Gabriela Stortoni [1]

# El acto administrativo informático

*SUMARIO:* 1. LA REGULACIÓN JURÍDICA DE LAS TÉCNICAS TELEMÁTICAS: ANTECEDENTES DE LA LEY DE FIRMA DIGITAL. 2. LA LEY DE FIRMA DIGITAL. 3. CONCLUSIÓN: APORTES DE LA LEY Y CUESTIONES PENDIENTES.

En 1998 tuve el honor de exponer algunas ideas sobre la problemática de la informática y el Derecho, con especial referencia a los actos administrativos, en las Jornadas organizadas por la Universidad Austral, gracias a mi Profesor y amigo Julio Rodolfo COMADIRA. Hoy nuevamente, gracias a la generosidad del Profesor Comadira y la actual convocatoria efectuada por el Profesor Luciano PAREJO ALFONSO, tengo la distinción de poder transmitirles los avances en la materia, como se verá a continuación.

Pues bien, en seis años, en Argentina se han dado una serie de avances en la materia que es menester destacar, tales como la digitalización de la información pública en sitios tales como mecon.gov.ar,

[1] Es abogada por la UNLP de Argentina. Es Magister Profesional en Derecho Administrativo de la Universidad Austral, Becaria JICA en Urbanismo y Transporte, y Máster en Economía, Derecho y Administración de los Servicios Públicos de las Universidades Carlos III, París X, Universidad de El Salvador y EPOCA. Ha ejercido la docencia en diversas Universidades públicas y privadas del país y es autora de diversos trabajos de la especialidad. Es miembro fundador de la Asociación de Juristas de Derecho Público del Mercosur y del Comité de Redacción de la revista *Actualidad en el Derecho Público*. Actualmente se desempeña como Gerente de Legales de la empresa multinacional América Latina Logística, S.A.

infoleg, gobierno electrónico, etc., en los cuales se vuelca la totalidad de las normas nacionales, provinciales y locales vigentes. En igual sentido, la Intranet para los servicios de justicia permite rápidamente analizar la evolución jurisprudencial. Ahora bien, qué impacto ostenta hoy el sistema en materia de emisión de actos administrativos y contratos públicos.

Como he dicho en otra oportunidad, «la evolución tecnológica de los medios de comunicación, en la era de la globalización, ha tornado corriente y cotidiano el uso de medios informáticos y telemáticos... Tales sistemas informáticos y telemáticos no sólo permiten agilizar las comunicaciones y economizar costos sino que evitan el uso y acumulación innecesaria de papel y técnicamente se consideran más confiables y perdurables sus registros»[2].

Esto es, a la denominada «despapelización» no puede ser ajena la Administración Pública, donde el uso de la informática y la telemática constituye una herramienta que agiliza el proceso de comunicación interorgánica e interadministrativa y de toma de decisiones, por un lado, y por el otro, en tanto permite economizar los procesos y transparentar el ejercicio de la función pública de cara al administrado.

Al escenario mencionado debe sumarse el impacto que producen los fenómenos políticos, económicos y culturales de integración de países y globalización[3], en el cual está inmerso nuestro país, en tanto desde el punto de vista del espacio integrado resulta necesario establecer nuevas técnicas compatibles de comercialización y negociación a distancia, de las cuales no podrá excluirse la Administración Pública.

Por todo lo expuesto, considero que el desafío que presenta la aplicación de la telemática y la informática al Derecho deberá estar acompañado por un marco regulatorio que garantice un sistema confiable, justo y seguro, que prevenga y reprima la comisión de los denominados delitos informáticos[4], y veremos a continuación si el mismo se verifica en nuestro sistema jurídico.

---

[2] Gabriela STORTONI, «Sobre la viabilidad de utilizar técnicas telemáticas para la notificación de actos administrativos», en *Procedimientos Administrativos,* (Jornadas organizadas por la Universidad Austral, Facultad de Derecho). Editorial Ciencias de la Administración, División Estudios Administrativos, Bs. As. (Argentina), 1998, pp. 327-341.

