, mediante el uso de la firma digital.

Creo que al celebrar el Convenio estábamos conscientes, que ese complemento, debía servir de trampolín para lo que soñamos inmediato abordaje legislativo. Las tempestades políticas y económicas que conmovieron la Nación, postergó de manera un tanto exagerada, que se concretara la comunicación electrónica mediante firma digital.

Estimo a la hora de esta conclusión, modestamente convencido de ello, que el mejor modo hacerlo es esbozando un proyecto de Ley de Comunicación Electrónica Interjurisdiccional que venga a llenar el vacío legal señalado, y que seguramente será enriquecido con valiosos aportes.

I. Anteproyecto de exposición de motivos ley de comunicación interjurisdiccional electrónica

I.1. Los antecedentes:

El proyecto reconoce los antecedentes que durante muchos años, desde la Primera Reunión llevada a cabo en Termas de Río Hondo, elaboraran los Poderes Judiciales de las Provincias Argentinas por intermedio de sus Cortes y Superiores Tribunales y los respectivos técnicos informáticos.

El documento elaborado en aquella oportunidad y otro subsiguiente también elaborado en Santiago del Estero, esta vez, en su ciudad Capital, convergieron en un Plenario llevado a cabo en la Capital Federal, que sentó las bases para la celebración el seis de septiembre de 2001, del Convenio de Comunicación Electrónica Interjurisdiccional, suscripto en la sede del Ministerio de Justicia de la Nación por la mayoría de los Poderes Judiciales de las Provincias Argentinas, la Procuración General de la Nación y Defensoría General de la Nación.

Dicho convenio se acompañó de un Protocolo Técnico de Comunicación Electrónica Interjurisdiccional, fruto del consenso logrado entre los técnicos informáticos de los poderes judiciales que pudieran intercambiar sus experiencias locales en los foros constituidos en las citadas reuniones.

Tales antecedentes son reconocidos de modo expreso en el proyecto en el artículo 10 inciso 1, exigiendo incluso, la adecuación a sus principios de la reglamentación que se encomienda a la Jefatura de Gabinete de Ministros.

Ello, por la valía de tales aportes, toda vez que reconoce su génesis en el propio seno de la Justicia destinataria de su aplicación. Es así, que, como se verá al analizar su articulado, el mismo, en general, respeta las normas contenidas en el citado convenio.

I.2. Las normas:

En los artículos primero y segundo la ley habilita la comunicación electrónica entre jueces de distintas jurisdicciones mediante el uso de la firma digital en un todo de acuerdo con la Ley 25.506 que regula la misma.

El primero de los artículos sigue parcialmente la redacción del artículo quinto del Convenio. Esta norma habilitó el sistema, con las limitaciones y reservas previstas en el artículo décimo del mismo. Su existencia posibilitó algunas erráticas experiencias y el consecuente dictado de algunas normativas en los Poderes Judiciales provinciales, (29) sin que se llegara a homogeneizar y generalizar la comunicación del modo ágil provisto por la tecnología, y del que se hace eco la ley diseñada.

La Ley 25.506 ha asimilado la firma digital a la ológrafa, y ha dotado su proceso de verificación de una red de seguridad, a la que se somete la ley proyectada.

Se deja a salvo en el artículo tercero la remisión anexa de aquellos documentos que por su naturaleza y objeto no pueden ser remitidos por vía electrónica, y en tal sentido recepta la norma contenida en el primer párrafo del artículo séptimo del Convenio.

En el artículo cuarto la ley dispone que las comunicaciones llevadas a cabo en su contexto vayan provistas de los correos electrónicos de organismos judiciales y ministerios públicos intervinientes, como asimismo abogados o personas que pudieran estar autorizadas a intervenir en la diligencia. Se prevé, asimismo, la cita de los respectivos números telefónicos. Téngase en cuenta que al momento de dictarse la Ley 22.172, no era usual recurrir a la

---

(29) v.gr.: así, el Superior Tribunal de Justicia de la Provincia de Jujuy mediante la Acordada Nº 70/02 adhiere al Convenio de Comunicación Electrónica Interjurisdiccional. Pasando revista de las páginas web de los poderes judiciales provinciales encontramos otros modos de manifestar la adhesión por parte del Poder Judicial a la normativa específica: así, mediante la Resolución Nº 398/05 del 24/08/05 el Superior Tribunal de Justicia de la Provincia de Río Negro autoriza la firma digital para las comunicaciones que materialicen trámites judiciales y administrativos de organismos interjurisdiccionales. En similares términos se expide el Poder Judicial de la Provincia de Chubut mediante Resolución Administrativa Nº 2737/05 SIJ del 30/09/05, entre otros. El Tribunal Superior de Justicia de la Provincia de Córdoba, mediante Acuerdo Reglamentario Nº 882 - Serie "A" autoriza la implementación del sistema de firma digital respecto de las sentencias y autos de los Juzgados de Ejecución Fiscal.

practicidad de la comunicación telefónica, tan frecuente en nuestros días, y no sólo entre oficiado y oficiante, sino con los respectivos abogados. La norma, como es lógico deja subsistente en su primer párrafo el cumplimiento de todos los datos exigidos por las leyes vigentes, con lo cual se esta aludiendo, especialmente, a los emanados del artículo tercero del Convenio de Comunicación entre Tribunales de la República, aprobado por la Ley 22.172, normas concordantes y correlativas.

En tal sentido el siguiente artículo quinto aborda centralmente la cuestión de tener por cumplidos mediante el procedimiento digital de esta ley los recaudos de firma y sello de juez y tribunal, y firma de secretario en cada foja de exigencia ritual por imperio del inciso sexto del artículo tercero del citado convenio de Comunicación entre Tribunales de la República aprobado por Ley 22.172.

En este aspecto la norma aborda de manera expresa una cuestión implícita en el convenio que reconoce como antecedente. Como se ha dicho la Ley 25.506 ha equiparado la firma digital a la ológrafa, y seguramente ello hizo que el convenio no abordara este tema. Lo cual por otro lado, y como es obvio, hubiera sido un vallado por su veda a legislar y dejar sin efecto alguna exigencia estatuida por ley.

La asimilación dispuesta por la Ley 25.506, habilita la posibilidad de opinar sobre la conveniencia o no de una expresa regulación legal sobre el tema. Sin duda al celebrarse el Convenio del seis de septiembre de 2001, se interpretó que no era conveniente o necesario.

En este caso, en el proyecto, se opta por la conveniencia de regular expresamente la cuestión, dando por cumplidos los recaudos enumerados en la vieja norma aprobada por Ley 22.172, mediante el sistema digital que se proyecta. Ello atendiendo al enraizado uso de la exigencia de tales recaudos, cuya práctica como es obvio genera una resistencia al cambio propuesto.

El artículo sexto recepta la norma contenida en el segundo párrafo del artículo séptimo del referido Convenio, estatuyendo que la impresión del correo con constancia de la actuaria e incorporación al expediente acreditará la comunicación.

La posibilidad de que el proceso de verificación arroje la existencia de alguna alteración se ha contemplado en el artículo séptimo, dejando sujeta la cuestión a la reglamentación. De ese modo se flexibiliza la atención del tema teniendo en cuenta los avances de la tecnología que pueden hacer variar las respuestas de un modo más dinámico, que el procedimiento de atender la cuestión por vía de una ley.

La Ley 25.506 prevé la existencia de un certificador licenciado que debe ser habilitado como tal por la autoridad de aplicación, y que siendo poseedor del respectivo código de seguridad del emisor de un documento digital, es el encargado de certificar su autenticidad. Vale remarcar que este es un procedimiento instantáneo y simultáneo a la emisión y recepción del documento.

En el proyecto se propone la creación del Instituto Certificador Judicial Licenciado, como ente certificante a los fines del sistema previsto en la ley. Se deja a cargo del mismo a las Justicias Nacional y Provinciales, con la debida representación del Ministerio Público. Con criterio práctico se sujeta a la reglamentación la proporcionalidad en que se integrarán al mismo, con el anhelo de que ello sea fruto del consenso que obviamente debe subyacer en la puesta operativa que contemplará el reglamento de la ley.

En tal sentido, el artículo décimo de la ley impone a la Jefatura de Gabinete la pronta aplicación operativa del sistema diseñado por la ley y al efecto establece un plazo no mayor a noventa días para el dictado de la aludida reglamentación, la que somete al respeto de los principios que fueran sentados por los Poderes Judiciales en el citado Convenio.

En el inciso segundo del referido artículo décimo se ordena la asignación de recursos y partidas presupuestarias necesarias y en el inciso tercero se establece que en un plazo no mayor a treinta días posteriores a la reglamentación deberá invitarse a la integración del Instituto creado y el otorgamiento al mismo de la correspondiente licencia prevista en la Ley 25.506 a los fines de su cometido.

Los artículos sexto, séptimo y octavo del Convenio de Comunicaciones entre Tribunales de la República aprobado por Ley 22.172 contemplan los casos de diligencias de notificaciones, inscripciones en registro y en general diligencias sin intervención del juez local. Ellas obviamente presuponen la existencia de oficinas receptoras que se encuentren en condiciones operativas de aplicar el sistema de la ley. Muchas de ellas, incluso, corresponden a dependencias de otros poderes del Estado, y no organismos judiciales. Vale destacar que no son pocas las que ya se encuentran operando del modo propuesto. A título de ejemplo; la AFIP.

Atendiendo a tales antecedentes se ha dejado sujeto a que el Instituto creado por la ley confeccione una propuesta de reglamentación operativa con referencia a las diligencias contempladas en los citados artículos sexto, séptimo y octavo, para lo cual obviamente habrá de munirse en forma previa de un adecuado relevamiento en los distintos estamentos de la administración pública que permita un ágil cumplimiento del objetivo de la ley.

II. Texto del anteproyecto:

Ley de Comunicación Interjurisdiccional Electrónica

Art. 1.— La comunicación directa entre organismos judiciales y ministerios públicos de distinta jurisdicción territorial podrá realizarse a través del correo electrónico, sin distinción de grado o clase, utilizando las direcciones de los mismos, debidamente dadas de alta por las respectivas autoridades.

Art. 2.— La comunicación prevista en el artículo anterior se llevará a cabo mediante la aplicación de la firma digital y documento digital en los términos y con los alcances previstos por la Ley 25.506.

Art. 3.— Los elementos y/o documentos que no puedan ser enviados por los medios previstos en la presente serán remitidos como anexo en otro soporte.

Art. 4.— Sin perjuicio de los requisitos establecidos en las leyes vigentes, la comunicación electrónica deberá contener designación completa de ambos organismos judiciales o ministerios públicos, y de las personas y abogados autorizados a intervenir en su diligenciamiento, cuando correspondiere. En todos los casos se indicará, número de teléfono, domicilio y dirección de correo electrónico.

Art. 5.— Los requisitos dispuestos por el inciso 6 del artículo 3 del convenio aprobado por Ley 22.172 (Convenio sobre comunicación entre tribunales de distinta jurisdicción territorial) se tendrán por cumplidos con la certificación extendida por el Instituto Certificador Judicial Licenciado con arreglo a la Ley 25.506 y a las disposiciones de la presente.

Art. 6.— La incorporación al expediente de la impresión del correo electrónico con la constancia actuarial será prueba suficiente a efectos de tener por acreditada la comunicación realizada.

Art. 7.— La reglamentación dispondrá el procedimiento a seguir en caso que la verificación de la firma digital informe alteración.

Del Instituto Certificador Judicial Licenciado

Art. 8.— Créase el Instituto Certificador Judicial Licenciado, que estará integrado por representantes de los Poderes Judiciales de las Provincias y de la Nación y del Ministerio Público, en la proporción que indique la reglamentación.

Art. 9.— El Instituto creado en el artículo precedente, tendrá por objeto expedir los certificados digitales necesarios a los fines de la comunicación electrónica prevista por esta ley.

Art. 10.— La Jefatura de Gabinete de Ministros dictará las normas necesarias y llevará a cabo los actos que fueran menester, para la pronta aplicación y operatividad de la presente, entre otros:

1. Elevará el proyecto de reglamentación en el plazo de noventa días de publicada. El mismo deberá adecuar los aspectos operativos de la presente a la Ley 25.506 y reconocerá como antecedente y receptará los principios y disposiciones contenidos en el Convenio de Comunicación Electrónica Interjurisdiccional, celebrado entre los Poderes Judiciales de las Provincias Argentinas, la Procuración General de la Nación y la Defensoría General de la Nación, y el Protocolo Técnico de Comunicación Electrónica Interjurisdiccional anexo.

2. Asignará las partidas presupuestarias y recursos pertinentes para el funcionamiento del Instituto creado por esta ley.

3. En un plazo no mayor de treinta días posteriores a la reglamentación, invitará a los poderes judiciales y ministerios públicos a la integración del Instituto Certificador Judicial Licenciado, al que otorgará la licencia prevista por la Ley 25.506.

Art. 11.— El Instituto Certificador Judicial Licenciado propondrá a los poderes judiciales de la Nación y de las Provincias, y a la Jefatura de Gabinete de Ministros, un proyecto que habilite la aplicación de la comunicación electrónica prevista en la presente, a los fines de las diligencias previstas en los artículos seis, siete y ocho del Convenio de comunicación entre tribunales de distinta jurisdicción territorial aprobado por Ley 22.172.

Art. 12.— De forma.

Este proyecto de ley fue presentado como tal, con algunas felices correcciones de forma, ante la Honorable Cámara de Diputados de la Nación, por los Sres. Diputados, Dr. Alfredo Carlos Dato y Dr. Luis Francisco Cigogna, integrantes de la Comisión de Justicia. (Expte. 4322-13-2008. Trámite Parlamentario: 102 del 19-08-2008)

III. Nota al proyecto de creación del Instituto Certificador Judicial Licenciado

Al momento de esta edición ha cobrado un meritorio impulso y una encomiable labor la Oficina Nacional de Tec. de la Información (conocida por su sigla ONTI). Muchas de las justicias provinciales, con criterio práctico y resultado eficiente, han acudido a la misma como encargada de la certificación de la firma, a los fines de aplicar la firma digital, en algunos temas puntuales en que avanzaran. Así por ejemplo la excelente decisión (referida en antecedentes y en anexo) del STJ de Córdoba de disponer la firma de sentencias en los tribunales de ejecución fiscal mediante el uso de la firma digital, reconoce la intervención de la ONTI a los fines de la certificación de la misma.

Reitero que la labor de dicha Oficina es de elevada factura técnica, y la idea en este proyecto de propiciar la creación de una autoridad certificante, a los fines de la comunicación entre jueces, está muy lejos de ir en mengua de la gestión de la ONTI. Al contrario, como se verá, hasta puede ser la encargada operativa de la tarea.

En efecto, me explico. La ONTI, más allá de su meritoria autonomía, no goza de la independencia constitucionalmente estatuida en tal grado de preservación, como la reglada para la Justicia; ella si bien puede, lamentablemente no ser una realidad práctica en muchos casos, sí es una realidad en el texto normativo constitucional, y por cierto, de manera indudable, un anhelo de toda la ciudadanía.

En ese marco creo conveniente que la certificación de la firma en la comunicación entre los jueces argentinos y entre estos y terceros, debe estar regida por la propia Justicia. Por ello se propicia este Instituto Certificador Judicial Licenciado (cuyo nombre respeta la nomenclatura de la Ley 25.506 y sus reglamentaciones) que se integra con representantes de los poderes involucrados, Justicia Nacional, Justicias Provinciales y Ministerio Público.

No se pretende crear una estructura administrativa ni generar costos. Tan solo los representantes, que encontrándose remunerados en su labor judicial, pueden desempeñar en forma ad-honorem esta honrosa carga. Es más, es posible, y sería plausible, que designados los representantes deleguen la tarea operativa en la ONTI; pero son ellos, los representantes de esas tres órbitas judiciales quienes encomiendan la gestión, y cualquier interferencia futura en tal tarea certificadora, podrán o decidir llevar directamente bajo su dependencia la gestión, contratando los técnicos necesarios y los equipos pertinentes (que para nada es un gasto sobredimensionado) o acudir a otro tercero que bajo su vigilancia pueda llevar a cabo la labor. Lamentablemente la realidad histórica política de nuestras repúblicas latinoamericanas, muestra el tristemente frecuente, uso de las vías de hecho en el ejercicio del poder, y la trasgresión de —entre otras— las normas que preservan la independencia del Poder Judicial, sometiendo a éste a fuertes presiones. Imaginemos una actividad judicial, que barrunto muy cercana —para bien de el—, en la que todas las comunicaciones judiciales se hagan con uso de la firma digital, y que quien ejerza del poder en turno, tenga un enfrentamiento con el Poder Judicial, o simplemente tenga interés en dilatar una o más medidas que en la Justicia se hubiera resuelto. Interferir en la tarea de certificación, obviamente, veda el acceso en la comunicación al destinatario. Un organismo de certificación funcionando en la órbita del Poder Ejecutivo, está expuesto a directivas de éste. No dudo que los actuales integrantes de la ONTI no se prestarían a ello. Pero a quien podrán designar en el futuro, eventuales políticos proclives al desborde en el ejercicio del poder? Aquellos futuros integrantes, responderán a un acto de esta naturaleza? Es eventualmente factible que acontezcan desbordes de esta naturaleza en el ejercicio del poder?. No creo pecar de pesimismo cuando concluyo que no es imposible que ello ocurra, y prefiero que siempre la Justicia tenga su propia supervisión sobre sus actos, y la facultad de elegir por propia decisión un atajo si encuentra algún inconveniente en el servicio o lo que es más grave una posible interferencia. Hoy, reitero, me parecería lo más adecuado: tener el Instituto habilitado por ley, y aconsejar a éste encomendar la operatividad de la certificación a la ONTI, con la facultad de los miembros de la Justicia que en forma ad-honorem integren el Instituto, de revocar dicha encomienda y —como he dicho— reasumirla en caso que las circunstancias fácticas lo hagan aconsejable.

IV. Proyecto de ley presentado en la h. cámara de diputados de la nación por su comisión de justicia

Vaya en primer término mi expreso reconocimiento al Sr. Diputado por Tucumán Dr. Alfredo Carlos Dato, quien después de un meritorio paso por la

Justicia tucumana hoy es legislador e integrante de la Comisión de Justicia, y desde ella no ha dejado de preocuparse por la tarea judicial.

En ese marco y con notable entusiasmo, consciente de los beneficios de este proyecto impulsó su presentación, siendo acompañado por el Sr. Presidente de la Comisión de Justicia Diputado Dr. Luis Francisco Cigogna.

Con algunas mínimas, pero seguramente atinadas, modificaciones el proyecto reproduce casi textualmente el anteproyecto elaborado en este trabajo. Se identifica como expte. 4322-13-2008, Trámite parlamentario 102 del 19 de Agosto de 2008.

Al momento de esta edición, y desde hace mucho, he escuchado frecuentes críticas a la Justicia, entre otras causas por su morosidad.

Concretado este proyecto —en su diseño, o en el que seguramente sabrán enriquecer los señores legisladores— no hay duda que significará una fuerte apuesta a combatir la mora, proporcionando celeridad en las diligencias. Como he dicho, de alguna manera, este proyecto sale de la propia Justicia, y en su impulso me toca ser un instrumento. Vaya mi esperanza de un pronto tratamiento y aprobación con las formas y modos que los encargados de sancionarla y promulgarla entiendan sea óptimo y eficiente para la Justicia.

TEXTO DEL PROYECTO DE LEY PRESENTADO POR LOS INTEGRANTES DE LA COMISIÓN DE JUSTICIA DE LA HONORABLE CÁMARA DE DIPUTADOS DE LA NACIÓN.

Ley de Comunicación Interjurisdiccional Electrónica

Artículo 1º: La comunicación directa entre organismos judiciales y ministerios públicos de distinta jurisdicción territorial, sin distinción de grado o clase, podrá realizarse a través de correo electrónico, utilizando las direcciones debidamente dadas de alta por las respectivas autoridades de dichos organismos.

Art. 2º: La comunicación prevista en el artículo anterior se llevará a cabo mediante la aplicación de la firma digital y documento digital en los términos y con los alcances previstos por la ley 25.506 —Ley de Firma Digital—.

Art. 3º: Los contenidos que no puedan ser enviados por los medios previstos en la presente serán remitidos como anexo en otro soporte.

Art. 4º: Sin perjuicio de los requisitos establecidos en las leyes vigentes, la comunicación electrónica deberá contener la designación completa del organismo remitente y del organismo destinatario y la designación y calidad de las personas autorizadas a intervenir en su diligenciamiento, cuando correspondiere. En todos los casos, se indicará domicilio, número de teléfono y dirección de correo electrónico.

Art. 5º: Los requisitos dispuestos por el inciso 6 del artículo 3 del Convenio aprobado por ley 22.172 —Convenio de comunicación entre tribunales de distinta jurisdicción— se tendrán por cumplidos con la certificación extendi-

da por el Instituto Certificador Judicial Licenciado con arreglo a la ley 25.506 —Ley de Firma Digital— y a las disposiciones de la presente.

Art. 6º: La comunicación electrónica se tendrá por acreditada con la incorporación al expediente del texto impreso del documento electrónico con la debida intervención del actuario.

Art. 7º: En el caso que la verificación de la firma digital registre alteración, la comunicación será nula, de nulidad absoluta. Sin perjuicio de que se abran otras instancias para investigar la alteración en forma independiente del expediente original.

Art. 8º: Créase el Instituto Certificador Judicial Licenciado, que estará integrado por representantes de los Poderes Judiciales de las Provincias y de la Nación y del Ministerio Público, en la proporción que indique la reglamentación.

Art. 9º: El Instituto creado en el artículo precedente, tendrá por objeto expedir los certificados digitales necesarios a los fines de la comunicación electrónica prevista por esta ley.

