# LA CERTIFICACIÓN ELECTRÓNICA VENEZOLANA:
## Desde una perspectiva reflexiva*

Gladys Stella Rodríguez*

**Resumen**

*Una de las consecuencias de una red abierta como Internet son los problemas de seguridad y confidencialidad. Por ello este trabajo consiste en describir el escenario donde se desarrolla con mayor fuerza la denominada «revolución tecnológica», como lo es Internet; exponer algunas consideraciones generales sobre los cambios que se han producido en la Red; determinar el valor de la certificación electrónica en Venezuela y, finalmente, presentar una propuesta de regulación supranacional. Se parte de un estudio exploratorio–descriptivo. Y se concluye que en las relaciones derivadas del uso de la tecnología es la buena fe la que prevalecerá, lo cual obliga a poner en marcha un marco de principios regulatorios flexibles y lo suficientemente generales que permitan, a las instituciones nacientes como la Superintendencia de Servicios de Certificación Electrónica Venezolana, aplicar los nuevos sistemas de seguridad como una estrategia de competitividad.*

**Palabras clave:** Seguridad, Confidencialidad, Internet, Certificado Electrónico.

*Fecha de recepción:* 14 de marzo de 2002

**Abstract**

One of the consequences of an open net as Internet is the problems of security and confidentiality. That is why this paper consists in describing the scenario where the

* Avance del Proyecto de Investigación *«Modelo Alternativo de una Infraestructura de Seguridad y Confidencialidad Informática frente al auge de los delitos en y contra Internet»*. Financiado por el CONDES, bajo el Nº 0095-2001.

** Doctora en Derecho. Magíster en Planificación y Gerencia de Ciencia y Tecnología. Abogada. Profesora e Investigadora de la Sección de Informática Jurídica y Derecho Informático y Derecho Internacional Público. Adscrita al Instituto de Filosofía del Derecho «Dr. J.M. Delgado Ocando». Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia. Inscrita en la Fundación Venezolana del Programa de Promoción del Investigador (PPI) Nivel I. *(gerordrigu@cantv.net)*

denominated "technological revolution" develops whit a greater force, as it is Internet; in exposing some general considerations about the changes that have taken place in the Web; in determining the value of the electronic certification in Venezuela, and finally, in presenting a proposal of a supranational regulation. This paper starts from an exploratory-descriptive study and it concludes that in the relations derived from the use of technology the good faith will prevail, which forces to put in motion a frame of flexible regulatory and sufficiently general principles which allow the rising institutions, as the Venezuelan Electronic Certification Services Superintendence to apply the new security systems as a competitiveness strategy.
**Key words:** Security, Confidentiality, Internet, Electronic certificate

## 1. INTRODUCCIÓN

A diferencia de lo que ocurrió con revoluciones y descubrimientos anteriores, nuestra era, sin embargo, parece ser la época de las revoluciones simultáneas de las denominadas «nuevas tecnologías», especialmente las tecnologías de la información y de la comunicación. Se trata de una época caracterizada por cambios radicales, cambios que ocurren en el marco de profundas contradicciones: de clases, de raza y de género.

Pero se debe tener cuidado, porque al igual que ocurrió con otras tecnologías, la aplicación de las redes teleinformáticas en sus inicios plantearon una visión utópica, en la que todo era considerado extremadamente positivo y se describía un mundo convertido en un nuevo Camelot, Arcadia o Utopía.

De igual forma, también se produjo una visión ludita (en referencia a Lud, que rechazaba toda innovación tecnológica), en la que las tecnologías deberían ser rechazadas, pues de ellas sólo puede esperarse toda suerte de males y consecuencias negativas. Desde luego, ni una ni otra visión responden a la realidad y parece un hecho innegable que hay indicadores que demuestran que, en un mundo tecnificado como el actual, algunos aspectos de la vida tienen mayor calidad que en el pasado.

Y aun cuando son muchas las incógnitas que todavía rodean esta herramienta comunicacional, todos y todas participan, en igualdad de

condiciones, con sólo disponer de un terminal y emplear un lenguaje lógico-técnico.

Por tal razón, este trabajo se dispone describir brevemente el escenario donde se desarrolla esta denominada «revolución tecnológica» con mayor apasionamiento, como lo es la de Internet, exponer algunas consideraciones generales sobre los cambios que se han producido en el marco de la red de redes, para seguidamente determinar el valor de la certificación digital en Venezuela y finalmente presentar la inquietud por una propuesta de regulación supranacional.