[3] En este sentido debe tenerse en cuenta que integración regional y globalización se potencian con el uso del comercio electrónico. Ello es así en tanto el mercado integrado, por su tamaño, necesita del comercio electrónico para desarrollarse, dado que brinda la posibilidad de acceder a una masa crítica de empresas y clientes (Economías de Red) más allá de las fronteras de una nación. Como expresa HALL, «el comercio electrónico constituye un factor vital para la cohesión y la integración de mercados como el Mercosur. El comercio electrónico le da a regiones periféricas nuevas oportunidades de acceder a importantes mercados». J. A. HALL, *Derecho de Alta Tecnología,* año VIII, n.º 91, marzo 1996.

[4] Se entiende por delito informático cualquier conducta ilegal no ética, o no autorizada, que involucra el procedimiento automático de datos y/o la transmisión de datos. Por otra parte, cabe destacar que: «La cooperación internacional está bastante avanzada en lo referente a

## 1. LA REGULACIÓN JURÍDICA DE LAS TÉCNICAS TELEMÁTICAS: ANTECEDENTES DE LA LEY DE FIRMA DIGITAL

Los primeros atisbos referidos a la utilización de formas distintas al papel para acreditar la existencia de actos administrativos se verifican con el facsímil y el e-mail como modos de notificación de los actos del poder público. El primero de ellos se ha implementado en el ámbito de la Administración Pública argentina, para notificar actos administrativos o para que el administrado curse información y documentos tales como recursos, impugnaciones, etc[5]. El correo electrónico[6], a diferencia del facsímil en tanto modo de comunicación, si el mismo utiliza sistemas de encriptamiento de datos puede resultar más seguro en cuanto a la autenticidad e inalterabilidad del contenido, admitiendo prueba en contrario. Este medio de comunicación tuvo su primera aplicación en el ámbito público de Argentina en el uso del sistema BBS *(Bulletin Board System)* en la ciudad de Trenque Lauquen, de la provincia de Buenos Aires.

Obviamente que el modo mencionado necesitaba de un grado de seguridad adicional que garantizara la autoría del documento electrónico. Y es así como empieza a trabajarse en la regulación de la firma digital. Así las cosas, la primera norma de importancia resulta la Resolución de la Función Pública n.º 45/97, la cual prevé la incorporación de firma digital a los procesos de informatización del sector público.

Posteriormente, el Poder Ejecutivo nacional introduce el sistema de digitalización y encriptado de datos, mediante el Decreto n.º 427/98, el cual se mantuvo vigente hasta la promulgación de la Ley de Firma Digital, la cual veremos a continuación.

---

numerosas áreas, tales como la lucha contra el crimen transnacional organizado en las nuevas redes de comunicación. Enfrentados con nuevas formas de delitos de alta tecnología e informático en las redes globales, los gobiernos han respondido a esto en forma vigorosa. En Europa la Europol se han organizado fuerzas de trabajo especializados (task forces), y se ha reforzado la cooperación operacional transfronteriza en áreas tales como "engaños a tiempo real", búsqueda de criminales on-line y búsqueda y captación de evidencia digital. También se han realizado esfuerzos a fin de armonizar la normativa sobre delitos a través de computadoras y de evitar "digital havens"». J. A. HALL, *Derecho de Alta Tecnología,* año VIII, n.º 91, marzo 1996.

[5] Así, por ejemplo, la Comisión Nacional de Valores dictó la Resolución General n.º 251. 94 CNV, la cual habilitó a la utilización del facsímil como medio para la presentación de escritos por parte de los administrados o como instrumento de notificación, subordinada a una opción voluntaria del interesado, a través de una presentación debidamente suscrita en la que harán constar que declaran conocer y aceptar las formas, modalidades y efectos a que estaría sujeta la utilización de facsímil.

[6] Ver Jorge Mario GALDÓS, «Correo electrónico, privacidad y daños», *Rev. de Derecho de Daños*, vol.2001-III, Rubinzal Culzoni, Bs. As., pp. 157 y ss.

El Decreto mencionado establece entonces el régimen al que se ajustará el empleo de la firma digital en la instrumentación de actos internos que no produzcan efectos jurídicos individuales en forma directa, que tendrán los mismos efectos que la firma ológrafa[7]. Ahora bien, veamos a continuación cómo funciona:

Para poder utilizar el sistema de firma digital es menester que el suscriptor cuente con un certificado de clave pública. Este certificado acredita la correspondencia entre una clave pública, elemento de par de claves que permite verificar una firma digital, y el agente titular de la misma, durante el término otorgado.