Art. 10º: La Jefatura de Gabinete de Ministros dictará las normas necesarias y llevará a cabo los actos que fueran menester, para la pronta aplicación y operatividad de la presente, entre otros:

a) Elevará el proyecto de reglamentación en el plazo de noventa días de publicada. El mismo deberá adecuar los aspectos operativos de la presente a la ley 25.506 y reconocerá como antecedente y receptará los principios y disposiciones contenidos en el Convenio de Comunicación Electrónica Interjurisdiccional, celebrado entre los Poderes Judiciales de las Provincias Argentinas, la Procuración General de la Nación y la Defensoría General de la Nación, y el Protocolo Técnico de Comunicación Electrónica Interjurisdiccional anexo;

b) Asignará las partidas presupuestarias y recursos pertinentes para el funcionamiento del Instituto creado por esta ley;

c) En un plazo no mayor de treinta días posteriores a la reglamentación, invitará a los poderes judiciales y ministerios públicos a la integración del Instituto Certificador Judicial Licenciado, al que otorgará la licencia prevista por la ley 25.506.

Art. 11º: El Instituto Certificador Judicial Licenciado propondrá a los poderes judiciales de la Nación y de las Provincias, y a la Jefatura de Gabinete de Ministros, un proyecto que habilite la aplicación de la comunicación electrónica prevista en la presente, a los fines de las diligencias previstas en los artículos seis, siete y ocho del Convenio de Comunicación entre Tribunales de distinta jurisdicción territorial aprobado por ley 22.172.

Art. 12º: Comuníquese al Poder Ejecutivo.

FUNDAMENTOS

Señor presidente:

El día 6 de septiembre de 2001 se celebró el Convenio de Comunicación Electrónica Interjurisdiccional, el cual surgió de la necesidad de agilizar la comunicación entre organismos judiciales y ministerios públicos de distinta jurisdicción territorial de manera electrónica y en una forma total y absolutamente confiable.

La crisis que sufrió nuestro país poco tiempo después, afectó de manera sensible aquel incipiente proceso. Sin embargo, habiendo pasado varios años de su implementación y habiéndose sancionado la ley 25.506 de Firma Digital, es que consideramos absolutamente necesario la aprobación de una ley que contemple el mencionado Convenio así como la ley de Firma Digital, la cual reconoció la eficacia jurídica de los documentos digitales.

Con los extraordinarios avances de las herramientas tecnológicas es imperioso en estos días dotar, al Sistema Judicial y a los Ministerios Públicos, de todos los instrumentos que faciliten su labor y que, al mismo tiempo, sean totalmente confiables. El uso de recursos tecnológicos idóneos es de suma importancia en la tarea de "despapelizar" y de hacer más eficaz y ágil la tarea de la justicia.

Consideramos vital este proyecto, basado en la Tesina que presentara el señor Ernesto N. Kozameh para obtener su Maestría en Derecho y Magistratura Judicial de la Universidad Austral.

Hoy, más que nunca, la Justicia Argentina se encuentra dotada de los elementos técnicos necesarios para superar el lento sistema de comunicación entre jueces que se cumple actualmente en soporte papel y con apego a la ley 22.172.

1.1 Antecedentes:

El proyecto reconoce los antecedentes que durante muchos años, desde la Primera Reunión llevada a cabo en Termas de Río Hondo, elaboraran los Poderes Judiciales de las Provincias Argentinas por intermedio de sus Cortes y Superiores Tribunales y los respectivos técnicos informáticos.

El documento elaborado en aquella oportunidad y otro subsiguiente, también elaborado en Santiago del Estero, esta vez en su ciudad Capital, convergieron en un Plenario llevado a cabo en la Capital Federal, que sentó las bases para la celebración el seis de septiembre de 2001, del Convenio de Comunicación Electrónica Interjurisdiccional, suscripto en la sede del Ministerio de Justicia de la Nación por la mayoría de los Poderes Judiciales de las Provincias Argentinas, la Procuración General de la Nación y Defensoría General de la Nación.

Dicho convenio se acompañó de un Protocolo Técnico de Comunicación Electrónica Interjurisdiccional, fruto del consenso logrado entre los técnicos

informáticos de los poderes judiciales que pudieron intercambiar sus experiencias locales en los foros constituidos en las citadas reuniones.

Tales antecedentes son reconocidos de modo expreso en el proyecto en el artículo 10º, inciso a, exigiendo incluso, la adecuación a sus principios de la reglamentación que se encomienda a la Jefatura de Gabinete de Ministros.

Ello, por la valía de tales aportes, toda vez que reconoce su génesis en el propio seno de la Justicia destinataria de su aplicación. Es así que, como se verá al analizar su articulado, el mismo, en general, respeta las normas contenidas en el citado convenio.

1.2 Las normas:

En los artículos 1º y 2º, la ley habilita la comunicación electrónica entre jueces de distintas jurisdicciones mediante el uso de la firma digital en un todo de acuerdo con la ley 25.506 que regula la misma.

El artículo 1º sigue parcialmente la redacción del artículo 5º del Convenio. Esta norma habilitó el sistema, con las limitaciones y reservas previstas en el artículo 10º del mismo. Su existencia posibilitó algunas erráticas experiencias y el consecuente dictado de algunas normativas en los Poderes Judiciales provinciales, (1) sin que se llegara a homogeneizar y generalizar la comunicación del modo ágil provisto por la tecnología, y del que se hace eco la ley diseñada.

La ley 25.506 ha asimilado la firma digital a la ológrafa, y ha dotado su proceso de verificación de una red de seguridad, a la que se somete la ley proyectada.

Se deja a salvo en el artículo 3º la remisión anexa de aquellos documentos que por su naturaleza y objeto no pueden ser remitidos por vía electrónica, y en tal sentido recepta la norma contenida en el primer párrafo del artículo 7º del Convenio.

En el artículo 4º la ley dispone que las comunicaciones llevadas a cabo en su contexto vayan provistas de los correos electrónicos de organismos judiciales y ministerios públicos intervinientes, como asimismo abogados o personas que pudieran estar autorizadas a intervenir en la diligencia. Se prevé asimismo, la cita de los respectivos números telefónicos. Téngase en cuenta que al momento de dictarse la ley 22.172, no era usual recurrir a la practicidad de la comunicación telefónica, tan frecuente en nuestros días, y no sólo entre oficiado y oficiante, sino con los respectivos abogados. La norma, como es lógico, deja subsistente en su primer párrafo el cumplimiento de todos los datos exigidos por las leyes vigentes, con lo cual se está aludiendo, especialmente, a los emanados del artículo 3º del Convenio de Comunicación entre Tribunales de la República, aprobado por la ley 22.172, normas concordantes y correlativas.

En tal sentido el siguiente artículo 5º aborda centralmente la cuestión de tener por cumplidos mediante el procedimiento digital de esta ley los recau-

dos de firma y sello de juez y tribunal, y firma de secretario en cada foja de exigencia ritual por imperio del inciso 6º del artículo 3º del citado Convenio de Comunicación entre Tribunales de la República, aprobado por la ley 22.172.

En este aspecto la norma aborda de manera expresa una cuestión implícita en el Convenio que reconoce como antecedente. Como se ha dicho, la ley 25.506 ha equiparado la firma digital a la ológrafa, y seguramente ello hizo que el convenio no abordara este tema. Lo cual, por otro lado, y como es obvio, hubiera sido un vallado por su veda a legislar y dejar sin efecto alguna exigencia estatuida por ley.

La asimilación dispuesta por la ley 25.506, habilita la posibilidad de opinar sobre la conveniencia o no de una expresa regulación legal sobre el tema. Sin duda al celebrarse el Convenio del seis de septiembre de 2001, se interpretó que no era conveniente o necesario.

En este caso, en el proyecto se opta por la conveniencia de regular expresamente la cuestión, dando por cumplidos los recaudos enumerados en la vieja norma aprobada por ley 22.172, mediante el sistema digital que se proyecta. Ello atendiendo al enraizado uso de la exigencia de tales recaudos, cuya práctica como es obvio genera una resistencia al cambio propuesto.

El artículo 6º recepta la norma contenida en el segundo párrafo del artículo 7º del referido Convenio, estatuyendo que la incorporación al expediente del texto impreso con la debida intervención del actuario e incorporación al expediente, acreditará la comunicación.

La posibilidad de que el proceso de verificación arroje la existencia de alguna alteración se ha contemplado en el artículo 7º. En ese caso la comunicación será nula. Tampoco impide que los avances tecnológicos mejoren el proceso de verificación sin afectar la ley.

La ley 25.506 prevé la existencia de un certificador licenciado que debe ser habilitado como tal por la autoridad de aplicación, y que siendo poseedor del respectivo código de seguridad del emisor de un documento digital, en el encargado de certificar su autenticidad. Vale remarcar que este es un procedimiento instantáneo y simultáneo a la emisión y recepción del documento.

En el proyecto se propone la creación del Instituto Certificador Judicial Licenciado, como ente certificante a los fines del sistema previsto en la ley. Se deja a cargo del mismo a las Justicias Nacional y Provinciales, con la debida representación del Ministerio Público. Con criterio práctico se deja librado a la reglamentación la proporcionalidad en que se integrarán al mismo, con el anhelo de que ello sea fruto del consenso que obviamente debe subyacer en la puesta operativa que contemplará el reglamento de la ley.

En tal sentido, el artículo 10º de la ley impone a la Jefatura de Gabinete la pronta aplicación operativa del sistema diseñado por la ley y al efecto establece un plazo no mayor a noventa días para el dictado de la aludida reglamentación,

la que somete al respeto de los principios que fueran sentados por los Poderes Judiciales en el citado Convenio.

En el inciso b, del referido artículo 10º se ordena la asignación de recursos y partidas presupuestarias necesarias y en el inciso c, se establece que en un plazo no mayor a treinta días posteriores a la reglamentación deberá invitarse a las integración del Instituto creado y el otorgamiento al mismo de la correspondiente licencia prevista en la ley 25.506 a los fines de su cometido.

Los artículos sexto, séptimo y octavo del Convenio de Comunicaciones entre Tribunales de la República aprobado por ley 22.172 contemplan los casos de diligencias de notificaciones, inscripciones en registro y en general diligencias sin intervención del juez local. Ellas obviamente presuponen la existencia de oficinas receptoras que se encuentren en condiciones operativas de aplicar el sistema de la ley. Muchas de ellas, incluso, corresponden a dependencias de otros poderes del Estado, y no organismos judiciales. Vale destacar que no son pocas las que ya se encuentran operando del modo propuesto. A título de ejemplo: la AFIP.

Atendiendo a tales antecedentes se ha dejado sujeto a que el Instituto creado por la ley confeccione una propuesta de reglamentación operativa con referencia a las diligencias contempladas en los citados artículos 6º, 7º y 8º, para lo cual previamente será necesario realizar un detallado relevamiento en los distintos estamentos de la administración pública, que permita un ágil cumplimiento del objetivo de la ley.

Conclusión:

Señor Presidente, estimamos sobreabundante resaltar el flagelo de la mora en el sistema judicial argentino, y el actual procedimiento de comunicaciones entre jueces, es una de las tantas razones dilatorias del proceso.

Consideramos realmente necesario trasladar la celeridad en las comunicaciones a las que nos hemos habituado en nuestra vida privada, al ámbito de la justicia y por imperio de esta ley, insertar este aporte tecnológico en el proceso.

Todo este laberinto burocrático puede ser sustituido con la inmediatez del uso de la informática, a través de su red de internet que nos vincula, y la seguridad derivada del cumplimiento de los recaudos que esta ley prevé.

Por los motivos expuestos solicito a los señores legisladores la aprobación del presente proyecto de ley.

(1) V. gr.: así, el Superior Tribunal de Justicia de la Provincia de Jujuy mediante la Acordada Nº 70/02 adhiere al Convenio de Comunicación Electrónica Interjurisdiccional. Pasando revista de las páginas web de los poderes judiciales provinciales encontramos otros modos de manifestar la adhesión por parte del Poder Judicial a la normativa específica: así, mediante la Resolución Nº 398/05 del 24/08/05 el Superior Tribunal de Justicia de la Provincia de Río Negro

autoriza la firma digital para las comunicaciones que materialicen trámites judiciales y administrativos de organismos interjurisdiccionales. En similares términos se expide el Poder Judicial de la Provincia de Chubut mediante Resolución Administrativa Nº 2737/05 SI del 30/09/05, entre otros.

ANEXOS

ANEXO I

Breve repaso de la cronología en la materia en base a la publicada en www.pki.gov.ar, con los agregados pertinentes:

Año 1996-1999

1996: Se inician las reuniones del Subcomité de Critpografía y Firma Digital en la sede de la Secretaría de la Función Pública (SFP), con la participación de representantes del BCRA, la CNV, el Ministerio de Justicia y la ANSeS. En Diciembre se elabora el Documento "Pauta mínimas para una normativa de Firma digital", el cual pasa a conformar el Anexo de la Resolución SFP Nº 45/02.

1997: El Subcomité de Criptografía y Firma Digital emite la Resolución SFP Nº 45/97 que establece pautas técnicas para elaborar una normativa sobre firma digital.

El Subcomité de Criptografía y Firma Digital inicia la redacción de lo que luego será el Decreto Nº 427/98.

1998: En abril se sanciona el Decreto Nº 427/98 que habilita el uso de Firma Digital en la Administración Pública Nacional (APN). Se asigna a la SFP la función de Organismo Licenciante (organismo que habilita el funcionamiento de Autoridades Certificantes en la APN).

Se elaboran los Estándares Tecnológicos y la Política de Certificación de la Infraestructura de Firma Digital del Sector Público Nacional (aprobados luego por la Resolución SFP Nº 212/98 y la Resolución Nº 194/98 respectivamente).

1999:

Implementación del Organismo Licenciante en la SFP según lo establecido por el Decreto Nº 427/98.

Licenciamiento del Ministerio de Economía como la primera Autoridad Certificante en la APN.

El Equipo de PKI desarrolla y pone en funcionamiento una Autoridad Certificante Pública para la emisión de certificados dentro de la APN.

Desarrollo de un software para la provisión de certificados digitales (APuN-CA) destinado a los organismos públicos que quieran implementar la tecnología de firma digital.

Implementación de la Autoridad Certificante Piloto de la Subsecretaría de la Gestión Pública con el objeto de entregar certificados digitales de prueba al público en general.

Inauguración en el mes de Octubre del Laboratorio de Firma Digital de la SGP, como unidad de difusión y capacitación en Firma Digital.

En junio de 1999 se celebra en Termas de Río Hondo, Santiago del Estero, la I Reunión de Ministros de Cortes y Superiores Tribunales de la República Argentina, para abordar el tema, y en paralelo de realiza la I reunión de sus técnicos informáticos, generándose el Foro Permanente de los mismos

Año 2000

Se celebra en Santiago del Estero la II reunión de los técnicos informáticos de los poderes judiciales de la R.A.

Se reemplaza la Autoridad Certificante Piloto de la SGP por la Autoridad Certificante de la SGP para Certificados de Correo electrónico.

Se firma el "Convenio de Cooperación entre la Subsecretaría de la Gestión Pública y el Superior Tribunal de Justicia de la Provincia de Chubut", el cual establece la puesta en marcha de un plan conjunto de implementación de las tecnologías de Firma Digital y Documento Electrónico.

Año 2001

Enero: Participación en las reuniones de responsables informáticos de los Poderes Judiciales.

Marzo: Se participa en la reunión del Comité Ejecutivo del Protocolo Técnico del Convenio de Comunicaciones Electrónicas Interjurisdiccionales (CCEI), en la cual se establece que la Subsecretaría de la Gestión Pública emitirá los certificados digitales que se usarán en las comunicaciones hasta tanto los Poderes Judiciales no creen su propia infraestructura.

Se inicia la distribución de la "Lista de Novedades sobre Firma Digital".

Se habilita la cuenta de correo institucional consulta@pki.gov.ar para la atención de consultas dirigidas al público en general.

Agosto: El proyecto de Ley de Firma Digital unificado recibe media sanción en la cámara de Diputados.

Septiembre: Se forma una comisión para la elaboración del Decreto Reglamentario de la Ley de Firma Digital.

Inicio de actividades de la comisión redactora del proyecto de Decreto Reglamentario, con la participación de prestigiosos abogados del sector académico, los Poderes Judiciales y el personal del equipo de Firma Digital.

Se firma el "Convenio de Comunicaciones Electrónicas Interjurisdiccionales" entre la Procuración General de la Nación, Defensoría General de la Nación, los Poderes Provinciales Judiciales, el Poder Judicial de la Ciudad Autónoma de Buenos Aires, la Secretaria para la Modernización del Estado de la Jefatura del Gabinete de Ministros, el Ministerio de Justicia y Derechos Humanos, los cuales se ponen de acuerdo para utilizar la tecnología que se indica en el Protocolo Técnico Anexo (Comunicación Electrónica con Firma Digital) para sus comunicaciones.

Octubre: Comienza a operar la Autoridad Certificante de la ONTI para la emisión de Certificados de Agente Público (AC-ONTI).

El equipo de Firma Digital pone en operaciones la Autoridad Certificante de la ONTI, disponible para la provisión de certificados de firma digital a funcionarios de la APN y miembros participantes del Convenio de Comunicación Electrónica Interjurisdiccional.

Noviembre: Se aprueba en al Cámara de Senadores el proyecto de Ley de Firma Digital unificado.

El Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires se constituye en Autoridad de Registro de la AC-ONTI (Disposición Nº 02/2001 del 23/11/2001).

Año 2002

Marzo: Se pone en circulación para discusión pública el anteproyecto de Decreto Reglamentario de la Ley de Firma Digital. Se envía a los principales organismos públicos, se distribuye a una lista de e-mail con más de 1000 participantes de más de 20 países alrededor del mundo y se publica en el sitio www.pki.gov.ar.

Participación en el Subgrupo de Trabajo Nº 13 Mercosur iniciando el área de Firma Digital. Primeros contactos con la Infraestructura de Clave Pública de Brasil. Se inicia un intercambio de información y la preparación de documentación de base y un anteproyecto de norma común con el objetivo de lograr el reconocimiento recíproco de certificados.

Abril: El Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires se constituye en Autoridad de Registro de la AC-ONTI (Disposición 01/2002 del 23/04/2002).

El Superior Tribunal de Justicia de Santiago del Estero se constituye en Autoridad de Registro de la AC-ONTI (Disposición Nº 02/2002 del 23/04/2002).

El Tribunal Superior de Justicia de la Provincia de Río Negro se constituye en Autoridad de Registro de la AC-ONTI (Disposición Nº 03/2002 del 23/04/2002).

Agosto: El Ministerio de Defensa se constituye en Autoridad de Registro de la AC-ONTI (Disposición Nº 01/2002 del 30/08/2002).

Septiembre: El Superior Tribunal de Justicia de la Provincia del Chaco se constituye en Autoridad de Registro de la AC-ONTI (Disposición Nº 02/2002 del 27/09/2002).

Noviembre: La Suprema Corte de Justicia de la Provincia de Mendoza se constituye en Autoridad de Registro de la AC-ONTI (Disposición Nº 04/2002 del 18/11/2002).

Diciembre: El Superior Tribunal de Justicia de la Provincia de Jujuy se constituye en Autoridad de Registro de la AC-ONTI (Disposición Nº 05/2002 del 04/12/2002).

Se aprueba el Decreto Nº 2628/2002. El decreto establece la creación de un Ente Administrador de Firmas Digitales.

La Secretaría General de la Presidencia de la Nación se constituye en Autoridad de Registro de la AC-ONTI (Disposición Nº 06/2002 del 27/12/2002).

Año 2003

Enero: El Superior Tribunal de Justicia de la Provincia de Salta se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 01/2003 del 10/01/2003).

Marzo: La Comisión Nacional de Actividades Espaciales se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 03/2003 del 03/03/2003).

La Procuración General de la Nación se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 04/2003 del 24/03/2003).

El Estado Mayor General del Ejército se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 05/2003 del 24/03/2003).

Agosto: La Administración de Parques Nacionales se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 01/2003 del 20/08/2003).

La Secretaría de Ciencia, Tecnología e Innovación Productiva se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 02/2003 del 20/08/2003).

Octubre: Por orden del Director de la ONTI el equipo de firma digital comienza a trabajar en la elaboración de los documentos referidos al proceso de licenciamiento de certificadores.

Noviembre: El Superior Tribunal de Justicia de la Provincia de Tierra del Fuego, Antártida e Islas del Atlántico Sur se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 6/2003 del 14/11/2003).

El Instituto Nacional Unico Coordinador de Ablación e Implante (INCUCAI) se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 7/2003 del 25/11/2003).

La Contaduría General de la Nación de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerio de Economía se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 8/2003 del 25/11/2003)

Diciembre: La Comisión Nacional de Energía Atómica (CNEA) se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 9/2003 del 18/12/2003).

La ONTI publica en su sitio web los textos preliminares de los documentos referidos al proceso de licenciamiento de certificadores con el fin de someterlos a consulta pública de acuerdo con lo establecido por la normativa legal vigente

Año 2004

Enero: La SGP convoca a diversas instituciones del país, a medios de prensa especializados y a los suscriptores de la lista de novedades sobre firma digital, a participar en la consulta pública sobre las versiones preliminares de los documentos referidos al proceso de licenciamiento de certificadores. El período de consulta se extiende durante los meses de Enero y Febrero.

Febrero: El Ministerio del Interior se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 02/2004 del 09/02/2004).

Marzo: Se inicia el análisis de los aportes recibidos en el período de consulta pública y la preparación de las versiones finales de los documentos referidos al licenciamiento de certificadores.

Mayo: El Gobierno de la Provincia de Mendoza se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 03/2004 del 04/05/2004).

La Legislatura de la Provincia de Tierra del Fuego se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 04/2004 del 05/05/2004).

El Poder Judicial de la Provincia de Entre Ríos se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 05/2004 del 24/05/2004).

Agosto: La Superintendencia de Seguros se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 06/2004 del 18/08/2004).

Noviembre: La Superintendencia de Servicios de Salud se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 09/2004 del 12/11/2004).

Año 2005

Marzo: El Ministerio de Trabajo, Empleo y Seguridad Social se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 01/2005 del 18/03/2005).