El certificado de clave pública deberá ser emitido por una autoridad certificante al suscriptor de clave pública. La autoridad certificante debe haber sido licenciada por el organismo licenciante, esto es, la Secretaría de la Función Pública, quien otorgará licencias a las autoridades certificantes para que éstas otorguen certificados de claves públicas y, asimismo, les otorgará las claves públicas a tales autoridades certificantes para verificar la autenticidad de sus certificados. La autoridad certificante deberá llevar un registro de claves públicas y dar a publicidad los certificados de claves públicas otorgadas. La autoridad licenciante debe verificar el uso de medios técnicamente confiables por parte de las autoridades certificantes, y revocará sus licencias en caso contrario o cuando tenga conocimiento que la clave privada se encuentre comprometida.

Por ende, el suscriptor de clave pública podrá remitir documentos con firma digital, encriptándolos con su clave privada, que sólo él conoce, y el destinatario podrá conocer del contenido del documento mediante el uso de la clave pública. El documento digital firmado –emitido de conformidad a las pautas establecidas en la reglamentación– se considera auténtico, hace plena prueba de su contenido y no es repudiable por su autor.

---

[7] Es menester destacar que se trató de una experiencia «piloto» y de alcances acotados, en tanto:

1. se autoriza por el plazo de dos años, a contar desde el dictado de los manuales de procedimientos y de los estándares determinados por parte de la Secretaría de ia Función Pública, el empleo de la firma digital (artículo 1.º del Decreto n.º 427/98).

2. comprende el sector público nacional, esto es, Administración Pública centralizada y descentralizada, entes autárquicos, las empresas del Estado, sociedades del Estado, sociedades anónimas con participación estatal mayoritaria, los bancos y entidades financieras oficiales y todo otro ente en el que el Estado Nacional o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones (artículo 3.º del Decreto n.º 427/98).

3. se podrá utilizar, solamente, para la instrumentación de actos internos del sector público nacional, que no produzcan efectos jurídicos individuales en forma directa (artículo 1.º del Decreto n.º 427/98).

4. la firma digital tendrá los mismos efectos que la firma ológrafa (artículo 1.º del Decreto n.º 427/98).

En síntesis, el documento encriptado con clave pública es el único que es oponible a terceros, y por ello goza de fuerza probatoria en un tribunal[8].

En tal sentido, el documento con firma digital resulta peritable en tanto:

1.º) El certificado de clave pública garantiza la correspondencia entre un documento digital firmado y el suscriptor de la clave pública correspondiente.

2.º) Si se establecen registros de memoria y encriptado de fechas y hora de creación y encriptado original del documento, toda modificación posterior quedaría registrada.

De tal modo, el sistema permite un grado de suficiencia comparable al uso del soporte papel y la ologrfia.

Posteriormente se dictaron las siguientes normas complementarias, a saber:

i) Resolución de la Secretaría de la Función Pública n.º 194, del 24 de noviembre de 1998, que estableció la Infraestructura de la Firma Digital e introdujo, entre otras cosas, las *smarts cards*[9].

ii) Resolución de la Secretaría de la Función Pública n.º 212/1998, que estableció la Política de Certificación para los actos internos de la Administración Pública signados digitalmente.

iii) Disposición, 1/99 de la Subsecretaría de Técnicas Informáticas que estableció el Reglamento de Operación del ArCert y su política de seguridad, a los fines de garantizar los contenidos en las redes informáticas[10].

---

[8] Se aclara que esto no significa que no pueda ser fraguado, como lo es posible incluso en un documento en soporte papel, sino que brinda un sistema de confianza y certeza de igual jerarquía que los documentos con firma ológrafa. Ampliar de mi autoría, «Sobre la viabilidad de utilizar técnicas telemáticas para la notificación de actos administrativos», en *Procedimientos Administrativos* (Jornadas organizadas por la Universidad Austral, Facultad de Derecho), Editorial Ciencias de la Administración, División Estudios Administrativos, Bs. As. (Argentina), 1998, pp. 327-341. Asimismo, ver Mario ZANETTI, «Documento Digital y Firma Digital en el ámbito de la Administración pública», en *Derecho Informático*, año 2000, Rosario, Juris, pp. 101 y ss.

[9] Sobre la importancia de las *smarts cards,* fíjese que fue con una que Clinton procedió a estampar su firma digital en la promulgación de la Ley de Firma Digital Federal el 30 de junio del año 2000. Para mayor información ver Pablo PALAZZI, «Comentario a la Ley Federal de firma electrónica de los Estados Unidos de Norteamérica», *Rev. de Derecho Comparado*, n.º 5, 2002, Rubinzal Culzoni, Bs. As.

[10] Establece una serie de políticas dirigidas a la protección de datos y servicios ofrecidos en la red, mediante ArCert (sigla que en traducción al castellano significa la coordinación de emergencias en redes teleinformáticas). Los aspectos salientes son: el establecimiento de una red telemática de la Administración nacional; la infraestructura de la firma digital; la digitalización del procedimiento administrativo; el establecimiento de un sistema único de expedientes; la racionalización del desarrollo de los portales.

iv) Decreto n.º 1023/2001, que establece el RÉGIMEN DE CONTRATACIONES DE LA ADMINISTRACIÓN NACIONAL. Contiene un capítulo dedicado a las contrataciones públicas informatizadas. El artículo 21 establece que: «Las contrataciones comprendidas en este régimen podrán realizarse en formato digital firmado digitalmente, utilizando los procedimientos de selección y las modalidades que correspondan. También podrán realizarse en formato digital firmado digitalmente los contratos previstos en el artículo 5.º del presente. Las jurisdicciones y entidades comprendidas en el artículo 2.º estarán obligadas a aceptar el envío de ofertas, la presentación de informes, documentos, comunicaciones, impugnaciones y recursos relativos a los procedimientos de contratación establecidos en este régimen, en formato digital firmado digitalmente, conforme lo establezca la reglamentación. Se considerarán válidas las notificaciones en formato digital firmado digitalmente, en los procedimientos regulados por el presente. Deberá considerarse que los actos realizados en formato digital firmados digitalmente cumplen con los requisitos del artículo 8.º de la Ley n.º 19.549, su modificatoria y normas reglamentarias, en los términos establecidos en las disposiciones referentes al empleo de la firma digital en el Sector Público Nacional, las que se aplicarán, en el caso de las contrataciones incluidas en los artículos 4.º y 5.º de este régimen, aun a aquellos actos que produzcan efectos individuales en forma directa. Los documentos digitales firmados digitalmente tendrán el mismo valor legal que los documentos en soporte papel con firma manuscrita, y serán considerados como medio de prueba de la información contenida en ellos». Por su parte, el artículo 22 establece que la reglamentación establecerá la regulación integral de las contrataciones públicas electrónicas, en particular el régimen de publicidad y difusión, lo referente al proceso electrónico de gestión de las contrataciones, los procedimientos de pago por medios electrónicos, las notificaciones por vía electrónica, la automatización de los procedimientos, la digitalización de la documentación y el expediente digital[11].

## 2. LA LEY DE FIRMA DIGITAL

El 11 de diciembre de 2001, pocos días antes de una de las crisis más dramáticas de la historia argentina, se promulga la Ley n.º 25506, denominada «Ley de Firma Digital», la cual instaura definitivamente el documento electrónico y la firma digital con validez jurídica en el país, continuando el proceso iniciado por el Decreto n.º 427/98 y complementarios citados *ut supra*.

[11] Más adelante retomaremos este punto de cara a establecer las pautas de una contratación posible mediante el uso de medios telemáticos.

La Ley establece por su artículo 2 que: «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». Asimismo, se destaca que la Ley regula cuándo una firma digital puede ser considerada como tal y gozar de las ventajas de la Ley. En este sentido se expresa que una firma digital es válida cuando: a) Ha sido creada durante el período de vigencia del certificado digital válido del firmante. b) Ha sido debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente. c) El certificado haya sido emitido o reconocido por un certificador licenciado. Y cuando se den estos extremos, entonces el documento gozará de las presunciones legales establecidas por la Ley en sus artículos 7 y 8. En efecto, la Ley ha querido dotar de garantías de certeza y seguridad jurídica como modo de promover el uso del sistema, a saber: la presunción de autoría y la presunción de integridad, esto es, que el documento es de quien ostenta el certificado y que, verificado el mismo, se supone que su contenido no ha sido violado o adulterado, por lo cual será obligación de quien alegue que no es legítimo la prueba de sus dichos[12].