En el marco del Convenio de Cooperación firmado con el Gobierno de la Provincia de Corrientes, se acuerda un plan de trabajo a fin de colaborar en la implementación de la tecnología de firma digital en la Dirección de Personal del gobierno provincial.

Julio: El Banco Central de la República Argentina se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 04/2005 del 12/07/2005).

El Instituto Nacional de la Propiedad Industrial se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 05/2005 del 20/07/2005).

Septiembre: La Administración de Programas Especiales se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI Nº 08/2005 del 09/09/2005).

Se extiende el período de validez del certificado de la AC-ONTI (Disposición ONTI Nº 09/2005 del 20/09/2005).

Se inicia la participación en el Proyecto Piloto de Certificados de Origen Digitales de ALADI (Asociación Latinoamericana de Integración).

Año 2006

Marzo: La ONTI publica en su sitio web los documentos que conforman la última versión del anteproyecto normativo referido al otorgamiento y revocación de licencias a los certificadores.

El Superior Tribunal de Justicia de la Provincia de Córdoba se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI 05/2006 del 01/03/2006).

El Gobierno de la Provincia de Tucumán se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI 6/2006 del 31/03/2006).

En el marco del Convenio de Cooperación firmado con el Gobierno de la Provincia de Chubut, se acuerda un plan de trabajo a fin de colaborar en la implementación de la tecnología de firma digital en la Dirección General de Gobierno Digital del Gobierno Provincial, para luego hacer extensible la tecnología citada a todas las áreas del Gobierno Provincial.

En el marco del Convenio de Cooperación firmado con el Gobierno de la Provincia de La Pampa, se acuerda un plan de trabajo a fin de colaborar en la implementación de la tecnología de firma digital en la Subsecretaría de Planeamiento y Control de Gestión del Gobierno Provincial, para luego hacer extensible la tecnología citada a todas las áreas de dicho Gobierno.

Junio: Se participa del Taller de Infraestructura de Claves Públicas y firma electrónica sobre software libre, a través de una teleconferencia organizada por SUSCERTE (Superintendencia de Servicios de Certificación Electrónica de Venezuela).

El Poder Ejecutivo Nacional aprueba el Decreto Nº 724/06 modificatorio del Decreto Nº 2628/02 reglamentario de la Ley Nº 25.506 de Firma Digital.

El Gobierno de la Provincia de Corrientes se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI 8/2006 del 14/06/2006).

La Sindicatura General de la Nación se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI 11/2006 del 29/06/2006).

El Gobierno de la Provincia de Chubut se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI 9/2006 del 29/06/2006).

Agosto: En el marco del Convenio de Cooperación firmado con el Gobierno de la Provincia de Entre Ríos, se acuerda un plan de trabajo a fin de colaborar en la implementación de la tecnología de firma digital en el Gobierno Provincial.

Setiembre: El Superior Tribunal de Justicia de la Provincia de Tucumán se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI 12/2006 del 04/09/2006).

El Superior Tribunal de Justicia de la Provincia de Santa Fe se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI 13/2006 del 15/09/2006).

El Gobierno de la Provincia de La Pampa se constituye en Autoridad de Registro de la AC-ONTI (Disposición ONTI 14/2006 del 15/09/2006).

Año 2007

El Poder Judicial de Córdoba, autoriza la firma digital en las sentencias de los Juzgados a cargo de las ejecuciones fiscales.

Existen antecedentes normativos que prevén la validez jurídica y eficacia probatoria de determinados documentos, si se satisfaces las condiciones de operatividad y autenticidad exigidas.

En efecto en el ámbito del Derecho Comercial, el art. 53 del Código de Comercio en materia de documentación contable y libros de comercio ha sido alterado por el art. 61 de la ley 19.550, al permitirse a las sociedades adoptar, bajo ciertas condiciones y límites, sistemas contemporáneos de contabilidad, permitiéndose la sustitución de las formalidades impuestas por ordenadores, medios mecánicos y o magnéticos u otros, exigiéndose la descripción del sistema y previa autorización.

Además hay que tener presente que hay instrumentos que siendo públicos, no llevan firma como, por ejemplo, en las acciones de las Sociedades

Anónimas, la autoridad de contralor, puede autorizar el reemplazo de la firma por una impresión que garantice la autenticidad de esos títulos, art. 212 ley 19.550, siendo instrumentos públicos según lo establecido por el art. 979 inc. 8 del Código Civil.

Otro antecedente importante es el tema que incorporó la ley 24.624, Complementaria del Presupuesto General de la Administración Nacional, que en su art. 30 prevé que la documentación financiera, la de personal y la de control de la Administración Pública Nacional podrá ser archivada y conservada en soporte electrónico u óptico indeleble, cualquiera sea el soporte primario en que estén redactados y construidos. Asimismo, dispone, que los documentos redactados en primera generación en soporte electrónico u óptico indeleble a partir de originales en cualquier soporte, serán considerados originales y poseerán, en consecuencia, pleno valor probatorio en los términos del Código Civil, facultando al Jefe de Gabinete de Ministros a reglamentar aquellas disposiciones.

Por otra parte el Poder Ejecutivo Nacional, a través de la aprobación del decreto Nº 427 del dieciséis de abril de 1998, dispuso la creación de la Infraestructura de firma Digital, aplicable a la Administración Pública Nacional (IFDAPN).

En su primer artículo ésta norma establece el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa, en las condiciones definidas en la infraestructura de Firma Digital para el Sector Público Nacional.

En el régimen del decreto la firma digital tendrá los mismos efectos de la firma ológrafa.

También podemos mencionar como antecedente la resolución MTSS 555/97 del Ministerio de Trabajo y Seguridad Social que determina los procedimientos para la incorporación de documentos digitales y la firma digital. La resolución Nº 45/97, 212/97 y 194/98 de la Secretaría de la Función Pública que reglamentó la incorporación de tecnología de la firma digital, estándares e infraestructura de Superintendencia de Administradoras de Fondos de Jubilaciones y Pensiones, de Incorporación del Correo Electrónico con Firma Digital.

Por último se dictó el decreto Nº 677/2001 que establece el Régimen de Transparencia de la Oferta pública, que acepta la posibilidad de celebrar reuniones de directorio y asambleas a través de medios no presenciales y modifica la ley 24.083 y se establece una serie de pautas referidas a la designación de la Comisión Nacional de Valores como autoridad de aplicación otorgando a ése organismo expresas facultades para establecer regímenes de información y requisitos diferenciales, previendo el sistema de la firma digital.

ANEXO II

Ley de Firma Digital

Ley 25.506

Sancionada: Noviembre 14 de 2001.

Promulgada de Hecho: Diciembre 11 de 2001.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

CAPITULO I

Consideraciones generales

ARTICULO 1º — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

ARTICULO 2º — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTICULO 3º — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

ARTICULO 4º — Exclusiones. Las disposiciones de esta ley no son aplicables:

a) A las disposiciones por causa de muerte;

b) A los actos jurídicos del derecho de familia;

c) A los actos personalísimos en general;

d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

ARTICULO 5º — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera

lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTICULO 6º — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTICULO 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

ARTICULO 8º — Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTICULO 9º — Validez. Una firma digital es válida si cumple con los siguientes requisitos:

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 presente, por un certificador licenciado.

ARTICULO 10. — Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

ARTICULO 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTICULO 12. — Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

CAPITULO II

De los certificados digitales

ARTICULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTICULO 14. — Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

a) Ser emitidos por un certificador licenciado por el ente licenciante;

b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:

1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;

2. Ser susceptible de verificación respecto de su estado de revocación;

3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;

4. Contemplar la información necesaria para la verificación de la firma;

5. Identificar la política de certificación bajo la cual fue emitido.

ARTICULO 15. — Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

ARTICULO 16. — Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o

b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

CAPITULO III

Del certificador licenciado

ARTICULO 17. — Del certificador licenciado. Se entiende por certificador licenciado a 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.

ARTICULO 18. — Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

ARTICULO 19. — Funciones. El certificador licenciado tiene las siguientes funciones:

a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;

b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;

c) Identificar inequívocamente los certificados digitales emitidos;

d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;

e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

1) A solicitud del titular del certificado digital.

2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.

5) Por resolución judicial o de la autoridad de aplicación.

f) Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

ARTICULO 20. — Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

ARTICULO 21. — Obligaciones. Son obligaciones del certificador licenciado:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;

c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

g) Mantener la confidencialidad de toda información que no figure en el certificado digital;

h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;

k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;

l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;

m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;

p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;

q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;

r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;

s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

u) Constituir domicilio legal en la República Argentina;

v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;

w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

ARTICULO 22. — Cese del certificador. El certificador licenciado cesa en tal calidad:

a) Por decisión unilateral comunicada al ente licenciante;

b) Por cancelación de su personería jurídica;

c) Por cancelación de su licencia dispuesta por el ente licenciante.

La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

ARTICULO 23. — Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:

a) Para alguna finalidad diferente a los fines para los cuales fue extendido;

b) Para operaciones que superen el valor máximo autorizado cuando corresponda;

c) Una vez revocado.

CAPITULO IV

Del titular de un certificado digital

ARTICULO 24. — Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;

c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;

d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

e) A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

ARTICULO 25. — Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;

c) 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;

d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

CAPITULO V

De la organización institucional

ARTICULO 26. — Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

ARTICULO 27. — Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

ARTICULO 28. — Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

CAPITULO VI

De la autoridad de aplicación

ARTICULO 29. — Autoridad de Aplicación. La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

ARTICULO 30. — Funciones. La autoridad de aplicación tiene las siguientes funciones:

a) Dictar las normas reglamentarias y de aplicación de la presente;

b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;

c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;

d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;

e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;

f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;

g) Determinar los niveles de licenciamiento;

h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;

i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;

j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;

k) Aplicar las sanciones previstas en la presente ley.

ARTICULO 31. — Obligaciones. En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:

a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;

b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;

c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;

d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;

e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

ARTICULO 32. — Arancelamiento. La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

CAPITULO VII

Del sistema de auditoría

ARTICULO 33. — Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación.

La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

ARTICULO 34. — Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

CAPITULO VIII

De la Comisión Asesora para la Infraestructura de Firma Digital

ARTICULO 35. — Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

ARTICULO 36. — Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

a) Estándares tecnológicos;

b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;

c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;

d) Metodología y requerimiento del resguardo físico de la información;

e) Otros que le sean requeridos por la autoridad de aplicación.

CAPITULO IX

Responsabilidad

ARTICULO 37. — Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente.

ARTICULO 38. — Responsabilidad de los certificadores licenciados ante terceros.

El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

ARTICULO 39. — Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;

b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X

Sanciones

ARTICULO 40. — Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

ARTICULO 41. — Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

a) Apercibimiento;

b) Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000);

c) Caducidad de la licencia.

Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación.

El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

ARTICULO 42. — Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:

a) Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;

b) No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones;

c) Cualquier otra infracción a la presente ley que no tenga una sanción mayor.

ARTICULO 43. — Multa. Podrá aplicarse sanción de multa en los siguientes casos:

a) Incumplimiento de las obligaciones previstas en el artículo 21;

b) Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios terceros, o se afectare gravemente la seguridad de los servicios de certificación;

c) Omisión de llevar el registro de los certificados expedidos;

d) Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;

e) Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante;

f) Incumplimiento de las normas dictadas por la autoridad de aplicación;

g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.

ARTICULO 44. — Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:

a) No tomar los debidos recaudos de seguridad en los servicios de certificación;

b) Expedición de certificados falsos;

c) Transferencia no autorizada o fraude en la titularidad de la licencia;

d) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;

e) Quiebra del titular.

La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

ARTICULO 45. — Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTICULO 46. — Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

CAPITULO XI

Disposiciones Complementarias

ARTICULO 47. — Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

ARTICULO 48. — Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156.

ARTICULO 49. — Reglamentación. El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTICULO 50. — Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

ARTICULO 51. — Equiparación a los efectos del derecho penal. Incorpórase el siguiente texto como artículo 78 (bis) del Código Penal:

Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

ARTICULO 52. — Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

ARTICULO 53. — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CATORCE DIAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL UNO.

— REGISTRADA BAJO EL Nº 25.506 —

RAFAEL PASCUAL. — EDUARDO MENEM. — Guillermo Aramburu. — Juan C. Oyarzún.

ANEXO III

Reglamentación de la Ley Nº 25.506.

Decreto 2628/2002

Consideraciones Generales. Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital. Ente Administrador de Firma Digital. Sistema de Auditoría. Estándares Tecnológicos. Revocación de Certificados Digitales. Certificadores Licenciados. Autoridades de Registro. Disposiciones para la Administración Pública Nacional.

Bs. As., 19/12/2002

VISTO la Ley Nº 25.506, el Decreto Nº 427 del 16 de abril de 1998, el Decreto Nº 78 del 10 de enero de 2002, el Decreto Nº 333 del 19 de febrero de 1985 y sus modificatorios y la Resolución Nº 194 del 27 de noviembre de 1998 de la ex SECRETARIA DE LA FUNCION PUBLICA, y

CONSIDERANDO:

Que la sanción de la Ley Nº 25.506 de firma digital representa un avance significativo para la inserción, de nuestro país en la sociedad de la información y en la economía digital, brindando una oportunidad para el desarrollo del sector productivo vinculado a las nuevas tecnologías.

Que otros países ya han normado sobre la materia, con positiva repercusión tanto en el ámbito privado como público.

Que con la sanción de la citada Ley Nº 25.506, de firma digital se reconoce el empleo de la firma, digital y de la firma electrónica y su eficacia jurídica en las condiciones que la misma ley establece.

Que dicho reconocimiento constituye un elemento esencial para otorgar seguridad a las transacciones electrónicas, promoviendo el comercio electrónico seguro, de modo de permitir la identificación en forma fehaciente de las personas que realicen transacciones electrónicas.

Que asimismo, la sanción de la Ley Nº 25.506 otorga un decisivo impulso para la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información pública y posibilitar la realización de trámites por Internet en forma segura.

Que la reglamentación de la Ley Nº 25.506 permitirá establecer una Infraestructura de Firma Digital que ofrezca autenticación, y garantía de integridad para los documentos digitales o electrónicos y constituir la base tecnológica que permita otorgarles validez jurídica.

Que debe regularse el funcionamiento de los certificadores licenciados de manera de garantizar la adecuada prestación de los servicios de certificación.

Que resulta necesario crear un Ente Administrador de Firma Digital, encargado de otorgar las licencias a los certificadores, supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de Firma Digital.

Que la citada Ley contempla la creación de una Comisión Asesora para la Infraestructura de Firma Digital, conformada por un equipo multidisciplinario de especialistas en la materia, con el fin de asesorar y recomendar a la Autoridad de Aplicación estándares tecnológicos, y otros aspectos que hacen al funcionamiento de la mencionada Infraestructura, por lo cual deben establecerse las bases para su formación y adecuado funcionamiento.

Que el Decreto Nº 427 del 16 de abril de 1998 ha sido una de las normas pioneras a nivel nacional e internacional en reconocer la validez jurídica de la firma digital, para lo cual creó una Infraestructura de Firma Digital para el Sector Público Nacional bajo la dependencia de la JEFATURA DE GABINETE DE MINISTROS.

Que esta experiencia ha sido un antecedente fundamental para la incorporación de la tecnología en la gestión pública, constituyendo una fuente de consulta para distintas jurisdicciones nacionales y provinciales.

Que dado que la Ley Nº 25.506 establece una Infraestructura de Firma Digital de alcance federal, a fin de optimizar el aprovechamiento de los recursos y las experiencias desarrolladas, resulta conveniente subsumir la mencionada Infraestructura del Sector Público Nacional dentro de la creada a nivel federal por la Ley citada.

Que a tal fin, corresponde derogar el Decreto Nº 427/98, por el cual se reconoce el empleo de la firma digital en el ámbito de la Administración Pública Nacional, ya que la Ley Nº 25.506 cubre los objetivos y el alcance del mencionado Decreto.

Que ha tomado intervención el servicio jurídico competente.

Que la presente medida se dicta en virtud lo dispuesto por el artículo 49 de la Ley Nº 25.506, y por el artículo 99, inciso 2, de la Constitución de la Nación Argentina.

Por ello,

EL PRESIDENTE
DE LA NACION ARGENTINA
DECRETA:

CAPITULO I

CONSIDERACIONES GENERALES

Artículo 1º — Objeto. La presente reglamentación regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.

En los casos contemplados por los artículos 3º, 4º y 5º de la Ley Nº 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad:

a) Firma electrónica,

b) Firma digital basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación,

c) Firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación,

d) Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos:

1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero.

2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.

Art. 2º — Validez de los certificados, digitales emitidos por certificadores no licenciados. Los certificados digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma electrónica.

Art. 3º — Certificados digitales emitidos por certificadores licenciados. Los certificados digitales contemplados, en el artículo 13 de la Ley Nº 25.506 son aquellos cuya utilización permite disponer de una firma digital amparada por las presunciones de autoría e integridad establecidas en los artículos 7º y 8º de la ley citada.

CAPITULO II

DE LA AUTORIDAD DE APLICACION

Art. 4º — Normas técnicas. Facúltase a la JEFATURA DE GABINETE DE MINISTROS, a determinar las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto en los artículos 11 y 12 de la Ley Nº 25.506.

Art. 5º — Conservación. El cumplimiento de la exigencia legal de conservar documentos, registros o datos, conforme a la legislación vigente a la materia, podrá quedar satisfecha con la conservación de los correspondientes, documentos digitales firmados digitalmente. Los documentos, registros o datos electrónicos, deberán ser almacenados por los intervinientes o por terceros confiables aceptados por los intervinientes, durante los plazos establecidos en las normas específicas.

Se podrán obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. La certificación de autenticidad se hará de con-

formidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia.

Art. 6º — Regulación. Facúltase a la JEFATURA DE GABINETE DE MINISTROS a establecer:

a) Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales.

b) Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente.

c) Las condiciones mínimas de emisión de certificados digitales.

d) Los casos en los cuales deben revocarse los certificados digitales.

e) Los datos considerados públicos contenidos en los certificados digitales.

f) Los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados.

g) La información que los certificadores licenciados deberán publicar por internet.

h) La información que los certificadores licenciados deberán publicar en el Boletín Oficial.

i) Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad.

j) El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías.

k) Las condiciones y procedimientos para el otorgamiento y revocación de las licencias.

l) Las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales.

m) El reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital.

n) El procedimiento de instrucción sumarial y la gradación de sanciones previstas en la Ley Nº 25.506, en virtud de reincidencia y/u oportunidad.

o) Los procedimientos aplicables para el reconocimiento de certificados extranjeros.

p) Las condiciones de aplicación de la presente ley en el Sector Público Nacional, incluyendo la autorización para prestar servicios de certificación digital para las entidades y jurisdicciones de la Administración Pública Nacional.

q) Los contenidos mínimos de las políticas de certificación de acuerdo con los estándares nacionales e internacionales y las condiciones mínimas que deberán cumplirse en el caso de cese de actividades de un certificador licenciado.

r) Los niveles de licenciamiento.

s) Reglamentar el uso y los alcances de los certificados de firma digital emitidos por los Registros Públicos de Contratos.

t) Exigir las garantías y seguros necesarios para prestar el servicio previsto.

u) Las condiciones de prestación de otros servicios en relación con la firma digital y otros temas cubiertos en la ley.

CAPITULO III

DE LA COMISION ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL

Art. 7º — Comisión Asesora para la Infraestructura de Firma Digital. En el ámbito de la JEFATURA DE GABINETE DE MINISTROS funcionará la Comisión Asesora para la Infraestructura de Firma Digital, que se constituirá de acuerdo a lo dispuesto por el artículo 35 de la Ley Nº 25.506.

Art. 8º — Integración. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por profesionales de carreras afines a la actividad, de reconocida trayectoria y experiencia, provenientes de organismos del Estado Nacional, Universidades, Cámaras, Colegios u otros entes representativos profesionales. Para integrar la Comisión Asesora para la Infraestructura de Firma Digital se deberán reunir los siguientes requisitos:

a) Poseer título universitario, expedido por Universidad Nacional o privada reconocida por el Estado, correspondiente a carrera profesional de duración no inferior a CUATRO (4) años, con incumbencias relacionadas con la materia.

b) Antecedentes académicos y/o profesionales o laborales en la materia.

Art. 9º — Ejercicio de funciones. El ejercicio de las funciones como miembro de la Comisión Asesora para la Infraestructura de Firma Digital será ad honorem.

Art. 10. — Consulta Pública. La Comisión Asesora para la Infraestructura de Firma Digital establecerá los mecanismos que permitan mantener un intercambio de información fluido con organismos públicos, Cámaras, usuarios y asociaciones de consumidores sobre los temas que se está tratando a los efectos de recibir aportes y opiniones. Para cumplir con este cometido podrá implementar consultas públicas presenciales, por escrito o mediante foros virtuales, abiertos e indiscriminados, o cualquier otro medio que la Comisión considere conveniente o necesario.

CAPITULO IV

DEL ENTE ADMINISTRADOR DE FIRMA DIGITAL

Art. 11. — Ente Administrador de Firma Digital. Créase el Ente Administrador de Firma Digital dependiente de la JEFATURA DE GABINETE DE MINISTROS, como órgano técnico, administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad, según las exigencias instituidas por el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro y de dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios.

Art. 12. — Autoridades del Ente Administrador de Firma Digital. El Ente Administrador de Firma Digital será conducido por un Directorio integrado por TRES (3) miembros, designados por el JEFE DE GABINETE DE MINISTROS, previo concurso. Hasta tanto, sea realizado el concurso el JEFE DE GABINETE DE MINISTROS designará a los integrantes del Directorio, uno de los cuales ocupará el cargo de Presidente del Ente. El gerenciamiento del Ente estará a cargo del Coordinador Ejecutivo designado por el JEFE DE GABINETE DE MINISTROS.

Art. 13. — Funciones del Ente Administrador.

Son funciones del Ente Administrador:

a) Otorgar las licencias habilitantes para acreditar a los certificadores en las condiciones que fijen el presente decreto y las normas reglamentarias, modificatorias o de aplicación que se dicten en el futuro.

b) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados.

c) Denegar las solicitudes de licencia a los prestadores de servicios de certificación que no cumplan con los requisitos establecidos, para su licenciamiento.

d) Revocar las licencias otorgadas a los Certificadores licenciados que dejen de cumplir con los requisitos establecidos para su licenciamiento.

e) Aprobar las políticas de certificación, el manual de procedimiento, el plan de seguridad, de cese de actividades y el plan de contingencia, presentado por los certificadores solicitantes de la licencia o licenciados.

f) Solicitar los informes de auditoría en los casos que correspondiere.

g) Realizar inspecciones a los certificadores licenciados por sí o por terceros.

h) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la presente reglamentación.

i) Disponer la instrucción sumarial, la aplicación de sanciones e inhabilitar en forma temporal o permanente a todo certificador o licenciado que no respetare o incumpliere los requerimientos y disposiciones de la Ley Nº 25.506, el presente decreto y las normas complementarias.

j) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos, direcciones de internet y certificados digitales de los certificadores licenciados.

k) Publicar en internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, los números telefónicos, direcciones de internet y certificados digitales de los certificadores cuyas licencias han sido revocadas.

I) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, el domicilio, números telefónicos, direcciones de internet y certificados digitales del Ente Administrador.

m) Administrar los recursos generados de acuerdo con lo dispuesto por el artículo 16 de la presente reglamentación, provenientes de las distintas fuentes de financiamiento.

n) Fijar el concepto y los importes de todo tipo de aranceles y multas previstos en la Ley Nº 25.506 y en el artículo 16 de la presente reglamentación.

o) Solicitar la ampliación o aclaración sobre la documentación presentada por el certificador.

p) Dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios.

Art. 14. — Obligaciones del Ente Administrador.

El Ente Administrador tiene idénticas obligaciones que los titulares, de certificados y que los Certificadores Licenciados, en su caso, y además debe:

a) Permitir el acceso público permanente a la nómina actualizada de certificadores licenciados con los datos correspondientes.

b) Supervisar la ejecución del plan de cese de actividades de los Certificadores licenciados que discontinúan sus funciones;

c) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

d) Supervisar la ejecución de planes de contingencia de los certificadores licenciados.

e) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas por el Ente Administrador para determinar si se han tomado las acciones correctivas correspondientes.

f) Recibir, evaluar y resolver los reclamos de los usuarios de certificados digitales relativos a la prestación del servicio por parte de certificadores licenciados.

Art. 15. — Organización del Ente Administrador. Dentro del plazo de SESENTA (60) días corridos de la fecha de constitución del Directorio, el ENTE ADMINISTRADOR DE FIRMA DIGITAL elevará para su consideración al JEFE DE GABINETE DE MINISTROS la propuesta de su estructura organizativa y de su reglamento de funcionamiento.

Art. 16. — Recursos del Ente Administrador. El Ente Administrador podrá arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con:

a) Los importes provenientes de los aranceles que se abonen por la provisión de los siguientes servicios:

1.— Servicios de certificación digital,

2.— Servicios de certificación digital de fecha y hora,

3.— Servicios de almacenamiento seguro de documentos electrónicos,

4.— Servicios prestados por autoridades de registro,

5. — Servicios prestados por terceras partes confiables,

6. — Servicios de certificación de documentos electrónicos firmados digitalmente

7.— Otros servicios o actividades relacionados a la firma digital.

b) Los importes provenientes de los aranceles de homologación de dispositivos de creación y verificación de firmas digitales.

c) Los importes provenientes de los aranceles de certificación de sistemas que utilizan firma digital.

d) Los importes provenientes de los aranceles de administración del sistema de auditoría y las auditorías que el organismo realice por sí o por terceros.

e) Los subsidios, herencias, legados, donaciones o transferencias bajo cualquier título que reciba.

f) El producido de multas.

g) Los importes que se le asignen en el cálculo de recursos de la respectiva ley de presupuesto para la administración nacional.

h) Los demás fondos, bienes, o recursos que puedan serle asignados en virtud de las leyes y reglamentaciones aplicables.

Art. 17. — Financiamiento del Ente Administrador. Instrúyese a la JEFATURA DE GABINETE DE MINISTROS para que proceda a incluir en su presupuesto los fondos necesarios para que el Ente Administrador pueda cumplir adecuadamente sus funciones.

Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta que se incluyan las partidas necesarias en el Presupuesto Nacional los costos de financiamiento del Ente Administrador serán afrontados con el crédito presupuestario correspondiente a la JEFATURA DE GABINETE DE MINISTROS.

CAPITULO V

DEL SISTEMA DE AUDITORIA

Art. 18. — Precalificación de entidades de auditoría. La JEFATURA DE GABINETE DE MINISTROS convocará a concurso público para la precalificación de entidades de auditoría entre las universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales, que acrediten experiencia profesional acorde en la materia, interesadas en prestar el servicio de auditoría de entidades prestadoras de servicios de certificación digital. A tal fin, elaborará un Pliego Estándar de Precalificación de Entidades de Auditoría, y determinará la periodicidad de la convocatoria.

Art. 19. — Informe de auditoría. El informe de auditoría evaluará los sistemas utilizados por el certificador de acuerdo con los requerimientos de la Ley Nº 25.506, el presente decreto y las normas complementarias.

Art. 20. — Conflicto de intereses. Para garantizar la objetividad e imparcialidad de la actividad de auditoría no podrán desempeñarse en la prestación de servicios de auditoría aquellas entidades o personas vinculadas con prestadores de servicios de certificación, lo que será establecido en el Pliego Estándar de Precalificación de Entidades de Auditoría previsto en el artículo 18 del presente decreto.

Art. 21. — Deber de confidencialidad. Las entidades auditantes y las personas que efectúen las auditorías deben mantener la confidencialidad sobre la información considerada amparada bajo normas de confidencialidad por el Certificado Licenciado.

CAPITULO VI

DE LOS ESTANDARES TECNOLOGICOS

Art. 22. — Aplicación provisoria de los estándares vigentes. Hasta tanto la JEFATURA DE GABINETE DE MINISTROS apruebe los Estándares Tecnológicos de Infraestructura de Firma Digital en consonancia con estándares

tecnológicos internacionales, mantendrán su vigencia los establecidos en la Resolución Nº 194/98 de la ex Secretaría de la Función Publica.

CAPITULO VII

DE LA REVOCACION DE CERTIFICADOS DIGITALES

Art. 23. — Revocación de certificados. Se deberán revocar los certificados digitales emitidos en los siguientes casos:

a) A solicitud del titular del certificado digital

b) Si se determina que un certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación.

c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) Por condiciones especiales definidas en las Políticas de Certificación.

e) Por Resolución Judicial o de la Autoridad de Aplicación debidamente fundada.

f) Por fallecimiento del titular.

g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.

h) Por declaración judicial de incapacidad del titular.

i) Si se determina que la información contenida en el certificado ha dejado de ser válida.

j) Por el cese de la relación de representación respecto de una persona.

CAPITULO VIII

DE LOS CERTIFICADORES LICENCIADOS

Art. 24. — Obtención de la licencia. Para obtener una licencia, los proveedores de servicios de certificación deberán particularizar las actividades para las cuales requieren la licencia y acreditar por los medios que este determine ante el Ente Administrador de Firma Digital:

a) Documentación que demuestre:

1.— En el caso de personas jurídicas, su personería.

2.— En el caso de registro público de contratos, tal condición

3.— En el caso de organización pública, la autorización de su máxima autoridad para iniciar el proceso de licenciamiento y la correspondiente aprobación de la JEFATURA DE GABINETE DE MINISTROS, de acuerdo con lo dispuesto en el artículo 41 de la presente reglamentación.

b) El cumplimiento de las condiciones establecidas en la ley; este decreto y las normas complementarias.

c) Las políticas de certificación para las cuales solicita licencia que respaldan la emisión de sus certificados, Manual de Procedimientos, Plan de Seguridad, Plan de Cese de Actividades y Plan de Contingencia satisfactorias de acuerdo con las normas reglamentarias.

d) Toda aquella información o requerimiento, que demande la Autoridad de Aplicación.

Art. 25. — Efectos del licenciamiento. El otorgamiento de la licencia no implica que el Ente Administrador de la Infraestructura de Firma Digital, la JEFATURA DE GABINETE DE MINISTROS, las entidades auditantes o cualquier organismo del Estado garantice la provisión de los servicios de certificación o los productos provistos por el Certificador Licenciado.

Art. 26. — Duración de la licencia. Las licencias tendrán un plazo de duración de CINCO (5) años y podrán ser renovadas.

Los certificadores licenciados deberán efectuar anualmente una declaración jurada en la cual conste el cumplimiento de las normas establecidas en la Ley Nº 25.506, en el presente decreto y en las normas complementarias.

Los certificadores licenciados serán sometidos a auditorías anuales.

Art. 27. — Causales de caducidad de la licencia. El Ente Administrador podrá disponer de oficio, y en forma preventiva la caducidad de la licencia en los siguientes casos:

a) Falta de presentación de la declaración jurada anual.

b) Falsedad de los datos contenidos en la declaración jurada anual.

c) Dictamen desfavorable de auditoría basado en causales graves.

d) Informe de la inspección dispuesta por el Ente Administrador desfavorable basado, en causales graves.

e) Cuando el certificador licenciado no permita la realización de auditorías o inspecciones dispuestas por el Ente Administrador.

Art. 28. — Reconocimiento de certificados extranjeros. De acuerdo a lo establecido en el artículo 6º de la presente reglamentación, facúltase a la JEFATURA DE GABINETE DE MINISTROS a elaborar y firmar acuerdos de reciprocidad con gobiernos de países extranjeros, a fin de otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por certificadores de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la Ley Nº 25.506 y su reglamentación para los certificados emitidos por certificadores nacionales.

Los certificadores licenciados no podrán reconocer certificaciones emitidas por certificadores extranjeros correspondientes a personas con domicilio o residencia en la República Argentina. El Ente Administrador de Firma Digital establecerá las relaciones que los certificadores licenciados deberán guardar entre los certificados emitidos en la República Argentina y los certificados reconocidos de certificadores extranjeros.

Art. 29. — Políticas de Certificación. La JEFATURA DE GABINETE DE MINISTROS definirá el contenido, mínimo de las políticas de certificación de acuerdo con los estándares nacionales e internacionales vigentes, las que deberán contener al menos la siguiente información:

a) Identificación del certificador licenciado.

b) Política de administración de los certificados y detalles de los servicios arancelados.

c) Obligaciones de la entidad y de los suscriptores de los certificados.

d) Tratamiento de la información suministrada por los suscriptores, y resguardo de la confidencialidad en su caso.

e) Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.

Art. 30. — Seguros. El certificador licenciado debe contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los siguientes requisitos.

a) Ser expedidos por una entidad aseguradora autorizada para operar en la República Argentina.

b) Establecer la obligación de la entidad aseguradora de informar previamente al Ente Administrador de la Infraestructura de Firma Digital la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.

Los certificadores licenciados pertenecientes a entidades y jurisdicciones del sector público quedarán exentos de la obligación de constituir el seguro previsto en el presente artículo.

Art. 31. — Responsabilidad de los certificadores licenciados. En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un certificador licenciado, público o privado, comprometerá la responsabilidad pecuniaria del Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital.

Art. 32. — Recursos de los certificadores licenciados. Para el desarrollo adecuado de las actividades de certificación, el certificador deberá acreditar que cuenta con un equipo de profesionales, infraestructura física tecnológica

y recursos financieros, como así también procedimientos y sistemas de seguridad que permitan:

a) Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.

b) Cumplir con lo previsto en sus políticas y procedimientos de certificación.

c) Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la Autoridad de Aplicación.

d) Expedir certificados que cumplan con:

1.— Lo previsto en los artículos 13 y 14 de la Ley Nº 25.506.

2.— Los estándares tecnológicos aprobados por la JEFATURA DE GABINETE DE MINISTROS.

e) Garantizar la existencia de sistemas de seguridad física y lógica que cumplimenten las normativas vigentes.

f) Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado.

g) Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.

h) Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.

i) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.

j) Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deban ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación.

k) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.

l) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

Art. 33. — Servicios de Terceros. En los casos en que el certificador licenciado requiera o utilice los servicios de infraestructura tecnológicos prestados por un tercero, deberá prever dentro de su Plan de Contingencia los procedi-

mientos a seguir en caso de interrupción de estos servicios, de modo tal que permita continuar prestando sus servicios de certificación sin ningún perjuicio para los suscriptores.

Los contratos entre el certificador licenciado y los proveedores de servicios o infraestructura deberán garantizar la ejecución de los procedimientos contemplados en el Plan de Cese de actividades aprobado por el Ente Licenciante. El certificador licenciado o en proceso de licenciamiento deberá facilitar al Ente Licenciante toda aquella información obrante en los contratos vinculada a la prestación de servicios de certificación y a la implementación del Plan de Cese de actividades y el Plan de Contingencia.

La contratación de servicios o infraestructura no exime al prestador de la presentación de los informes de auditoría, los cuales deberán incluir los sistemas y seguridades del prestador contratado.

Art. 34. — Obligaciones del certificador licenciado. Además de lo previsto en el artículo 21 de la Ley Nº 25.506, los certificadores licenciados deberán:

a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.

b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.

d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.

e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.

g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.

i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

j) Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

l) Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;

m) Cumplir las normas y recaudos establecidos para la protección de datos personales.

n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley Nº 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.

El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.

o) Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada.

p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.

q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

CAPITULO IX

DE LAS AUTORIDADES DE REGISTRO

Art. 35. — Funciones de las Autoridades de Registro. Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación.

Una autoridad de Registro es una entidad responsable de las siguientes funciones:

a) La recepción de las solicitudes de emisión de certificados.

b) La validación de la identidad y autenticación de los datos de los titulares de certificados.

c) La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.

d) La remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.

e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.

f) La identificación y autenticación de los solicitantes de revocación de certificados.

g) El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.

h) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.

i) El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Art. 36. — Responsabilidad del certificador licenciado respecto de la Autoridad de Registro. Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado. El Certificador, Licenciado es responsable con los alcances establecidos en la Ley Nº 25.506, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

CAPITULO X

DISPOSICIONES PARA LA ADMINISTRACION PUBLICA NACIONAL

Art. 37. — Despapelización del Estado. Sin perjuicio de la aplicación directa de la ley en lo relativo a la validez jurídica de la firma electrónica, de la firma digital y de los documentos digitales, la implementación de las disposiciones de la ley y del presente decreto para la digitalización de procedimientos y trámites internos de la Administración Pública Nacional, de las Administraciones Públicas Provinciales, y de los Poderes Legislativos y Judiciales del orden nacional y provincial, así como los vinculados a la relación de las mencionadas jurisdicciones y entidades con los administrados, se hará de acuerdo a lo que fijen reglamentariamente cada uno de los Poderes y Administraciones.

Art. 38. — Aplicaciones en organismos de la Administración Pública Nacional. Los organismos de la Administración Pública Nacional que para la tramitación de documentos digitales o la implementación de aplicaciones requieran firma digital, solamente aceptarán certificados digitales emitidos por Certificadores, Licenciados, o certificados digitales emitidos por certificadores extranjeros reconocidos por acuerdos internacionales o por certificadores licenciados del país.

Las entidades y jurisdicciones pertenecientes al sector público podrán ser certificadores licenciados y emitir certificados para agentes y funcionarios públicos destinados a las aplicaciones de gestión interna de los organismos públicos a que éstos pertenecieran. Cuando razones de orden público o de interés social lo ameriten y cuenten con la autorización de la JEFATURA DE GABINETE DE MINISTROS podrán emitir certificados a particulares.

En aquellas aplicaciones en las que el Estado interactúe con la comunidad, se deberá admitir la recepción de documentos digitales firmados digitalmente utilizando certificados digitales emitidos por certificadores licenciados privados o públicos, indistintamente.

Art. 39. — Autoridades de Registro pertenecientes a la Administración Pública Nacional. En las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional, las áreas de recursos humanos cumplirán las funciones de Autoridades de Registro para los agentes y funcionarios de su jurisdicción. En el caso, y si las aplicaciones de que se trate lo requieren, la máxima autoridad del organismo podrá asignar, adicionalmente, a otra unidad las funciones de Autoridad de Registro.

Art. 40. — Agentes y funcionarios. La Autoridad de Aplicación podrá requerir para el cumplimiento de lo establecido en la presente reglamentación la adscripción de agentes y funcionarios pertenecientes a las entidades y jurisdicciones comprendidas en el artículo 8º de la Ley Nº 24.156 y sus modificatorias.

Art. 41. — Utilización por las entidades y jurisdicciones de la Administración Pública Nacional. La JEFATURA DE GABINETE DE MINISTROS, establecerá las normas de aplicación de la presente reglamentación en la Administración Pública Nacional, que deberán contemplar:

a) Las acciones tendientes a promover el uso masivo de la firma digital con el fin de posibilitar el trámite de los expedientes en forma simultánea, búsquedas automáticas de información, seguimiento y control por parte de los interesados.

b) Las acciones tendientes a implementar la progresiva despapelización del Estado, a fin de contar en un plazo de CINCO (5) años con la totalidad de la documentación administrativa en formato digital.

c) La interoperabilidad entre aplicaciones.

d) La autorización para solicitar el licenciamiento como certificador ante el Ente Administrador de la Infraestructura de Firma Digital para las entidades y jurisdicciones de la Administración Pública Nacional.

e) La participación del Cuerpo de Administradores Gubernamentales a los fines de difundir el uso de la firma digital y facilitar los procesos de despapelización.

Art. 42. — Presentación de documentos electrónicos. Los organismos de la Administración Pública Nacional deberán establecer mecanismos que garanticen la opción de remisión, recepción, mantenimiento y publicación de información electrónica, siempre que esto sea aplicable, tanto para la gestión de documentos entre organismos como para con los ciudadanos.

Art. 43. — Normas para la elaboración y redacción de la documentación administrativa. Lo dispuesto en la presente reglamentación constituye una alternativa a lo establecido por el Decreto Nº 333/85 y sus modificatorios.

Art. 44. — Glosario. Apruébase el glosario que obra como Anexo I del presente Decreto.

Art. 45. — Derogación. Derógase el Decreto Nº 427/98.

Art. 46. — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — DUHALDE. — Alfredo N. Atanasof. — Juan J. Alvarez.

ANEXO I GLOSARIO

1.— Firma Electrónica: Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez (artículo 5º, Ley Nº 25.506).

2.— Firma digital: Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes (artículo 2º, Ley Nº 25.506).

3.— Documento Digital o Electrónico: Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte: utilizado para su fijación, almacenamiento archivo. Un documento digital también satisface el requerimiento de escritura (artículo 6º, Ley Nº 25.506).

4.— Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13, Ley Nº 25.506).

5.— Certificador Licenciado: Se entiende por certificador licenciado a 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 (artículo 17, Ley Nº 25.506).

6.— Política de Certificación: Conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios en particular o a un conjunto de aplicaciones con similares requerimientos de seguridad. En inglés Certification Policy (CP).

7.— Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la remisión y administración de los certificados. En inglés Certification Practice Statement (CPS).

8.— Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección; de los recursos del certificador licenciado.

9.— Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.

10.— Plan de Contingencias: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

11.— Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés Certificate Revocation List (CRL).

12.— Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.

13.— Terceras partes confiables: Entidades independientes que otorgan seguridad y confiabilidad al manejo de la información.

14.— Proveedor de servicios de certificación digital: Entidad que provee el servicio de emisión y administración de certificados digitales.

15.— Homologación de dispositivos de creación y verificación de firmas digitales: Proceso de comprobación efectuado para establecer la adecuación de los dispositivos a requerimientos mínimos establecidos.

16.— Certificación de sistemas que utilizan firma digital: Proceso de comprobación efectuado para establecer la adecuación de un sistema o aplicación a requerimientos mínimos establecidos.

17.— Suscriptor o Titular de certificado digital: Persona a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el mismo.

Decreto Nº 724/2006

Modifícase la reglamentación de la Ley Nº 25.506

Bs. As., 8/6/2006

VISTO la Ley Nº 25.506 y el Decreto Nº 2628 del 19 de diciembre de 2002, modificado por el Decreto Nº 1028 del 6 de noviembre de 2003, y

CONSIDERANDO:

Que la Ley Nº 25.506 de Firma Digital reconoce la eficacia jurídica del empleo del documento electrónico, la firma electrónica y la firma digital.

Que el Decreto Nº 2628/02 reglamentario de la Ley antes mencionada, establece las condiciones que deben cumplir a tal fin los certificadores que soliciten una licencia.

Que entre dichas condiciones se encuentra la de contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los requisitos establecidos en el mencionado decreto.

Que a fin de eliminar condiciones que resulten gravosas sobre la actividad de certificación, considerando especialmente que se trata de un área de reciente desarrollo, resulta conveniente derogar el artículo 30 del mencionado Decreto.

Que asimismo, el mencionado Decreto contiene disposiciones de aplicación específica a la Administración Pública Nacional, entre las cuales se encuentra la de aceptar en sus aplicaciones certificados digitales de certificadores públicos y privados.

Que en virtud de las capacidades desarrolladas por la propia Administración Pública Nacional en materia de firma digital y con el fin de evitar que se encarezcan innecesariamente las tramitaciones que efectúe la comunidad ante al Estado, resulta conveniente la utilización de certificados emitidos por certificadores licenciados públicos en forma gratuita.

Que conforme surge de la facultad contenida en el artículo 52 de la ley 25.506 se procede a actualizar los contenidos del anexo I correspondiente a dicha normativa definiendo el alcance del término "Tercero Usuario".

Que el artículo 23 de la Ley Nº 25.506 de Firma Digital establece el desconocimiento de la validez de un certificado digital si es utilizado para alguna finalidad diferente para la cual fue expedido.

Que en virtud de ello, el tercero usuario tiene derecho a aceptar o rechazar documentos electrónicos firmados digitalmente utilizando certificados cuya política de certificación no reúna las condiciones por él requeridas.

Que a fin de adecuar el decreto reglamentario al espíritu de la Ley 25.506, se considera conveniente modificar su artículo 1º inciso b), reconociendo que los certificados digitales emitidos por certificadores no licenciados permiten verificar firmas electrónicas.