Así entonces se instaura –exceptuando los casos que requieran una forma solemne de emisión de la voluntad; las disposiciones de última voluntad; los actos jurídicos relativos al derecho de familia o los actos personalísimos– la firma digital al mismo nivel que la firma ológrafa.

La Ley asimismo distingue entre firma digital y firma electrónica, siendo la primera una especie de la segunda, no obstante destacar que no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada una de ellas, 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 titu-

[12] Estas presunciones implican la responsabilidad en el uso de un certificado por parte del usuario, en tanto la prueba de la no autoría o de no integridad del documento será de carácter imposible y será el titular del certificado el que deberá asumir las consecuencias de un obrar negligente.

lar, 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 Comunidad Europea, o «firma electrónica», utilizado en otros países como Brasil o Chile.

La Ley también define el documento digital en su artículo 6, expresando que :«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». Esta definición no identifica la calidad de instrumento público o privado del documento digital, sino sólo se definió a los fines de asimilarlo a un documento con valor probatorio.

Desde el punto de vista de la ingeniería pensada para el funcionamiento del nuevo sistema debo destacar que en principio se ha burocratizado en demasía el sistema sobre todo teniendo en cuenta las normas reglamentarias de la Ley. En efecto, se crean diversos organismos, a saber: a) La Autoridad de Aplicación, que establece la política aplicable. b) El Ente Licenciante o Administrador de la Firma Digital, que otorga las licencias para funcionar las autoridades certificantes[13]. c) La Autoridad Certificante, que son los organismos que certifican la titularidad de una clave pública y un usuario por un tiempo determinado, otorgando al efecto un certificado habilitante. d) Una Comisión Asesora para la Infraestructura de Firma Digital, con funciones consultivas. e) El Sistema de Auditoría, de carácter privado. Finalmente, la Ley establece la extensión del sistema a los tres poderes del Estado, debiéndose llegar en el plazo de CINCO (5) años, contados a partir de la entrada en vigencia de la Ley, para aplicarse 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 8.º de la Ley n.º 24156.

## 3. CONCLUSIÓN: APORTES DE LA LEY Y CUESTIONES PENDIENTES

En este breve recorrido por la legislación y sus aristas más destacadas, varios son los aportes que la misma ha traído consigo, así como

[13] En forma antágonica, la Ley Federal de Firma Electrónica de Estados Unidos regula una intervención mínima, confiando en el sistema en competencia las autoridades certificantes. De hecho, ser una autoridad certificante seleccionada por gigantes como Microsoft, por ejemplo, da la plena confianza en el sistema. Se destacó así en el debate que «donde la intervención del gobierno resulte necesaria, su objetivo debe ser apoyar y promover un ambiente legal simple y mínimo para el comercio». Ver Pablo PALAZZI, «Comentario a la Ley Federal de firma electrónica de los Estados Unidos de Norteamérica», *Rev. de Derecho Comparado,* n.º 5, 2002, Rubinzal Culzoni, Bs. As.

también varias son las cuestiones que se abren al futuro y merecen especial detenimiento, a saber:

- Es remarcable el valor que se le ha dado al documento firmado digitalmente como al menos instrumento privado[14], y que en las condiciones legales de emisión incluso rechaza su repudio por principio y por imperio de las presunciones de autoría e integridad que la Ley le otorga.
- En segundo lugar, aun cuando se trate de un documento con firma electrónica, estamos en presencia de un documento que se considera válido, salvo prueba en contrario.
- En términos generales, desde la vigencia de la Ley, cuando el ordenamiento jurídico requiera una firma manuscrita, dicha exigencia estará cumplida con la firma digital o la firma electrónica.
- Asimismo, se establece la voluntad de homogeneizar todos los procesos de producción de normas administrativas, leyes y en su caso el poder judicial, y todo ello dentro del plazo máximo de cinco años contados desde la vigencia de la Ley de Firma Digital, venciendo en consecuencia en noviembre de 2006.
- En síntesis, la aplicación del sistema en la Administración Pública es una clara manifestación a favor de la participación del ciudadano en el sistema de cara a alcanzar el denominado «Gobierno Electrónico», y que realza los principios de celeridad, economía, sencillez, informalismo a favor del administrado, etc., que deben orientar la función pública e informar el procedimiento administrativo.