Que ha tomado intervención el servicio jurídico permanente de la jurisdicción.

Que la presente medida se dicta en virtud de lo dispuesto por el artículo 99, inciso 2, de la Constitución de la Nación Argentina.

Por ello,

EL PRESIDENTE
DE LA NACION ARGENTINA
DECRETA:

Artículo 1º — Derógase el artículo 30 del Decreto Nº 2628 del 19 de diciembre de 2002.

Art. 2º — Sustitúyese el texto del artículo 38 del Decreto Nº 2628 del 19 de diciembre de 2002 por el siguiente: "Artículo 38.— Las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional podrán ser certificadores licenciados emitir certificados para agentes y funcionarios públicos y particulares, tanto sean personas físicas como jurídicas. Dichos certificados deberán ser provistos en forma gratuita.

En aquellas aplicaciones en las que la Administración Pública Nacional interactúe con la comunidad, solamente se admitirá la recepción de documentos digitales firmados digitalmente utilizando certificados emitidos por certificadores licenciados o certificados extranjeros reconocidos en los términos del artículo 16 de Ley 25.506."

Art. 3º — Incorpórase al Anexo I del Decreto Nº 2628 del 19 de diciembre de 2002, la siguiente definición: "18. TERCERO USUARIO: persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente."

Art. 4º — Incorpórase como artículo 34 bis del Decreto Nº 2628 del 19 de diciembre de 2002, el siguiente texto: "Aceptación por parte de terceros usuarios de documentos electrónicos firmados digitalmente. Los terceros usuarios que sean personas jurídicas 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. Dichas características y requerimientos deben ser manifestados previamente en forma clara y transparente a los titulares de certificados que pretendan operar con ellos."

Art. 5º — Modifícase el texto del artículo 1º inciso b) del Decreto Nº 2628 del 19 de diciembre de 2002 por el siguiente: "Artículo 1º inciso b):

Firma electrónica basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación".

Art. 6º — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — KIRCHNER. — Alberto A. Fernández. — Alberto J. B. Iribarne.

Decisión Administrativa 6/2007

Establécese el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten.

Bs. As., 7/2/2007

VISTO la Ley Nº 25.506, los Decretos Nros. 2628 del 19 de diciembre de 2002, 624 del 21 de agosto de 2003, 1028 del 6 de noviembre de 2003; 409 del 2 de mayo de 2005 y 724 del 8 de junio de 2006.

CONSIDERANDO:

Que la Ley Nº 25.506 legisló sobre la firma digital, la firma electrónica y el documento digital.

Que dicha normativa ha significado un salto cualitativo importante a fin de habilitar la validez legal del documento digital, otorgándole las condiciones de autoría e integridad imprescindibles como base del comercio electrónico, el gobierno electrónico y la sociedad de la información.

Que resulta necesario dictar las normas técnicas que permitan implementar definitivamente el sistema de licenciamiento establecido en la mencionada ley, regulando la Infraestructura de Firma Digital de la República Argentina.

Que el Decreto Nº 2628/02, reglamentario de la Ley Nº 25.506 de Firma Digital creó, a través de su artículo 11, el Ente Administrador de Firma Digital dependiente de la JEFATURA DE GABINETE DE MINISTROS, como órgano técnico administrativo encargado de otorgar las licencias a los certificadores, de supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y la protección de los usuarios de Firma Digital.

Que el Decreto Nº 624/03 aprobó la estructura organizativa de primer nivel operativo de la JEFATURA DE GABINETE DE MINISTROS, estableciendo

la responsabilidad primaria de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION de la SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Que el Decreto Nº 1028/03, modificatorio del Decreto Nº 624/03, a fin de reordenar y racionalizar los recursos en materia de infraestructura de firma digital, disolvió el Ente Administrador de Firma Digital y resolvió que su accionar sea llevado a cabo por la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION, como así también asignarle la responsabilidad de intervenir en la definición de las normas y procedimientos reglamentarios del régimen de firma digital establecido en la Ley Nº 25.506.

Que conforme al Decreto Nº 409/05, uno de los objetivos de la SUBSECRETARIA DE LA GESTION PUBLICA es actuar como autoridad de aplicación del régimen normativo de Firma Digital así como en las funciones de entidad licenciante de certificadores.

Que el Decreto Nº 724/06 modifica el Decreto Nº 2628/02 en sus artículos 1º inciso b), 30 y 38, regulando la aceptación por parte de terceros usuarios de los documentos firmados digitalmente.

Que ha tomado intervención el servicio jurídico competente.

Que la presente medida se encuadra en las facultades atribuidas por el artículo 100 incisos 1 y 2 de la Constitución Nacional y el artículo 6 del Decreto Nº 2628 del 19 de diciembre de 2002.

Por ello,

EL JEFE
DE GABINETE DE MINISTROS
DECIDE:

CAPITULO I

Artículo 1º — Establécese el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten, conforme a los requisitos y procedimientos de la presente Decisión y sus correspondientes Anexos.

Art. 2º — Apruébanse los "Requisitos para el licenciamiento de certificadores" que como Anexo I forma parte de la presente Decisión.

Art. 3º — Apruébanse los "Requisitos Mínimos para Políticas de Certificación" que como Anexo II forma parte de la presente Decisión.

Art. 4º — Apruébase el "Perfil Mínimo de Certificados y Listas de Certificados Revocados" que como Anexo III forma parte de la presente Decisión.

Art. 5º — Apruébanse los "Contenidos Mínimos del Resumen de la Política de Certificación y del Manual de Procedimientos de Certificación para Suscriptores" que como Anexo IV forma parte de la presente Decisión.

Art. 6º — Apruébanse los "Contenidos Mínimos de los Acuerdos con Suscriptores" que como Anexo V forma parte de la presente Decisión.

Art. 7º — Apruébanse los "Contenidos Mínimos de los Términos y Condiciones con Terceros Usuarios" que como Anexo VI forma parte de la presente Decisión.

Art. 8º — Apruébanse los "Montos de aranceles y garantías" que como Anexo VII forma parte de la presente Decisión.

Art. 9º — Apruébanse los "Contenidos Mínimos de la Política de Privacidad" que como Anexo VIII forma parte de la presente Decisión.

CAPITULO II

PRINCIPIOS GENERALES

Art. 10. — Principios. La actividad de los certificadores licenciados se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

Art. 11. — Alcance. El cumplimiento de las normas reglamentarias técnicas establecidas en la presente Decisión sólo será obligatorio para aquellas entidades que decidan obtener el carácter de certificador licenciado.

Art. 12. — Confidencialidad. Toda la documentación exigida durante el proceso de licenciamiento conforme lo determinado en el Anexo I "Requisitos para el licenciamiento de certificadores", será considerada confidencial.

El ente licenciante sólo procederá a su utilización a los fines de evaluar la aptitud del certificador para cumplir con sus funciones y obligaciones inherentes al licenciamiento, absteniéndose de proceder a revelarla, utilizarla para otros fines o bien divulgarla a terceros aún después de haber finalizado el proceso de licenciamiento, salvo respecto de aquella información que la normativa vigente establezca como pública.

CAPITULO III

INFRAESTRUCTURA DE FIRMA DIGITAL
DE LA REPUBLICA ARGENTINA

Art. 13. — Alcance. Se definen como componentes de la Infraestructura de Firma Digital de la República Argentina:

a) al ente licenciante y su Autoridad Certificante Raíz,

b) los certificadores licenciados, incluyendo sus Autoridades Certificantes y sus Autoridades de Registro,

c) los suscriptores de los certificados digitales de esas Autoridades Certificantes y

d) los terceros usuarios de esos certificados.

Art. 14. — De la Autoridad Certificante Raíz. Es la Autoridad Certificante administrada por el ente licenciante que emite certificados digitales a las Autoridades Certificantes de los certificadores licenciados correspondientes a sus Políticas de Certificación aprobadas. Al otorgar la licencia respecto a una Política de Certificación, el ente licenciante procederá a emitirle un certificado digital a través de su Autoridad Certificante Raíz.

Art. 15. — Vínculo entre las Políticas de Certificación licenciadas y las Autoridades Certificantes de los certificadores. El certificador licenciado debe implementar una Autoridad Certificante por cada una de sus Políticas de Certificación licenciadas. La Autoridad Certificante Raíz emitirá un certificado digital para cada una de esas Autoridades Certificantes.

Art. 16. — De las Autoridades Certificantes de certificadores licenciados: Los certificadores licenciados emitirán certificados digitales a los suscriptores de sus Políticas de Certificación, a través de las Autoridades Certificantes que forman parte de su infraestructura tecnológica. Diferentes Autoridades Certificantes de un certificador licenciado podrán compartir la misma infraestructura tecnológica, previa aprobación por parte del ente licenciante.

Art. 17. — De la infraestructura tecnológica. Se entiende por infraestructura tecnológica del certificador al conjunto de servidores, software y dispositivos criptográficos utilizados para la generación, almacenamiento y publicación de los certificados digitales y para la provisión de información sobre su estado de validez. La infraestructura tecnológica que soporta los servicios del certificador, deberá estar situada en territorio argentino, bajo su control y afectada exclusivamente a las tareas de certificación.

No se admitirá compartir infraestructuras tecnológicas entre distintos certificadores.

Art. 18. — Condiciones de uso de la infraestructura tecnológica. El certificador podrá utilizar la misma infraestructura tecnológica, para emitir certificados digitales de políticas de certificación no licenciadas, mientras use los mismos procedimientos y recursos utilizados para sus políticas de certificación licenciadas siempre y cuando no se afecten las condiciones de seguridad y control que dieron lugar al otorgamiento de la licencia. En todos los casos debe mediar autorización previa del ente licenciante.

Art. 19. — Restricciones a la emisión de certificados digitales por parte de los certificadores licenciados. Un certificador licenciado no podrá emitir certificados a Autoridades Certificantes subordinadas.

CAPITULO IV

DE LOS ESTANDARES TECNOLOGICOS Y OPERATIVOS DE LA INFRAESTRUCTURA DE FIRMA DIGITAL

Art. 20. — Estándares tecnológicos. 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 acuerdo con las pautas definidas en el Anexo III.

Art. 21. — Estándares operativos. Establécense como estándares operativos de la Infraestructura de Firma Digital de la República Argentina, los contenidos en los Anexos I y II.

CAPITULO V

DE LOS CERTIFICADORES LICENCIADOS

Art. 22. — Certificadores licenciados. Aquellas entidades que soliciten el carácter de certificadores licenciados deberán cumplir con los requisitos de licenciamiento establecidos en el Anexo I.

Art. 23. — Consentimiento de los suscriptores de certificados digitales. Para la emisión de certificados, los certificadores licenciados y/o sus autoridades de registro, deberán contar con el consentimiento libre, expreso e informado del suscriptor, el que deberá constar por escrito. Este consentimiento debe incluir la confirmación, por parte del suscriptor, de que la información a incluir en el certificado es correcta.

El certificador licenciado no podrá llevar a cabo publicación alguna de los certificados que hubiere emitido sin previa autorización de su correspondiente titular, sin perjuicio de lo dispuesto en el inciso f) del artículo 19 de la Ley Nº 25.506.

Art. 24. — Publicación de información adicional. Conforme lo establecido en el inciso k) del Artículo 21 de la Ley Nº 25.506, los certificadores licenciados adicionalmente deberán publicar en Internet, en forma permanente e ininterrumpida, los actos administrativos por los cuales les fueron otorgadas y eventualmente revocadas sus licencias, los acuerdos con suscriptores y términos y condiciones con terceros usuarios, para cada una de las políticas de certificación por la cual obtuvo una licencia, y toda otra información relevante relativa a ella.

Art. 25. — Domicilio del certificador licenciado. El certificador licenciado deberá encontrarse domiciliado en el territorio de la República Argentina, considerándose que cumple con este requisito, cuando el establecimiento en el cual desempeña en forma permanente, habitual o continuada su actividad, se encuentre situado en el territorio argentino.

Art. 26. — Comunicación de cambios. Los certificadores licenciados están obligados a notificar al ente licenciante con una antelación no menor a DIEZ (10) días, cualquier modificación que proyecten realizar sobre los aspectos que fueron objeto de revisión para el otorgamiento de su licencia, reservándose el ente licenciante la facultad de aceptar o rechazar dichos cambios.

Art. 27. — Uso del término “licenciado” Queda absolutamente prohibido el uso del término “licenciado” a todos aquellos prestadores del servicio de

certificación u otros servicios relacionados con la firma digital, que no hayan cumplido con el correspondiente proceso de licenciamiento establecido por la presente Decisión.

Art. 28. — Reconocimiento de certificados extranjeros. Sin perjuicio de la validación que a dicho efecto deberá realizar la Autoridad de Aplicación, todo aquel certificador licenciado que quiera garantizar la validez y vigencia de certificados extranjeros en los términos del inciso b) del artículo 16 de la Ley Nº 25.506, deberá presentar al ente licenciante para su aprobación una política de certificación apropiada a los fines de la obtención de la licencia correspondiente, como así también acreditar el cumplimiento de los demás requisitos exigidos.

CAPITULO VI

REGISTRO DE CERTIFICADORES LICENCIADOS

Art. 29. — Registro de certificadores licenciados. El ente licenciante deberá mantener actualizado en forma regular y continua, y accesible por Internet, un registro de certificadores licenciados y de aquellos certificadores cuyas licencias hayan vencido o hayan sido revocadas.

Este registro deberá contener el número de Resolución que concede, renueva o revoca la licencia, el o los certificados digitales del certificador licenciado, la identificación del certificador, su domicilio y números telefónicos, la dirección de su sitio en Internet, las políticas de certificación del certificador licenciado, así como las correspondientes Resoluciones que las aprueban. Toda nueva Política de Certificación presentada por dicho certificador licenciado para su licenciamiento y aprobada por el ente licenciante, será incluida en el registro de certificadores mencionado en el presente artículo, con su correspondiente Resolución.

CAPITULO VII

CERTIFICADOS DE PERSONAS JURIDICAS

Art. 30. — Certificados de personas jurídicas. Podrán solicitar certificados digitales las personas jurídicas a través de sus representantes legales o apoderados con poder suficiente a dichos efectos.

La custodia de los datos de creación de firma asociados a cada certificado digital correspondiente a la persona jurídica solicitante, será responsabilidad de su representante legal o apoderado, debiendo su identificación ser incluida en dicho certificado.

Art. 31. — Certificados de aplicaciones. Las personas jurídicas podrán solicitar certificados digitales para utilizar en sus aplicaciones informáticas. Dicha solicitud deberá ser realizada según lo establecido en el artículo anterior.

La constancia de la identificación de la persona física responsable de la custodia de los datos de creación de firma asociados a cada certificado digital,

deberá ser conservada por el certificador como información de respaldo de la emisión del certificado.

CAPITULO VIII

AUDITORIAS

Art. 32. — Auditorías Ordinarias. El ente licenciante realizará auditorías ordinarias a los certificadores y a sus autoridades de registro a fin de verificar el cumplimiento de los requisitos de licenciamiento. Dichas auditorías se realizarán previamente al otorgamiento de la licencia y posteriormente en forma anual.

Art. 33. — Inspecciones extraordinarias El ente licenciante podrá realizar inspecciones extraordinarias de oficio o en caso de denuncias de terceros basadas en posibles deficiencias o incumplimientos incurridos por el certificador licenciado.

CAPITULO IX

ARANCELES Y GARANTIAS

Art. 34. — Establecimiento de aranceles y garantías. De acuerdo a los artículos 30 inciso f) y 32 de la Ley de Firma Digital el ente licenciante procederá, cuando lo estime necesario, a la actualización de los montos de los respectivos aranceles de licenciamiento y renovación, monto de garantía de caución y multas por incumplimientos. Asimismo, conforme al Anexo VII de la presente medida, procederá a fijar aranceles para los nuevos servicios que pudieran prestarse en el marco de la Infraestructura de Firma Digital de la República Argentina.

Art. 35. — Arancel de licenciamiento. El proceso de evaluación por parte del ente licenciante acerca del cumplimiento de todas las condiciones legales y técnicas que hacen al carácter de certificador licenciado, genera la obligación de pago del arancel de licenciamiento. Dicho arancel no será reembolsable en caso alguno.

Art. 36. — Exención al pago del arancel. Los certificadores licenciados pertenecientes a entidades y jurisdicciones del sector público quedarán exentos de la obligación de pago del arancel de licenciamiento.

Art. 37. — Lugar de pago de aranceles y multas. Los aranceles y las multas que pudieran aplicarse deberán ser abonados en la COORDINACION DE TESORERIA dependiente de la DIRECCION GENERAL TECNICO ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS.

Art. 38. — Garantías. Las entidades privadas que soliciten licencia de certificador deberán constituir un seguro de caución a fin de garantizar el cumplimiento de las obligaciones de la presente.

Las pólizas de seguro de caución deberán reunir las siguientes condiciones básicas:

a) Instituir al ente licenciante como asegurado.

b) Mantener la vigencia del seguro de caución mientras no se extingan las obligaciones cuyo cumplimiento se cubre.

La garantía exigida deberá ser acreditada por el certificador como requisito previo al otorgamiento de la licencia y sus renovaciones.

Art. 39. — Incumplimiento de obligaciones. Dictada la Resolución que establece la responsabilidad del certificador licenciado por el incumplimiento de las obligaciones a su cargo y, previa intimación infructuosa de pago, el ente licenciante, en su calidad de asegurado, procederá a exigir al asegurador el pago pertinente, el que deberá efectuarse dentro del término de QUINCE (15) días de serle requerido, no siendo necesaria ninguna otra interpelación ni acción previa contra sus bienes.

CAPITULO X

NORMAS DE PROCEDIMIENTO

Art. 40. — Plazos. Todos los términos y plazos fijados en la presente normativa se regirán según lo establecido en la Ley Nº 19.549 y sus modificatorias.

Art. 41. — Inicio del trámite. Se dará inicio al procedimiento de licenciamiento cuando el interesado presente la solicitud de licencia conjuntamente con toda la documentación detallada en el Anexo I.

Art. 42. — Admisibilidad de la solicitud. Recibida la solicitud de licencia, se procederá a su estudio de forma o admisibilidad mediante la verificación de los antecedentes requeridos.

El interesado deberá subsanar las omisiones o bien ampliar o efectuar aclaraciones sobre la documentación presentada dentro de los DIEZ (10) días de haber sido notificado, caso contrario se procederá a rechazar la solicitud.

Art. 43. — Adecuación de condiciones. Cuando del análisis de la documentación presentada o de las auditorías realizadas surgieran observaciones, se procederá a informar al solicitante a los fines de que proceda a subsanarlas dentro del plazo que el ente licenciante determine a dichos fines y efectos.

Art. 44. — Dictamen de aptitud. Una vez aceptada la documentación en las condiciones requeridas por la presente decisión, se procederá a emitir en el término de SESENTA (60) días el dictamen legal y técnico respecto a la aptitud del certificador para cumplir con las funciones y obligaciones inherentes al licenciamiento. Este plazo no se computará a los fines del artículo precedente.

Art. 45. — Finalización del trámite. Emitido el dictamen legal y técnico que acredite la aptitud del certificador y, habiéndose presentado el seguro de caución en los casos que así correspondiese, el ente licenciante procederá al

dictado de la Resolución que otorgue la correspondiente licencia y ordenará su publicación en el Boletín Oficial.

Art. 46. — Rechazo de la solicitud. En caso que el dictamen legal y técnico fuera desfavorable, el ente licenciante procederá a dictar una Resolución fundada denegando la solicitud la cual deberá ser publicada en el Boletín Oficial.

RENOVACION

Art. 47. — Renovación de licencias. Todo inicio de trámite de renovación está supeditado al pago del correspondiente arancel, el que deberá ser abonado con anterioridad a la presentación de la solicitud.

El trámite de renovación se regirá por las mismas normas establecidas en los artículos precedentes y deberá ser iniciado con SESENTA (60) días de anticipación al vencimiento de la licencia original.

Es responsabilidad del certificador tomar los recaudos necesarios en previsión de demoras en la renovación de la licencia, para evitar que el vencimiento de certificados y políticas afecte a sus suscriptores.

CAPITULO XI

CESE DE ACTIVIDADES

Art. 48. — Cese de actividades. El plan de cese de actividades deberá llevarse a cabo en un todo conforme a lo establecido en el Anexo I.

Art. 49. — Notificación del cese de actividades. Si el cese se produce por decisión unilateral del certificador licenciado, esta circunstancia se deberá comunicar al ente licenciante y a los suscriptores de certificados con una antelación de TREINTA (30) días.

Si el cese se produjera por caducidad de su licencia dispuesta por el ente licenciante o bien por cancelación de su personería jurídica, el ente licenciante procederá, en un plazo no mayor a CUARENTA Y OCHO (48) horas, a publicar dicho cese en el Boletín Oficial.

CAPITULO XII

DEFENSA DEL USUARIO

Art. 50. — Obligación de informar. Los certificadores licenciados deberán informar a todo solicitante, previo a la emisión de los correspondientes certificados, la política de certificación bajo la cual serán emitidos, sus condiciones y límites de utilización, condiciones de la licencia obtenida y todo aquello que fuere relevante con relación a un uso correcto y seguro de dichos certificados, como así también prever procedimientos que aseguren la resolución preventiva de conflictos.

Art. 51. — Reclamos. En caso de reclamos de los usuarios de certificados digitales que se encuentren relacionados con la prestación de los servicios de

un certificador licenciado conforme los términos de la presente normativa, el ente licenciante, previa constancia de haberse formulado el reclamo previo correspondiente ante su propio certificador licenciado con resultado negativo, procederá a recibir la denuncia correspondiente, la que deberá ser evaluada y resuelta mediante la instrucción de las actuaciones correspondientes, sin perjuicio de dejar a salvo los derechos de las partes en conflicto de recurrir a la vía judicial cuando así lo creyeran conveniente.

CAPITULO XIII

SANCIONES

Art. 52. — Gradación de Sanciones. En caso de incumplimiento a las disposiciones de la Ley Nº 25.506, su Decreto Reglamentario y la presente normativa el ente licenciante, previa instrucción sumarial procederá a aplicar las sanciones administrativas que correspondan.

La gradación de las sanciones referidas en el artículo 41 de la Ley Nº 25.506 será realizada por el ente licenciante teniendo en cuenta el tipo de infracción, su repercusión social, el número de usuarios afectados y la gravedad del ilícito.

Art. 53. — Cuantía de multas. El ente licenciante graduará la cuantía de las multas que se impongan, dentro de los límites indicados, teniendo en cuenta lo siguiente:

a) La existencia de dolo o intencionalidad.

b) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por acto administrativo firme.

c) La naturaleza y cuantía de los perjuicios causados.

d) El tiempo durante el que se haya venido cometiendo la infracción.

e) El beneficio que haya reportado al infractor la comisión de la infracción.

Art. 54. — Inscripción de Sanciones. Cuando se imponga una sanción, será inscripta en el Registro de certificadores licenciados.

Art. 55. — Publicación de sanción de caducidad. En los supuestos previstos en el artículo 44 de la Ley Nº 25.506, será obligación del ente licenciante llevar a cabo la publicación en el Boletín Oficial de la Resolución que ordene la caducidad de la licencia previamente otorgada, circunstancia que deberá constar obligatoriamente en la página de inicio del sitio de Internet del certificador.

CAPITULO XIV

DISPOSICIONES GENERALES.

Art. 56. — Facúltase al Señor SUBSECRETARIO DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS a dictar las normas aclaratorias y complementarias de la presente medida.

Art. 57. — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Alberto A. Fernández. — Alberto J. B. Iribarne.

ANEXOS DEL I AL VIII

NOTA: Esta Decisión Administrativa se publica sin Anexos. La documentación no publicada puede ser consultada en la Sede Central de esta Dirección Nacional (Suipacha 767 — Ciudad Autónoma de Buenos Aires) y en http://www.boletinoficial.gov.ar/

ANEXO IV

PRIMERAS JORNADAS DE COORDINACION INFORMATICA DE LOS PODERES JUDICIALES PROVINCIALES DE LA REPUBLICA ARGENTINA

JU.FE.JUS.

ACTA ACUERDO DE LAS TERMAS DE RIO HONDO, SANTIAGO DEL ESTERO.

CONVENIO DE COLABORACION Y RECIPROCIDAD EN MATERIA DE INFORMATICA

En la ciudad de Termas de Río Hondo, a dieciocho días del mes de junio de mil novecientos noventa y nueve, reunidos en Asamblea Ministros de Cortes de los diferentes poderes judiciales provinciales que integran la Junta Federal de Cortes y Superiores Tribunales de las Provincias Argentinas, con la presencia de los siguientes Ministros:

(...)

Luego de un amplio debate e intercambio de opiniones, declaran:

Conscientes de que:

- La realidad actual de nuestro país exige un servicio de justicia de mejor calidad y más eficiente.
- La informática aplicada a la administración de justicia es uno de los elementos para mejorar la calidad del servicio a través de la agilización de los trámites, el seguimiento pautado de los expedientes y el acceso de modo rápido, eficaz y actualizado a la información referente a ellos, así como la relativa a la legislación, jurisprudencia y doctrina.
- Se han venido realizando importantes esfuerzos para incorporar la informática en sus diferentes aspectos a la administración de justicia, y muchos de ellos realizados en forma individual por cada Poder Judicial pueden ser aprovechados por los poderes judiciales de otras provincias.
- La colaboración entre poderes judiciales en materia de informática pude resultar de gran interés en razón de la economía de recursos que puede resultar de estos emprendimientos.

Expresan su voluntad de:

- Brindarse recíprocamente los poderes judiciales provinciales, y asimismo brindar a la Junta Federal de Cortes la más amplia información respecto de los adelantos de informatización.

- En cuanto los compromisos con terceros lo permitan: Posibilitar, a través de convenios, que el trabajo propio realizado en materia de informática sea aprovechado por los demás poderes judiciales, tanto en lo que respecta a información cargada como en lo referente a desarrollo de programas de gestión o de recuperación de la información.

- Facilitar el contacto entre los técnicos de cada poder judicial a través de reuniones periódicas, a fin de poner en común las tareas realizadas y los posibles desarrollos para el futuro.

- Promover políticas informáticas consensuadas entre los diferentes poderes judiciales, teniendo como norte: el mejor aprovechamiento de los sistemas, sin perder de vista cada realidad provincial.

- Encarar proyectos de desarrollo en común.

- Impulsar el desarrollo de páginas Web con información de utilidad para las provincias miembros de la Junta y para la población en general.

- Exhortar a la Junta Federal de Cortes y Superiores Tribunales de Justicia a la creación de un Foro u organismo permanente, que desde su seno, atienda y promueva la presente temática.

MINISTROS DE CORTES FIRMANTES: Ernesto Nicolás Kozameh (Vicepresidente 2º de la JU.FE.JUS. — Santiago del Estero); Berta Kaller de Orchansky (Vocal de la JU.FE.JUS. — Córdoba); Héctor Fernando Arnedo (Jujuy); Aníbal Atilio Astudillo (San Luis); José Antonio Azar (Santiago del Estero); Carlos Böhm (Mendoza); José Alberto Brito (Tucumán); Oscar Eduardo Gatica (San Luis); Daniel César Herrera (La Rioja); Julio Martín Herrera (Entre Ríos); Clara Herrera de Céliz (Santiago del Estero); Carlos Martín Leoni Beltrán (Santiago del Estero); Fernando Macome (Neuquén); Alberto Mario Modi (Chaco); César E. Oviedo (Catamarca); Alfredo Gustavo Puig (Salta).

ASISTENTES INVITADOS: Juan Carlos Caballero Vidal (San Juan); Julio Maier (Ciudad Autónoma de Bs. As.).

REPRESENTANTES DEL MINISTERIO DE JUSTICIA DE LA NACION: José Domingo Coronel y María Angélica Goñi.

AUSENTES ADHERIDOS: Superiores Tribunales de Justicia de las Provincias de Formosa y Misiones.

REPRESENTANTES DEL AREA INFORMATICA: Santiago Aja Espil (Minist. de Just. de la Nación); Mario Accattoli (La Pampa); Guillermo Aranda (Santiago del Estero); Miguel Angel Arregui (Córdoba); José Luis Beltrán Baldiviezo (Formosa); Martín Berrizbeitía (Tucumán); Adriana Bestani (Tucumán); Alicia Briniuk (Chaco); Ramón Broggi (Santiago del Estero); Beatriz Josefina Cantora (Santa Fe); Alberto Rubén Casares (San Luis); Guillermo R. Cosentino

(Chubut); Silvia de la Colina de Martínez (La Rioja); Federico Santiago Díaz Lannes (Santiago del Estero); Marcela Alejandra Fortuny (Salta); Virginia Gómez de Rodríguez (San Juan); José Carlos Libutti (Corrientes); Rosa Paula Liendo (Tucumán); Alejandra Marino de Victorio (San Juan); Juan Carlos Martínez (Mendoza); Nicolás Mendoza (Santiago del Estero); Julio Daniel Moreyra (Chubut); Miguel Angel Muñiz (Santa Cruz); Renato Pablo Musella (Catamarca); Gustavo Nabac (Santiago del Estero); Lidia Palomo de Roldán (Santiago del Estero); Jorge Pinto (Minist. de Just. de la Nación); Alejandro Poclava (Jujuy); Amalia Raimundo (Entre Ríos); Ariel Rodríguez (Santiago del Estero); Jorge Fabián Rodríguez (Misiones); María Laura Sánchez de Sosa (Santiago del Estero); Eduardo Sagüés (Neuquén); Alicia Elizabeth Santana (Santa Cruz); Rita Sapino de Parma (Santa Fe); Julio Oscar Trajtenberg (Santiago del Estero); María Adriana Victoria (Santiago del Estero).

REUNION DE TECNICOS INFORMATICOS DEL PODER JUDICIAL DE LA NACION, DE LOS PODERES JUDICIALES DE LAS PROVINCIAS ARGENTINAS Y DEL MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE LA NACION

"Protocolo Técnico de Comunicación Electrónica Interjurisdiccional"

En la ciudad de Santiago del Estero, capital de la provincia del mismo nombre, a nueve días del mes de marzo del año dos mil uno, reunidos los abajo firmantes en su carácter de funcionarios integrantes de los Poderes Judiciales de la Nación, de las Provincias, del Ministerio de Justicia y Derechos Humanos de la Nación, y de la Procuración General de la Nación, en el seno de la "Primera Reunión del Comité Ejecutivo" del "Protocolo Técnico de Comunicación Electrónica Interjurisdiccional", en el marco del "Programa Integral de Reforma Judicial" perteneciente a la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos de la Nación, declaran:

Conscientes de que:

La búsqueda de una justicia de mejor calidad y más eficiente es la meta que persiguen los Poderes Judiciales tanto nacional como provinciales y el Ministerio de Justicia y Derechos Humanos de la Nación.

La Informática es una herramienta a ser aplicada tanto a la gestión como al registro, carga y consulta de bases de datos jurídicas.

Los esfuerzos mancomunados es la ratio puesta de manifiesto en el accionar de los Poderes Judiciales y el Ministerio de Justicia y Derechos Humanos de la Nación desde hace tiempo.

Los antecedentes del Acta Acuerdo de Las Termas de Río Hondo, de la provincia de Santiago del Estero sobre Convenio de Colaboración y Reciprocidad en materia Informática, emanada de "Las Primeras Jornadas de Coordinación de Informática de los Poderes Judiciales Provinciales de la República Argen-

tina (JU.FE.JUS.)", realizadas en la ciudad de Termas de Río Hondo, provincia de Santiago del Estero, el 18 de junio de 1999, cabal manifestación de dicho accionar,

Y la Reunión celebrada en la ciudad de Buenos Aires el 12 de diciembre del año 2000 y que contó con la participación de funcionarios integrantes de los Poderes Judiciales de la Nación, de las provincias, de la Ciudad Autónoma de Buenos Aires, y del Ministerio de Justicia de la Nación, oportunidad en que suscribieron el "Protocolo Técnico de Cooperación Electrónica Interjurisdiccional" que complementa el proyecto de "Convenio de Comunicación Electrónica Interjurisdiccional".

Expresan su voluntad de:

Reafirmar la voluntad y accionar en cuanto a brindarse recíprocamente amplia colaboración e información en relación a los avances de informatización en sus respectivos ámbitos.

Continuar con la promoción de políticas informáticas consensuadas y el desarrollo de proyectos en común.

Facilitar el contacto entre los técnicos de los ámbitos descriptos, en reuniones periódicas.

Brindar un amplio apoyo al Programa Integral de Reforma Judicial de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos de la Nación.

Cumplir el protocolo anexo suscripto fruto de las conclusiones de la presente reunión y avanzar en el desarrollo del mismo.

FIRMANTES: Ernesto Nicolás Kozameh (Presidente del Excmo. Suprior Tribunal de Justicia de Santiago del Estero — Vocal de la JU.FE.JUS.); Germán Garavano (Coordinador del Proyecto de Reforma Judicial de la Nación — Ministerio de Justicia y Derechos Humanos de la Nación).

VOCALES DEL SUPERIOR TRIBUNAL DE JUSTICIA DE SANTIAGO DEL ESTERO: Clara Luz Herrera de Céliz (Vicepresidente Primera); José Antonio Azar (Vicepresidente Segundo).

COMITE EJECUTIVO: Alejandro Javier Biaggio (Chubut); José Luis Beltrán Baldivieso (Formosa); Javier Fernández Moore (Buenos Aires); Juan Carlos Martínez (Mendoza); Daniel Mario Proumo (Buenos Aires); Julio Trajtenberg (Santiago del Estero).

REPRESENTANTES DEL AREA INFORMATICA INVITADOS: Susana G. Belcastro (Río Negro); Alicia Briniuk (Chaco); García Cáneva (Neuquén); Diego De la Serna (Neuquén); Federico Santiago Díaz Lannes (Santiago del Estero); Alejandra Marino de Vitorio (San Juan); Walter Marta (Buenos Aires); Juan Carlos Martínez (Mendoza); Víctor Martínez (Chaco); Molina Quiroga

(Ciudad Autónoma de Buenos Aires); José Luis Montoto (Misiones); Armando Moretti (Santiago del Estero); Gustavo Nabac (Santiago del Estero); Alejandro Poclava (Jujuy); María Laura Sánchez de Sosa (Santiago del Estero); Alicia Elizabeth Santana (Santa Cruz); Rita Sapino de Parma (Santa Fe); Juan R. Vera van Gelderen (Tucumán); María Adriana Victoria (Santiago del Estero); Marisa Waintal (Ciudad Autónoma de Buenos Aires).

ANEXO V

CONVENIO DE COMUNICACION ELECTRONICA INTERJURISDICCIONAL

En la CIUDAD AUTONOMA DE BUENOS AIRES, a los seis días del mes de septiembre del año dos mil uno, entre la PROCURACION GENERAL DE LA NACION, representada para este acto por el señor Procurador General de la Nación, doctor Nicolás BECERRA, la DEFENSORIA GENERAL DE LA NACION, representada para este acto por el señor Defensor General de la Nación, doctor Miguel Angel ROMERO, el PODER JUDICIAL DE LA PROVINCIA DE BUENOS AIRES, representado para este acto por el señor Presidente de la Suprema Corte de Justicia de dicha provincia, doctor Elías Homero LABORDE, el PODER JUDICIAL DE LA PROVINCIA DE CATAMARCA, representado para este acto por el señor Presidente de la Corte de Justicia de dicha provincia, doctor César Ernesto OVIEDO, el PODER JUDICIAL DE LA PROVINCIA DEL CHACO, representado para este acto por el señor Presidente del Superior Tribunal de Justicia, doctor Ricardo Fernando FRANCO, el Poder Judicial de la Provincia de Chubut, representado para este acto por el señor Ministro del Superior Tribunal de Justicia de dicha provincia, doctor Fernando Salvador Luis ROYER, el PODER JUDICIAL DE LA CIUDAD AUTONOMA DE BUENOS AIRES, representado para este acto por el señor Presidente del CONSEJO DE LA MAGISTRATURA de dicha ciudad, doctor José Octavio GAUNA y el señor Presidente del Superior Tribunal de Justicia de dicha ciudad, doctor Guillermo MUÑOZ, el Poder Judicial de la Provincia de Córdoba, representado para este acto por el señor Ministro del Tribunal Superior de Justicia de dicha provincia, doctor Domingo Juan SESIN, el Poder Judicial de la Provincia de Corrientes, representado para este acto por el señor Ministro del Superior Tribunal de Justicia de dicha provincia, doctor Federico AOSTRI, el Poder Judicial de la Provincia de Entre Ríos, representado para este acto por el señor Presidente del Superior Tribunal de Justicia de dicha provincia, doctor Julio César BERLARI, el Poder Judicial de la Provincia de Formosa, representado para este acto por el señor Ministro del Superior Tribunal de Justicia de dicha provincia, doctor Gerardo GONZALEZ, el Poder Judicial de la Provincia de Jujuy, representado para este acto por el señor Presidente del Superior Tribunal de Justicia de dicha provincia, doctor José Manuel Del Campo, el Poder Judicial de la Provincia de La Rioja, representado para este acto por el señor Ministro del Tribunal Superior de Justicia de dicha provincia, doctor Domingo Carlos Alberto TULIAN, el Poder Judicial de la Provincia deL Neuquén, representado en este acto por el señor Ministro del Tribunal Superior de Justicia de dicha provincia, doctor Arturo González TABOADA, el Poder Judicial de la Provincia de Rio Negro, representado para este acto por el señor Ministro del Superior Tribunal de Justicia de dicha provincia, doctor Alberto Italo BALLADINI, el Poder Judicial de la Provincia de Salta, representado para este acto por la señora Ministro de la Corte de Justicia de dicha provincia, doctora Maria Cristina GARROS MARTINEZ, el Poder Judicial de la Provincia de San Juan, representado para este acto por el señor Ministro de la Corte de Justicia de dicha provincia, doctor

Adolfo CABALLERO, el Poder Judicial JUDICIAL de la Provincia de San Luis, representado para este acto por la señora Ministro del Superior Tribunal de Justicia de dicha provincia, doctora Elvecia del Carmen GATICA, el PODER JUDICIAL DE LA PROVINCIA DE SANTA FE, representado para este acto por el señor Presidente de la Corte Suprema de Justicia de dicha provincia, doctor Rafael Francisco GUTIERREZ, el poder Judicial de la Provincia de Santiago del Estero representado para este acto por el señor Presidente del Superior Tribunal de Justicia de dicha provincia doctor Ernesto Nicolás KOZAMEH, el Poder Judicial de Tierra del Fuego, representado para este acto por el señor Presidente del Superior Tribunal de Justicia de dicha provincia, doctor Carlos Ernesto ANDINO, el Poder Judicial de la Provincia de Tucumán, representado en este acto por el señor Ministro de la Corte Suprema de Justicia de dicha provincia doctor Alberto José BRITO, la SECRETARIA PARA LA MODERNIZACION DEL ESTADO de la JEFATURA DE GABINETE DE MINISTROS, representada para este acto por el señor Secretario, doctor Marcos P. MAKON, el Ministerio de Justicia y Derechos Humanos de la Nación representado para este acto por el señor Ministro, doctor Jorge DE LA RUA y con la presencia del señor Jefe de Gabinete de Ministros, doctor Chrystian G. COLOMBO, conscientes de la necesidad de establecer lazos y realizar esfuerzos comunes para contribuir al desarrollo de un sistema judicial ágil y eficiente, aprovechando los beneficios que ofrece el empleo de las nuevas tecnologías, y promoviendo la participación de todos los Poderes Judiciales y Ministerios Públicos de la Nación Argentina y de otros países en el marco de la cooperación jurídica internacional e interregional, convienen en celebrar el siguiente Convenio:

CAPITULO I

NORMAS GENERALES

COMPROMISO DE COOPERACION

ARTICULO 1º.— Las Partes acuerdan promover el intercambio y cooperación entre sus áreas informáticas y de comunicaciones en los siguientes temas: recursos humanos técnico — informáticos, pliegos técnicos, requisitos, fundamentos de los mismos, resultados obtenidos en su utilización, listado de proveedores técnico — informáticos, observaciones de los mismos, desarrollo de software en las distintas jurisdicciones, capacitación y encuentros técnicos informáticos.

ARTICULO 2º.— Con el objeto de hacer posible un uso racional y adecuado de las nuevas tecnologías de la información, las Partes se comprometen a homogeneizar los nombres de dominio por ellas utilizados, dentro del plazo de SEIS (6) meses contados a partir de la fecha de la firma del presente Convenio, y a realizar las gestiones necesarias a tal fin, por ante el NIC ARGENTINA, conforme las normas establecidas en el Protocolo Técnico de Comunicación Electrónica lnterjurisdiccional.

ARTICULO 3º.— Con idéntica finalidad, las Partes se comprometen, dentro del plazo de UN (1) año de la fecha de la firma del presente, a homogeneizar las

direcciones de correo electrónico de los organismos judiciales, conforme las normas establecidas en el **Protocolo Técnico de Comunicación Electrónica lnterjurisdiccional.**

CAPITULO II

COMUNICACION ELECTRONICA INTERJURISDICCIONAL

ARTICULO 4º.— Las Partes suscriben el presente Convenio con el propósito de complementar lo dispuesto por la Ley nº 22.172, y de incorporar progresivamente el uso de las nuevas tecnologías en las comunicaciones interjurisdiccionales.

ARTICULO 5º.— La comunicación directa entre organismos judiciales y ministerios públicos de distinta jurisdicción territorial podrá realizarse a través del correo electrónico, sin distinción de grado o clase, utilizando las direcciones de los mismos a partir del momento en que el organismo emisor y el organismo receptor se encuentren debidamente dados de alta por los máximos Tribunales y Ministerios Públicos de cada Jurisdicción o el organismo con atribuciones para ello. A este fin, cada una de las partes firmantes deberá mantener una guía actualizada de las direcciones de correo electrónico de los organismos judiciales y ministerios públicos en su sitio en Internet. Otro tipo de comunicaciones entre organismos judiciales y ministerios públicos se incorporará conforme lo señale el Protocolo Técnico de Comunicación Electrónica Interjurisdiccional.

ARTICULO 6º.— Sin perjuicio de los requisitos establecidos por las leyes vigentes y en la medida de lo aplicable, la comunicación electrónica deberá contener: 1) designación completa del organismo judicial o ministerio público emisor; 2) nombre, domicilio y dirección de correo electrónico de otras personas autorizadas a intervenir en el trámite, cuando correspondiere; 3) número de teléfono, domicilio y dirección de correo electrónico del organismo judicial o ministerio público.

El correo electrónico será autenticado conforme las indicaciones y metodología determinadas en el Protocolo Técnico de Comunicación Electrónica lnterjurisdiccional.

ARTICULO 7º.— La comunicación electrónica podrá ser efectuada por correo electrónico, salvo el caso de elementos y/o documentos probatorios que requieran imprescindiblemente la remisión anexa de la información en otro soporte. La impresión e incorporación del correo electrónico con la constancia actuarial al expediente, será prueba suficiente a efectos de tener por acreditada la comunicación.

ARTICULO 8º.— En caso de que el proceso de verificación de la firma electrónica informe alteración del mensaje recibido se procederá según lo determine el Protocolo Técnico de Comunicación Electrónica lnterjurisdiccional.

ARTICULO 9º.— El Protocolo Técnico de Comunicación Electrónica lnterjurisdiccional confeccionado por los representantes designados por las Partes a tal efecto, será actualizado periódicamente para evitar la obsolescencia tecnológica, por una Comisión Técnica compuesta por los responsables informáticos de las partes, sin necesidad de suscribir nuevos convenios a tales efectos. Las actualizaciones al Protocolo Técnico entrarán en vigencia transcurridos TRE (3) meses desde la fecha de su comunicación a las Partes si no fueran formuladas observaciones.