Ahora bien, el sistema deja varios sectores desguarnecidos, y destacaré al menos dos de ellos, a saber:

a) Burocratización extrema: la multiplicación de organismos públicos y privados de control atenta contra la eficacia del mismo y la efectiva responsabilidad de los actores del proceso[15]. En tal sentido considero medular acrecentar la figura de la Autoridad Certificante y que no se restrinja a ningún sector en particular, sino que sea abierta a quien

[14] Es preciso destacar que no vamos a analizar si estamos ante un instrumento privado o público. Éste es un problema adicional que merece su reflexión y estudio por parte de los civilistas. En este sentido se recomienda la lectura del estudio de los Dres. CHAYER, GOLDFELD y VENTURA «Una nueva categoría de instrumento jurídico: el documento firmado digitalmente – Parte III», ED T(200)567 y ss. Para estos autores, por las presunciones de que les ha dotado la Ley, los documentos firmados digitalmente tienen más valor que un instrumento privado, constituyendo una especie intermedia, según los autores citados.

[15] Hoy la legislación establece todas las responsabilidades en la Autoridad Certificante, ya desde el ámbito civil respecto a terceros, administrativa, así como penal, pero nada se ha regulado respecto a los demás organismos que interactúan con el mismo.

–previa inscripción en el Registro de la Autoridad de Aplicación– sea el organismo que emita los certificados. En primer lugar, se destaca que el rol podría ser cubierto por los Colegios Públicos de Abogados o Escribanos[16] o empresas privadas que compitan por garantizar el mejor servicio al usuario.

b) Inexactitudes en torno a la aplicación del sistema telemático a las compras y contrataciones públicas: las normas todavía no distinguen las variables de adaptación del denominado *e-procurement* a la Administración Pública. La posibilidad de aplicación de una contienda *online,* debe realizarse garantizando el principio de transparencia e igualdad licitatoria. Por ello es preciso abocarse a la regulación de estos procesos, que en materia de Hacienda Pública serán los de mayor aplicación del sistema informático, sin duda alguna.

En síntesis, el antes fenómeno de la informática aplicada al Derecho es hoy una realidad concreta y que ha nacido incluso al ordenamiento jurídico con la Ley n.º 25506. Resta entonces continuar en la tarea de profundizar y agudizar los procesos de aplicación de la misma, bregando por alcanzar un sistema austero, que evite monopolios, por un lado, y erogaciones inútiles –ya en creación de organismos como en la duplicidad de controles inoperantes–, por el otro, y que otorgue la confiabilidad del sistema informático, que de hecho aparece superior al sistema de soporte papel. En otras palabras, Argentina, que era pionera en la materia, hoy se encuentra un paso atrás en materia de aplicaciones informáticas; ahora la prisa no debe ser motivo de pérdida de calidad, por lo cual es importante que la política pública se dirija a institucionalizar un sistema que erradique los vicios de antaño de la Administración Pública y que tanto daño le han hecho al crecimiento sostenido de nuestro país. Obviamente, la informática es sólo una herramienta, pero que se convierte en esencial llave hacia la transparencia de la gestión pública cuando se pretende instaurar el Gobierno Electrónico, pero como herramienta en sí no es mágica y precisa de la toma de medidas que permitan el control y la gestión eficiente de cara al ciudadano, que debe ser el beneficiario del sistema y no la víctima de una nueva burocracia.

[16] Se destaca la posición de Mauricio DEVOTO, quien expresa en su artículo «Claves para el éxito de una infraestructura digital», LL, V.2004, p. 1045, la necesidad de encomendar la calidad de autoridad certificante a los notarios en tanto existe una especie de otorgamiento de fe pública delegada por el Estado en las autoridades certificantes de idéntico tenor a la encomendada a los escribanos. Este punto encuentra otra variable en España, donde el Colegio Público de Abogados ha bregado por la creación de un carné digital del letrado. Para conseguir este empeño, expresa el Colegio, el Consejo General de la Abogacía Española tendrá que erigirse como entidad certificadora. Ver www.pki.gov.ar.