La Comisión Ejecutiva se compone de SEIS (6) miembros titulares y SEIS (6) miembros suplentes, representantes de las diversas regiones judiciales del país, que duran UN (1) año en el ejercicio de sus funciones, y son elegidos por las Partes mediante mayoría simple.

La Comisión Ejecutiva tiene a su cargo el seguimiento y evaluación de los acuerdos y del cumplimiento de las medidas que se adopten, organizando las reuniones pertinentes y manteniendo periódicas comunicaciones con las Partes.

CAPITULO III

DISPOSICIONES TRANSITORIAS

ARTICULO 10.-

a) Durante el plazo de UN (1) año no se transmitirán providencias, resoluciones o sentencias que contengan medidas cautelares o transferencias de sumas dinero, títulos u otros valores. Antes de la finalización de dicho período, las partes suscribirán un Anexo que contendrá las medidas para optimizar el sistema de comunicaciones aquí previsto. La adhesión a dicho Anexo, a formularse en los términos que el artículo 12 establece respecto del Convenio, deberá ser expresa.

b) En una primera etapa, hasta la fecha de la firma del Anexo, el uso de los mecanismos de autenticación tendrá carácter experimental y formativo, asumiendo las Partes el compromiso de realizar una planificación específica para su implantación.

c) Al cabo del primer año, las guías judiciales que se editen deberán contener las direcciones electrónicas de los organismos judiciales y los ministerios públicos.

CAPITULO IV

DISPOSICIONES COMPLEMENTARIAS

ARTICULO 11.— El Convenio comenzará a regir recíprocamente entre las Partes a partir de la fecha de su suscripción.

Durante el transcurso de la etapa estipulada en el artículo 10, y optimizado el sistema en su fase experimental y formativa, el Ministerio de Justicia y Dere-

chos Humanos de la Nación remitirá un proyecto de ley sobre comunicación interjurisdiccional al Congreso de la Nación.

ARTICULO 12.— Este Convenio estará abierto a la adhesión de otros Poderes Judiciales, Ministerios Públicos, registros, órganos extrapoder, y órganos de los poderes ejecutivos nacional, provinciales y de la Ciudad Autónoma de Buenos Aires. Las adhesiones deberán ser comunicadas al Ministerio de Justicia y Derechos Humanos de la Nación para su registro y comunicación al resto de las Partes. El número mínimo requerido de jurisdicciones ratificantes o adherentes a los efectos del presente artículo será de DOS (2).

Se deja constancia de que se expiden DOS (2) ejemplares de un mismo tenor y a un sólo efecto, en la Ciudad Autónoma de Buenos Aires, a los 6 días del mes de Septiembre del año 2001.-

PROTOCOLO TECNICO DE COMUNICACION ELECTRONICA INTERJURISDICCIONAL

ARTICULO 1º.— NOMBRES DE DOMINIO.— La homogeneización de los nombres de dominio se formulará de acuerdo con los criterios que a continuación se ejemplifican: 1) el vocablo "jus" o "justicia" y/o el nombre o abreviatura, en su caso, de la jurisdicción respectiva, seguido de un punto; 2) la expresión "gov" seguida de un punto; 3) la expresión "ar"; como ejemplo: www.juschubut.gov.ar o www.justiciacordoba.gov.ar.

Las Partes se comprometen a incluir vínculos entre sus respectivos sitios de lnternet. Se detallan en Anexo los nombres de dominio que serán utilizados por las Partes.

ARTICULO 2º.— DIRECCIONES DE CORREO.— Cada organismo judicial tendrá una dirección de correo electrónico, la que deberá validarse de acuerdo con el siguiente criterio: 1) hasta CUATRO (4) letras designando el tipo de organismo judicial; 2) hasta CUATRO (4) letras que identifiquen al Fuero, cuando correspondiere; 3) número o letra identificatorio cuando existiere; 4) optativamente, un guión medio; 5) hasta TRES (3) letras o números designando el Distrito, Departamento o Circunscripción judicial, cuando existiere; 6) el símbolo "arroba" (@); 7) el dominio, según lo definido en el Anexo al presente Protocolo. Por ej.: juzciv-cor@justiciacordoba.gov.ar, juzciv6nqn@jusneuquen.gov.ar, juzciv1-bch@jusrionegro.gov.ar (este último ejemplo corresponde al Juzgado Letrado de Primera Instancia número 1 en lo Civil, Comercial y de Minería de la III° Circunscripción Judicial, con asiento en SAN CARLOS DE BARILOCHE).

ARTICULO 3º.— Los correos electrónicos serán confeccionados en formatos estándares sin archivos adjuntos.

Cada una de las Partes instrumentará mecanismos de resguardo para conservar copias de los mensajes emitidos.

El organismo judicial receptor deberá emitir aviso de la recepción del mensaje en forma inmediata.-

En caso de que el mensaje presentare alteraciones, el organismo judicial receptor solicitará su reenvío.

ARTICULO 4º.— Las direcciones de correo de los organismos judiciales serán públicas, y se insertarán en las Guías judiciales y en el Directorio actualizado de su sitio Internet. Cada Parte se compromete a actualizar semestralmente al 1º de febrero y al 1º de agosto de cada año, la correspondiente información.

ARTICULO 5º.— Autenticación. Los correos serán firmados digitalmente por el juez o funcionario competente, para garantizar su autenticidad, integridad e inalterabilidad. Hasta tanto las Partes organicen su propia Autoridad de certificación, se comprometen a gestionar y obtener certificados o identificadores digitales emitidos por alguna de las partes o la Subsecretaría de la Gestión Pública de la Nación (Autoridad Certificante), constituyéndose como autoridades de registro.

ANEXO: LISTADO DE NOMBRES DE DOMINIO

www.dgn.gov.ar (Defensoría General de la Nación)

www.jusbuenos aires.gov.ar (Provincia de Buenos Aires)

www.juschubut.gov.ar (Provincia de Chubut)

www.juscorrientes.gov.ar (Provincia de Corrientes)

www.jusentrerios.gov.ar (Provincia de Entre Ríos)

www.jusformosa.gov.ar (Provincia de Formosa)

www.juslarioja.gov.ar (Provincia de La Rioja)

www.jusneuquen.gov.ar (Provincia del Neuquén)

www.jusrionegro.gov.ar (Provincia de Río Negro)

www.jussantiago.gov.ar (Provincia de Santiago del Estero)

www.justiciacatamarca.gov.ar (Provincia de Catamarca)

www.justiciachaco.gov.ar (Provincia del Chaco)

www.justiciacordoba.gov.ar (Provincia de Córdoba)

www.justiciajujuy.gov.ar (Provincia de Jujuy)

www.justiciasalta.gov.ar (Provincia de Salta)

www.jussanjuan.gov.ar (Provincia de San Juan)

www.justiciasanluis.gov.ar (Provincia de San Luis)

www.justiciasantafe.gov.ar (Provincia de Santa Fe)

www.justierradelfuego.gov.ar (Provincia de Tierra del Fuego)

www.justucuman.gov.ar (Provincia de Tucumán)

www.mpf.gov.ar (Ministerio Público Fiscal de la Nación)

ANEXO VI

Ley 22.172

Apruébase un convenio suscripto entre el señor Gobernador de la Provincia de Santa Fe y el señor Ministro de justicia de la Nación sobre comunicaciones entre tribunales de distinta jurisdicción territorial.

Buenos Aires, 22 de febrero de 1980.

Excelentísimo Señor Presidente:

TENEMOS el honor de dirigirnos al Excelentísimo señor Presidente, a fin de someter a su consideración el adjunto proyecto de ley, por el cual se aprueba el convenio entre el señor Gobernador de la Provincia de Santa fe y el señor Ministro de Justicia de la Nación, sobre comunicaciones entre tribunales de distinta jurisdicción territorial.

Tanto en la II Reunión del Poder Judicial de la Nación, sobre comunicaciones entre tribunales de distinta jurisdiccional territorial.

Tanto en la II Reunión del Poder Judicial de la Nación y de las Provincias, como en los congresos de especialistas en la materia, ha sido principal preocupación el logro de una ley que compatibilice los diferentes puntos de vista sostenidos al respecto y que supere algunas imperfecciones técnicas de los convenios aprobados por las Leyes Nº 17.009 y 21642, a fin de lograr la adhesión de todas las provincias a un régimen uniforme de comunicaciones entre tribunales que agilice al máximo las diligencias a practicarse en extraña jurisdicción.

En ese orden de ideas el Ministerio de Justicia ha elaborado un nuevo convenio, manteniendo la estructura vigente, aunque reubicando ciertos artículos por razones de técnica legislativa.

De la lectura del cuadro comparativo que se acompaña, pueden advertirse las innovaciones introducidas en el convenio de ratificación se solicita, pudiendo destacarse entre las más significativas:

a) El convenio comprende a todos los tribunales, cualquiera sea su competencia en razón de la materia;

b) La regulación del trámite aplicable en los supuestos de ordenarse el secuestro de bienes que han sido objeto de idéntica medida por disposición de otro tribunal;

c) El procedimiento a seguirse para la traba de medidas cautelares;

d) La instauración de un sistema que permita dar certeza a la autenticidad de los documentos que deban inscribirse en los registros u oficinas públicas,

e) La inscripción mediante oficio de toda medida que deba anotarse en los registros públicos, aún cuando previamente deban tributar impuestos locales;

f) La reglamentación más precisa de la citación de testigos;

g) La regulación de los honorarios por parte del juez oficiado y de acuerdo al arancel local, incluso cuando se trate del diligenciamiento de medidas realizadas sin intervención de dicho tribunal (v.gr: inscripciones en registros, mandamientos, notificaciones, etc.)

h) La unificación de los recaudos formales que deben contener los distintos medios de comunicación.

Dios, guarde a Vuestra Excelencia. —Albano E. Harguindeguy — Alberto Rodríguez Varela.

LEY 22.172

Convenio de comunicaciones entre tribunales de distinta jurisdicción

Sancionada y promulgada: 25-2-1980

B O.: 29-02-1980

Artículo 1º.-Apruébase el convenio celebrado con fecha nueve de octubre de mil novecientos setenta y nueve entre el Poder Ejecutivo Nacional, representado por el señor ministro de Justicia, y el Poder Ejecutivo de la provincia de Santa Fe, sobre comunicaciones entre tribunales de distinta jurisdicción territorial, cuyo texto se anexa y forma parte integrante de la presente.

Artículo 2º.-Conforme a lo acordado en el punto tercero del convenio que se aprueba por esta ley, sus normas entrarán en vigencia a los treinta (30) días de publicada la última ley ratificatoria.

Artículo 3º.-La multa prevista en el artículo 11 del convenio será actualizada semestralmente por el Ministerio de Justicia de la Nación de acuerdo con la variación sufrida durante ese período por el índice de precios al por mayor nivel general que publicare el Instituto Nacional de Estadística y Censos. La primera actualización se practicará el 1º de abril de 1980.

Los fondos provenientes de dichas multas, cuando sean aplicadas por los tribunales nacionales ingresarán a la cuenta "infraestructura judicial", creada por la Ley de Tasas Judiciales 21.859.

Artículo 4º.-Si otras provincias adhirieran al convenio a que se refiere esta ley, sus disposiciones se aplicarán, respecto de ellas, a partir de los diez (10) días del depósito de una copia de la ley de adhesión en el Ministerio de Justicia de la Nación, quedando derogadas, con relación a ellas las leyes 17.009, 20.081 y 21.642. El Ministerio de Justicia de la Nación hará saber la adhesión a las demás provincias en las que rija el convenio.

Artículo 5º.-El Poder Ejecutivo Nacional gestionará la adhesión de las demás provincias al convenio que se aprueba por la presente.

Artículo 6º.-Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.

En la ciudad de Santa Fe, a los nueve días del mes de octubre de 1979, entre el Poder Ejecutivo Nacional— representado por el señor ministro de Justicia doctor Alberto Rodríguez Varela-y el Poder Ejecutivo de la provincia de Santa Fe, representado por el señor gobernador vicealmirante (R.E.) Jorge Anibal Desimoni, convienen:

PRIMERO: Aprobar en todas sus partes el convenio que a continuación se transcribe:

CONVENIO

Comunicación entre tribunales de la República

Artículo 1.-La comunicación entre tribunales de distinta jurisdicción territorial, se realizará directamente por oficio, sin distinción de grado o clase, siempre que ejerzan la misma competencia en razón de la materia.

No regirá esta última limitación cuando tenga por objeto requerir medidas vinculadas con otro juicio o con una oficina de la dependencia del tribunal al cual se dirige el oficio.

Si en el lugar donde debe cumplirse la diligencia tuvieren su asiento tribunales de distintas competencias en razón de la cantidad, tramitará el oficio en el tribunal competente según las leyes locales.

Ley aplicable

2.-La ley del lugar del tribunal a que se remite el oficio rige su tramitación, salvo que en este se determine expresamente la forma de practicar la diligencia, con transcripción de la disposición legal en que se funda.

En caso de colisión de normas, el tribunal al que se dirige el oficio resolverá la legislación a aplicar y lo diligenciará.

Recaudos

3.-El oficio no requiere legalización y debe contener:

1. Designación y número del tribunal y secretaría y nombre del juez y del secretario.

2. Nombre de las partes, objeto o naturaleza del juicio y el valor pecuniario, si existiera.

3. Mención sobre la competencia del tribunal oficiante.

4. Transcripción de las resoluciones que deban notificarse o cumplirse y su objeto claramente expresado si no resultare de la resolución transcripta.

5. Nombre de las personas autorizadas para intervenir en el trámite.

6. El sello del tribunal y la firma del juez y del secretario en cada una de sus hojas.

Facultades del tribunal al que se dirige el oficio

4.-El tribunal al que se dirige el oficio examinará sus formas y sin juzgar sobre la procedencia de las medidas solicitadas, se limitará a darle cumplimiento dictando las resoluciones necesarias para su total ejecución, pudiendo remitirlo a la autoridad correspondiente.

El tribunal que interviene en el diligenciamiento del oficio no dará curso a aquellas medidas que de un modo manifiesto violen el orden publico local.

No podrá discutirse ante el tribunal al que se dirige el oficio, la procedencia de las medidas solicitadas, ni plantearse cuestión de ninguna naturaleza. Las de competencia solo podrá deducirse ante el tribunal oficiante.

Cuando el tribunal oficiante ordenase el secuestro de un bien que ya se encontrare secuestrado o depositado judicialmente por orden de otro magistrado, el tribunal oficiado hará saber esa circunstancia al oficiante y adoptará las medidas de seguridad necesarias para que el secuestro ordenado se haga efectivo inmediatamente en caso de cesar el secuestro o depósito judicial existente.

Si el tribunal oficiante insistiere en que el bien debe ser puesto a su disposición, se hará conocer esta decisión al magistrado que ordenó la medida vigente, y si éste formulase oposición se enviarán sin otra sustanciación las actuaciones al tribunal competente para dirimir la contienda, con comunicación a ambos magistrados.

Tramitación

5.-No será necesario decreto del tribunal para impulsar la tramitación ni para librar oficios, agregar documentos o escritos y conferir vistas; bastará al efecto nota del secretario. Los secretarios dispondrán todas las medidas de ordenamiento para facilitar el examen, ubicación y custodia de las actuaciones.

Notificaciones, citaciones, intimaciones, etcétera

6.-No será necesaria la comunicación por oficio al tribunal local, para practicar notificaciones, citaciones e intimaciones o para efectuar pedidos de informes en otra jurisdicción territorial. Las cédulas, oficios y mandamientos que al efecto se libren, se regirán en cuanto a sus formas por la ley del tribunal de la causa y se diligenciarán de acuerdo a lo que dispongan las normas vigentes en el lugar donde deban practicarse.

Llevarán en cada una de sus hojas y documentos que se acompañen el sello del tribunal de la causa y se hará constar el nombre de las personas autorizadas para intervenir en el trámite. Estas recabarán directamente su diligenciamiento al funcionario que corresponda, y éste, cumplida la diligencia, devolverá las actuaciones al tribunal de la causa por intermedio de aquellos.

Cuando la medida tenga por objeto la transferencia de sumas de dinero, títulos y otros valores, una vez cumplida y previa comunicación al tribunal de la causa, se archivará en la jurisdicción en que se practicó la diligencia.

Igual procedimiento se utilizará cuando se trate de hacer efectivas medidas cautelares que no deban inscribirse en registros o reparticiones públicas y siempre que para su efectivización no se requiera el auxilio de la fuerza pública.

Inscripción en los registros

7.-Tampoco será necesaria la comunicación por oficio al tribunal local, cuando se trate de cumplir resoluciones o sentencias que deban inscribirse en los registros o reparticiones públicas de otra jurisdicción territorial.

Se presentará ante dichos organismos testimonio de la sentencia y resolución, con los recaudos previstos en el artículo 3º y con la constancia que la resolución o sentencia esta ejecutoriada salvo que se trate de medidas cautelares.

En dicho testimonio constará la orden del tribunal de proceder a la inscripción y solo será recibido por el registro o repartición si estuviere autenticado mediante el sello especial que a ese efecto colocarán una o más oficinas habilitadas por la Corte Suprema, Superior Tribunal de Justicia o máximo tribunal judicial de la jurisdicción del tribunal de la causa. El sello especial a que se refiere este artículo será confeccionado por el Ministerio de Justicia de la Nación, quien lo entregará a las provincias que suscriban o se adhieran al convenio.

La parte interesada dará cuenta del resultado de la diligencia, con la constancia que expida el registro o repartición que tome razón de la medida, quien archivará el testimonio de inscripción.

En las inscripciones vinculadas a la transmisión hereditaria o a cualquier acto sujeto al pago de gravámenes los testimonios se presentarán previamente a la autoridad recaudadora para su liquidación, si así correspondiere.

Personas autorizadas

8.-Los oficios, cédulas, mandamientos y testimonios serán presentados para su tramitación por abogados o procuradores matriculados en la jurisdicción donde deba practicarse la medida. Cuando las personas autorizadas para intervenir en el trámite no revistiesen ese carácter deberán sustituir la autorización a favor de profesionales matriculados.

Salvo limitación expresa asumen todas las obligaciones y ejercen todos los derechos del mandatario judicial, inclusive el de sustituir la autorización. Están facultados para hacer peticiones tendientes al debido cumplimiento de la medida siempre que no alteren su objeto.

Expedientes, protocolos o documentos originales

9.-No se remitirán a otra jurisdicción piezas originales, protocolos o expedientes, excepto cuando resultaren indispensables y así lo hubiese dispuesto el tribunal oficiante mediante auto fundado.

En los demás casos se enviarán testimonios o fotocopias certificadas de los documentos solicitados.

Comparecencia de testigos

10.-Los testigos que tengan su domicilio en otra jurisdicción pero dentro de los setenta kilómetros del tribunal de la causa, están obligados a comparecer a prestar declaración ante éste.

Cuando el traslado resulte dificultoso o imposible, se dispondrá de oficio, a pedido del testigo o de parte que presten declaración ante el juez, juez de paz o alcalde de su domicilio. También lo harán ante estos últimos los testigos domiciliados a una distancia mayor a la mencionada precedentemente.

Responsabilidad

11.-Sin perjuicio de la responsabilidad disciplinaria, civil y criminal derivada del mal ejercicio de las funciones que se asignen por este convenio a los profesionales o personas autorizadas, toda transgresión será reprimida con multa de catorce mil novecientos trece australes a setecientos cuarenta y cinco mil seiscientos sesenta y cuatro australes.

La causa se sustanciará sumariamente en incidente por separado y en la forma que determine la ley del tribunal ante el cual se compruebe la infracción.

Toda resolución definitiva referente a la actuación de los profesionales será inmediatamente comunicada al tribunal o entidad que tenga a su cargo el gobierno de la matrícula y a los colegios o asociaciones profesionales de las jurisdicciones intervinientes.

El monto de las multas establecidas por este artículo será actualizado semestralmente por el Ministerio de Justicia de la Nación de acuerdo a la variación sufrida durante ese periodo por el Indice de precios al por mayor, nivel general que publicare el Instituto Nacional de Estadística y Censos. La primera actualización se practicará el 1º de abril de 1980.

Los fondos provenientes de las multas serán destinados para infraestructura del Poder Judicial en la forma que lo determinen los respectivos poderes ejecutivos en cada jurisdicción.

Regulación de honorarios

12.-La regulación de honorarios corresponderá al tribunal oficiado, quien la practicará de acuerdo a la ley arancelaria vigente en su jurisdicción, teniendo en cuenta el monto del juicio si constare, la importancia de la medida a realizar y demás circunstancias del caso.

Los honorarios correspondientes a la tramitación de medidas ordenadas por tribunales de otra jurisdicción, sin intervención del tribunal local, también serán regulados por este de acuerdo a lo dispuesto en el párrafo anterior. A ese efecto, presentarán al tribunal fotocopia de las actuaciones tramitadas y una constancia del organismo, funcionario o entidad encargada de su diligenciamiento o toma de razón, en la que se dará cuenta del resultado de la diligencia.

13.-En materia penal, los oficios, cédulas, mandamientos y testimonios, serán directamente diligenciados por la autoridad local encargada de su cumplimiento, cuando no se hubiere autorizado a persona determinada para ello.

14.-Quedan derogadas todas las leyes y disposiciones locales que se opongan al presente convenio.

SEGUNDO: Tramitar la ratificación legislativa de este convenio en ambas jurisdicciones, dentro del término de sesenta (60) días a partir de la fecha.

TERCERO: Establecer que las leyes de este convenio entrarán en vigencia a partir de los treinta (30) días de publicada la última ley ratificatoria.

CUARTO: Acordar que podrán adherirse al presente convenio todas las provincias, mediante la sanción de la ley ratificatoria correspondiente. Hasta tanto se adhieran, mantendrán su vigencia con relación a ellas, los convenios sobre comunicaciones entre magistrados de distintas jurisdicciones celebrados con anterioridad. Las leyes ratificatorias serán comunicadas al Ministerio de Justicia de la Nación para su registro.

Los comparecientes firman el presente convenio de conformidad en dos ejemplares del mismo tenor.

Provincias adheridas a la ley 22.172

Buenos Aires mediante ley 9613 Catamarca mediante ley 3580 Chaco mediante ley 2493 Chubut mediante ley 1793 Córdoba mediante ley 6425 Corrientes mediante ley 3556 Entre Ríos mediante ley 6587 Formosa mediante ley 914 Jujuy mediante ley 3718 La Pampa mediante ley 1012 La Rioja mediante ley 3955 Mendoza mediante ley 4455 Misiones mediante ley 1243 Neuquén mediante ley 1229 Río Negro mediante ley 1457 Salta mediante ley 5624 San Juan mediante ley 4732 San Luis mediante ley 4093 Santa Cruz mediante ley 1334 Santa Fe mediante ley 8586 Santiago del Estero mediante ley 4889 Tucumán mediante ley 5191 Tierra del Fuego, Antártida e Islas del Atlántico Sur mediante ley 147

ANEXO VII

DOCUMENTO ESCRITO Y DOCUMENTO ELECTRONICO

Cuadro comparativo

Documento escrito	Documento electronico
No puede concebirse sin el soporte material (papel)	Soporte: sistema de conformacion electronica expresado en un lenguaje binario
Resulta dificil (no imposible) modificar el registro sin dejar huellas	El registro informatico puede ser modificado
Firma: ologrefa	Firma: electronica y digital
Se distingue la copia del original	Desaparece la diferencia entre la copia y el original

ANEXO VIII

FIRMA OLOGRAFA, ELECTRONICA Y DIGITAL

Cuadro Comparativo

Firma ologrefa	Firma electronica	Firma digital
No hay transformacion	No hay transformacion	Es la transformacion de la firma en un lenguaje encriptado
No se usan claves	Clave de acceso o password	Se utiliza una clave publica y una clave privada
Asegura la autoria	Se utiliza para identificar al signatario (emisor)	Asegura la autoria
Es la estampacion de la firma en un soporte fisico de puño y letra	Puede ser la representacion electronica de una firma ologrefa	No es una represenatcion electronica de una firma ologrefa
Asegura la integridad del texto	No asegura la integridad	Asegura la integridad del lenguaje encriptado
Realizada por medio de un elemento escritor	Puede ser estampada por medio de elementos de digitalizacion	Es una especificidad dentro de la firma electronica
No es un reconocimiento por medios barometricos	Se incluye el reconocimiento por medios barometricos	No es un reconocimiento por medios barometricos
No se vincula con otra tecnologia especifica	Se vincula con otras tecnologias como la mecanica, magnetica, optica, etc	No se vincula con otra tecnologia especifica
Existe una presuncion de validez iuris tantum (salvo prueba en contrario)	En caso de ser desconocida, corresponde a quien la invoca acreditar su validez	Existe una presuncion de validez iuris tantum (salvo prueba en contrario)

ANEXO IX

IX. CRIPTOGRAFIA Y CRIPTOANALISIS

I.1. Introducción

La firma digital se basa en la utilización combinada de dos técnicas distintas, que son la criptografía asimétrica o de clave pública para cifrar mensajes y el uso de las llamadas funciones hash o funciones resumen.

Según el Diccionario de la Real Academia, la palabra criptografía proviene del griego cripto,_que significa oculto, y grafía, que significa escritura, y se define como: "arte de escribir con clave secreta o de un modo enigmático."

La criptografía consiste en una forma de escribir en la que el mensaje que se quiere decir está codificado o encriptado para que no lo puedan leer todas las personas. Es un conjunto de técnicas que mediante la utilización de algoritmos y métodos matemáticos sirven para cifrar y descifrar mensajes.

Tradicionalmente se ha hablado de dos tipos de sistemas criptográficos: los simétricos o de clave privada y los asimétricos o de clave pública:

Sistemas criptográficos simétricos: son aquellos en los que dos personas, que van a intercambiarse mensajes entre sí, utilizan ambos la misma clave para cifrar y descifrar el mensaje. Así, el emisor del mensaje, lo cifra utilizando una determinada clave, y una vez cifrado, lo envía al receptor. Recibido el mensaje, el receptor lo descifra utilizando la misma clave que usó el emisor para cifrarlo. Los sistemas criptográficos simétricos más utilizados son los conocidos con los nombres de DES, TDES y AES.

Los principales inconvenientes del sistema simétrico son los siguientes:

a) La necesidad de que emisor y receptor se intercambien previamente por un medio seguro la clave que ambos van a utilizar para cifrar y descifrar los mensajes.

b) La necesidad de que exista una clave para cada par de personas que vayan a intercambiarse mensajes cifrados entre sí.

Las dos dificultades apuntadas determinan que los sistemas de cifrado simétricos no sean aptos para ser utilizados en redes abiertas como Internet, en las que confluye una pluralidad indeterminada de personas que se desconocen entre sí y que en la mayoría de los casos no podrán intercambiarse previamente claves de cifrado por ningún medio seguro.

Sistemas criptográficos asimétricos o de clave pública: se basan en el cifrado de mensajes mediante la utilización de un par de claves diferentes, privada y pública, de ahí el nombre de asimétricos, que se atribuyen a una persona determinada y que tienen las siguientes características:

Una de las claves, la privada, permanece secreta y es conocida únicamente por la persona a quien se ha atribuido el par de claves y que la va a utilizar para cifrar mensajes.

La segunda clave, la pública, es o puede ser conocida por cualquiera.

Ambas claves, privada y pública, sirven tanto para cifrar como para descifrar mensajes.

A partir de la clave pública, que es conocida o puede ser conocida por cualquiera, no se puede deducir ni obtener matemáticamente la clave privada, ya que si partiendo de la clave pública, se pudiese obtener la clave privada, el sistema carecería de seguridad dado que cualquier podría utilizar la clave privada atribuida a otra persona pero obtenida ilícitamente por un tercero partiendo de la clave pública.

El criptoanálisis consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la clave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación.

En general el criptoanálisis se suele llevar a cabo estudiando grandes cantidades de pares mensaje-criptograma generados con la misma clave.

El mecanismo que se emplee para obtenerlos es indiferente, y puede ser resultado de escuchar un canal de comunicaciones, o de la posibilidad de que el objeto de nuestro ataque responda con un criptograma cuando se envía un mensaje.

Obviamente, cuanto mayor sea la cantidad de pares, más probabilidades de éxito tendría el criptoanálisis.

Uno de los tipos de análisis es el de texto plano escogido, que parte de que se conocen una serie de pares de textos planos, elegidos, y sus criptogramas correspondientes.

También se puede de criptoanalizar un sistema aplicando el algoritmo de descifrado, con todas y cada una de las claves, a un mensaje codificado que se posea y comprobar cuáles de las salidas que se obtienen tienen sentido como posible texto plano.

Este método y todos los que buscan exhaustivamente por el espacio de claves K, se denominan ataques por la fuerza bruta, y en muchos casos no suelen considerarse como auténticas técnicas de criptoanálisis, reservándose este término para aquellos mecanismos que explotan posibles debilidades intrínsecas en el algoritmo de cifrado.

Sin embargo, existen longitudes de clave para las que resultaría imposible a todas luces un ataque de este tipo.

Un par de métodos de criptoanálisis que han dado interesantes resultados son el análisis diferencial y el análisis lineal.

El primero de ellos, partiendo de pares de mensajes con diferencias mínimas, usualmente de un bit, estudia las variaciones que existen entre los mensajes cifrados correspondientes, tratando de identificar patrones comunes.

El segundo emplea operaciones XOR (30) entre algunos bits del texto plano y algunos bits del texto cifrado, obteniendo finalmente un único bit.

Otro tipo de análisis, esta vez para los algoritmos asimétricos, consistiría en tratar de deducir la clave privada a partir de la pública.

Suelen ser técnicas analíticas que básicamente intentan resolver los problemas de elevado coste computacional en los que se apoyan estos criptosistemas: factorización, logaritmos discretos, etc.

La criptografía no sólo se emplea para proteger información, también se utiliza para permitir su autentificación, es decir, para identificar al autor de un mensaje e impedir que nadie suplante su personalidad.

En estos casos surge un nuevo tipo de criptoanálisis que está encaminado únicamente a permitir que elementos falsos pasen por buenos.

Puede que ni siquiera interese descifrar el mensaje original, sino simplemente poder sustituirlo por otro falso y que supere las pruebas de autentificación.

La gran variedad de sistemas criptográficos produce necesariamente gran variedad de técnicas de criptoanálisis, cada una de ellas adaptada a un algoritmo o familia de ellos.

Con toda seguridad, cuando en el futuro aparezcan nuevos mecanismos de protección de la información, surgirían con ellos nuevos métodos de criptoanálisis.

La seguridad de los criptosistemas se suele medir en términos del número de computadoras y del tiempo necesarios para romperlos, y a veces simplemente en función del dinero necesario para llevar a cabo esta tarea con garantías de éxito.

I.2. La seguridad y la informática

El concepto de seguridad en la información es mucho más amplio que la simple protección de datos a nivel lógico.

Para proporcionar una seguridad real hemos de tener en cuenta múltiples factores, tanto internos como externos.

---

(30) La operación XOR corresponde a la tabla de verdad de la disyunción excluyente.

En primer lugar habría que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podríamos hacer la siguiente subdivisión:

a) Sistemas aislados. Son los que no están conectados a ningún tipo de red. De unos años a esta parte se han convertido en minoría, debido al auge que ha experimentado Internet.

b) Sistemas interconectados. Hoy por hoy casi cualquier ordenador pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes de ordenadores sean cada día más complejas y supongan un peligro potencial que no puede en ningún caso ser ignorado.

En cuanto a las cuestiones de seguridad que hemos de fijar podríamos clasificarlas de la siguiente forma:

a. Seguridad física. Englobaremos dentro de esta categoría a todos los asuntos relacionados con la salvaguarda de los soportes físicos de la información, más que de la información propiamente dicha.

En este nivel estarían, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de backup, etc.

También se suelen tener en cuenta dentro de este punto aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.

b. Seguridad de la información: La preservación de la información frente a observadores no autorizados.

Para ello podemos emplear tanto criptografía simétrica como asimétrica, estando la primera únicamente indicada en sistemas aislados, ya que si la empleáramos en redes, al tener que transmitir la clave por el canal de comunicación, estaríamos asumiendo un riesgo excesivo.

c. Seguridad del canal de comunicación. Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.

d. Problemas de autentificación. Debido a los problemas del canal de comunicación, es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente creemos que viene. Para esto se suele emplear criptografía asimétrica en conjunción con funciones resumen

e. Problemas de suplantación. En las redes tenemos el problema añadido de que cualquier usuario autorizado puede acceder al sistema desde fuera, por lo que hemos de confiar en sistemas fiables para garantizar que los usuarios no están siendo suplantados por intrusos.

Normalmente se emplean mecanismos basados en password para conseguirlo.

I.3. Algoritmos y criptoanálisis (31)

La gran mayoría de los algoritmos de cifrado simétricos se apoyan en los conceptos de confusión y difusión inicialmente propuestos por Shannon que se combinan para dar lugar a los denominados cifrados de producto.

La confusión consiste en tratar de ocultar la relación que existe entre el texto plano, el texto cifrado y la clave.

Un buen mecanismo de confusión haría demasiado complicado extraer relaciones estadísticas entre las tres cosas.

Por su parte la difusión trata de repartir la influencia de cada BIT del mensaje original lo más posible entre el mensaje cifrado.

He de hacer notar que la confusión por sí sola sería suficiente, ya que si establecemos una tabla de sustitución completamente diferente para cada clave con todos los textos planos posibles tendremos un sistema extremadamente seguro.

Sin embargo, dichas tablas ocuparían cantidades astronómicas de memoria, por lo que en la práctica serían inviables.

Lo que en realidad se hace para conseguir algoritmos fuertes sin necesidad de almacenar tablas enormes es intercalar la confusión (sustituciones simples con tablas pequeñas) y la difusión (permutaciones).

Esta combinación se conoce como cifrado de producto.

La mayoría de los algoritmos se basan en diferentes capas de sustituciones y permutaciones, estructura que se denomina Red de Sustitución — Permutación.

En muchos casos el criptosistema no es más que un paso simple de sustitución-permutación repetido n veces, como ocurre con DES. El algoritmo DES es el algoritmo simétrico más extendido mundialmente. Data de mediados de los setenta, cuando fue adoptado como estándar para las comunicaciones seguras por el Gobierno de los Estados Unidos. El problema real de DES no radica en su diseño, sino en que emplea una clave demasiado corta, lo cual hace que con el avance actual de las computadoras los ataques comiencen a ser opciones reales.

El algoritmo IDEA (International Data Encryption Algorithm) es bastante más joven que DES, pues data de 1992. Para muchos constituye el mejor y más seguro algoritmo simétrico disponible en la actualidad. Como en el caso de DES, se usa el mismo algoritmo tanto para cifrar como para descifrar. IDEA

(31) Más información en http://www.pki.gov.ar

es un algoritmo bastante seguro, y hasta ahora se ha mostrado resistente a multitud de ataques, entre ellos el criptoanálisis diferencial. No presenta claves débiles, y su longitud de clave hace imposible en la práctica un ataque por la fuerza bruta. Como ocurre con todos los algoritmos simétricos de cifrado por bloques, (32) IDEA se basa en los conceptos de confusión y difusión, haciendo uso de un sin fin de operaciones elementales. Independientemente del método empleado para codificar, hemos de tener en cuenta lo que ocurre cuando la longitud de la cadena que queremos cifrar no es un múltiplo exacto del tamaño de bloque. Entonces tenemos que añadir información al final para que sí lo sea.

El modo ECB (electronic codebook) es el método más sencillo y obvio de aplicar un algoritmo de cifrado por bloques. Simplemente se subdivide la cadena que se quiere codificar en bloques del tamaño adecuado y se cifran todos ellos empleando la misma clave. A favor de este método podemos decir que permite codificar los bloques independientemente de su orden, lo cual es adecuado para codificar bases de datos o ficheros en los que se requiera un acceso aleatorio. También es resistente a errores, pues si uno de los bloques sufriera una alteración, el resto quedaría intacto. Al contrario, si el mensaje presenta patrones repetitivos, el texto cifrado también los presentaría, y eso es peligroso, sobre todo cuando se codifica información muy redundante (como ficheros de texto), o con patrones comunes al inicio y final (como el correo electrónico). Otro riesgo bastante importante que presenta el modo ECB es el de la sustitución de bloques. El atacante puede cambiar un bloque sin mayores problemas, y alterar los mensajes incluso desconociendo la clave y el algoritmo empleados.

Ni el criptograma diferencial (33) ni el criptoanálisis lineal (34) han conseguido doblegar a DES, pero sí representan mecanismos significativamente más eficientes.

---

(32) En los algoritmos cifrados por bloque usualmente se añade información, rellenando con ceros o algún otro patrón el último bloque que se codifica, cuando la longitud de la cadena que queremos cifrar no es un múltiplo exacto del tamaño del bloque.

(33) Se basa en el estudio de los pares de criptogramas que surgen cuando se codifican dos textos planos con diferencias particulares, analizando la evolución de dichas diferencias a lo largo de las rondas de DES.

Para llevar a cabo un criptoanálisis diferencial se toman dos mensajes cualesquiera, incluso aleatorios, idénticos salvo en un número concreto de bits.

Usando las diferencias entre los textos cifrados, se asignan probabilidades a las diferentes claves de cifrado. Conforme tenemos más y más pares, una de las claves aparece como la más probable. Esa sería la clave buscada.

(34) El criptoanálisis lineal, basa su funcionamiento en tomar algunos bits del texto plano y efectuar una operación XOR entre ellos, tomar algunos del texto cifrado y hacerles lo mismo, y finalmente hacer un XOR de los dos resultados anteriores, obteniendo un único bit.

Efectuando esa operación a una gran cantidad de pares de texto plano y criptograma diferentes podemos ver si se obtienen más ceros o más unos.

Los algoritmos de clave pública, o algoritmos asimétricos, han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet).

El más popular por su sencillez es RSA, (35) que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable.

Otros algoritmos son los de El Gamal y Rabin.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado por bloques.

Como ya se dijo los algoritmos asimétricos poseen dos claves diferentes en lugar de una, Kp y KP, denominadas clave privada y clave pública. Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar. Dependiendo de la aplicación que le demos al algoritmo, la clave pública sería la de cifrado o viceversa.

Por otro lado, el algoritmo MD5 (36) constituye uno de los más populares algoritmos de generación de signaturas, debido a su inclusión en las primeras versiones de PGP.

Los algoritmos simétricos pueden ser empleados para autenticar dispositivos, siempre que éstos permitan hacer operaciones de cifrado-descifrado a la vez que impidan acceder físicamente a la clave que llevan almacenada.

I.4. Los métodos de autentificación

Por autentificación entendemos cualquier método que nos permita comprobar de manera segura alguna característica sobre un objeto.

Existen combinaciones de bits que, bien escogidas, dan lugar a un sesgo significativo en la medida anteriormente definida, es decir, que el número de ceros o unos es apreciablemente superior.

Esta propiedad nos va a permitir poder asignar mayor probabilidad a unas claves sobre otras y de esta forma descubrir la clave que buscamos.

(35) De entre los algoritmos simétricos, RSA aparece como el más sencillo de comprender e implementar. Sus pares de claves son duales, por lo que sirve tanto para codificar como para autenticar. RSA se basa en la dificultad para factorizar grandes números. Las claves pública y privada se calculan a partir de un número que se obtiene como producto de dos números primos grandes.

(36) El algoritmo MD5 procesa los mensajes de entrada en bloques de 512 bits, y produce una salida de 128 bits.

En primer lugar, el mensaje se alarga hasta que su longitud es exactamente 64 bits inferior a un múltiplo de 512 bits.

El alargamiento se lleva a cabo añadiendo un uno seguido de tantos ceros como sea necesario.

En segundo lugar, se añaden 64 bits que representan la longitud del mensaje original, sin contar los bits añadidos en el proceso anterior.

De esta forma tenemos el mensaje como un número entero de bloques de 512 bits, y le hemos añadido información sobre la longitud del mensaje.

Dicha característica puede ser su origen, su no manipulación, su identidad, etc.

Consideraremos tres grandes tipos dentro de los métodos de autentificación:

a) Autentificación de mensaje. Queremos garantizar la procedencia de un mensaje conocido, de forma que podamos asegurarnos de que no es una falsificación. Este mecanismo se conoce habitualmente como firma digital.

b) Autentificación de usuario mediante contraseña. En este caso se trata de garantizar la presencia de un usuario legal en el sistema. El usuario debería poseer una contraseña secreta que le permita identificarse.

c) Autentificación de dispositivo. Se trata de garantizar la presencia de un dispositivo válido. Este dispositivo puede estar solo o tratarse de una llave electrónica que sustituye a la contraseña para identificar a un usuario.

La criptografía asimétrica, como ya se dijo, es la que permite autenticar información, es decir, poder asegurar que un mensaje proviene de un emisor determinado y no de cualquier otro.

La autenticación se lleva a cabo empleando una función resumen y no codificando el mensaje completo.

Dichas funciones resumen son las que van a permitir crear firmas digitales. Un mensaje puede ser autenticado codificando con la llave privada (37) el resultado de aplicarle una función resumen, EKp(r(m)). Esa información adicional, que denominaremos firma o signatura del mensaje m, sólo puede ser generada por el poseedor de la clave privada.

Cualquiera que tenga la llave pública correspondiente estaría en condiciones de decodificar y verificar la firma.

(37) Kp: llave privada. KP: llave pública.

ERNESTO NICOLÁS KOZAMEH

Biografía profesional y académica

Nació en Santiago del Estero, provincia en la que en el año 1995 y luego de aprobarse por unanimidad sus pliegos en la Legislatura santiagueña, se desempeñó como miembro del Superior Tribunal de Justicia de esa provincia. Presidió dicho Tribunal desde el año 1996 hasta su retiro en el año 2003. En su gestión se creó la Escuela de Capacitación de Magistrados José B. Gorostiaga de esa Provincia, y la primera Escuela de Informática para el Poder Judicial, marcando la impronta de su gestión en esos dos pilares de la capacitación y la aplicación de nuevas tecnologías en el Poder Judicial. Asimismo durante ese período instrumentó el Consejo de la Magistratura, a partir de lo cual operó el mismo para la selección de magistrados a los fines de su ingreso al Poder Judicial. Celebró convenio con la Universidad Austral, para el dictado en Santiago del Estero de la Maestría en Derecho y Magistratura Judicial, a fin de posibilitar el cursado de esos estudios superiores a todos los miembros del Poder Judicial de esa provincia. Cursó dicha Maestría, en cuyo seno y a los fines de su graduación presentó su trabajo "Comunicaciones Interjurisdiccionales Electrónicas". Dictó numerosos cursos y conferencias.

Representando a Santiago del Estero, participó de la fundación de la Junta Federal de Cortes y Superiores Tribunales de la República Argentina, de la que luego fuera Vicepresidente segundo, en cuya gestión tuvo a su cargo convocar en su provincia natal a las Primeras y Segundas Jornadas de Coordinación Informática de los Poderes Judiciales de la República Argentina, que dieran base a la constitución del Foro Permanente de Técnicos Informáticos de las justicias de todas las provincias. Tales antecedentes permitieron y viabilizaron la celebración del Convenio de Comunicaciones Interjurisdiccionales Electrónicas de los poderes judiciales de la República Argentina, que lo contó entre sus participantes.

Radicado en Córdoba desde su retiro, continúa la labor de investigación en la aplicación de nuevas tecnologías en el Derecho y la Justicia, siendo consultor de diversos estudios.

SE TERMINO DE IMPRIMIR EN LA 2da. QUINCENA DE JUNIO DE 2010
EN LOS TALLERES GRAFICOS DE “LA LEY” S.A.E. e I. - BERNARDINO RIVADAVIA 130
AVELLANEDA - PROVINCIA DE BUENOS AIRES - REPUBLICA ARGENTINA