## 2. LA INTERNET

El crecimiento acelerado no sólo en el campo de lo físico sino en el ciberespacio ha hecho surgir toda una infraestructura de información, a veces llamada *«la superautopista de la informática»* o *«red de redes»*, o simplemente *«Internet»*.

La Internet es uno de los sistemas principales de transferencia de archivos y mensajes digitales por una red de enlaces de conexiones y computadoras, con un crecimiento exponencial que une a más de treinta y cinco millones de *«ciudadanos internacionales»* (Neff, 1997).

La Internet nace en 1973 como un proyecto de la Agencia de Proyectos de Investigación Avanzados (ARPA) de Estados Unidos, la cual tenía antecedentes en el desarrollo de redes de cómputos desde 1967 cuando creó ARPANET, para atender sus necesidades de comunicación, y cuya misión era garantizar la supremacía tecnológica de Estados Unidos en relación con la Unión Soviética.

Por su parte, Quey y Ryer (1994) consideran que el proyecto del cual surgió la Internet tuvo otra finalidad: desarrollar técnicas y tecnologías para la interconexión de redes de datos de diversos tipos, lo cual produjo un conjunto de protocolos conocidos como *TCP/IP (Transmisión Control Protocolo/Internet Protocolo)*, que han permitido actualmente la interconexión de redes de computadoras de las características más disímiles. (Urdaneta, 1996).

Desde su apertura al público Internet conoce un desarrollo impetuoso; el grado de rendimiento se está duplicando en un promedio de 18 meses, y debería alcanzar en el presente siglo 32 veces más que un computador personal de 1993 (Barón, 1990).

Esto quiere decir que las «nuevas tecnologías de la información y de la comunicación» vienen a configurar, quizás, una excelente oportunidad de desarrollo y competitividad para la misma sociedad.

## 3. ALGUNAS CONSIDERACIONES GENERALES SOBRE LOS CAMBIOS EN LA ERA DE INTERNET

Como consecuencia del acelerado desarrollo de las nuevas tecnologías son varios los cambios que se han experimentado, y uno de los más significativos recae sobre el Comercio, el cual sin duda se ha transformado, y hoy se habla de la existencia de un comercio electrónico o digital que está consolidándose en nuestro país; y del cual se espera que en los próximos años alcance un incalculable período de crecimiento, gracias a la implantación definitiva de los protocolos que garantizarán la seguridad de las transacciones y el incremento progresivo de usuarios de la red (Rivas, 1999).

Es decir, el rápido crecimiento del comercio electrónico en los últimos años ha hecho que Internet haya pasado de ser un medio para buscar y conseguir información a ser considerado una especie de «megamercado» planetario donde se producen todo tipo de intercambios.

De esto se ha originado otro cambio importante: la necesidad de buscar mecanismos de pago «a distancia» que sean lo suficientemente seguros y cómodos para que todo este comercio *on line* pueda consolidarse y prosperar (Font, 2000).

Ahora bien, desde el punto de vista del Derecho, hay dos grandes enfoques para enfrentar este reto:

a) Aceptar y someterse al Derecho tal como está regulado, sin tener en cuenta la discrepancia entre la evolución tecnológica y la regulación jurídica vigente y
b) Formular propuestas a fin de que el Derecho asuma nuevas formas, que no sólo no obstaculicen el uso de las nuevas tecnologías sino que lo regulen adecuadamente, revisando y reformulando las nuevas bases legales.

La solución no puede ser otra que esta última, que a su vez plantea problemas jurídicos-políticos, ya que todo progreso técnico no representa necesariamente una mejora en la calidad de vida ni un mayor respeto por los derechos individuales (Castro, 1995).

Si bien es cierto que el final del siglo XX significó una revolución cuyos efectos fueron significativos, se espera que en el siglo XXI se produzcan cambios aún más radicales. La tecnología informática está en todas partes. La información se ha convertido en el cuarto mayor factor económico, casi superando a las materias primas, trabajo y capital. Con la revolución de la tecnología informática, la información se ha convertido en un factor de producción cada vez más importante, cuya rápida disponibilidad, interconexión y ahorro son muy importantes para aumentar la competitividad de la economía y asegurar una alta calidad de vida (Kalt, 1996).

Y es que el modelo informático está caracterizado por bajos costos con tendencias declinantes. El precio de las computadoras, con relación a su desempeño, se ha venido reduciendo anualmente, en el transcurso de los últimos treinta años, en una proporción de 25%. En términos relativos, tal reducción de costos no tiene precedentes entre los insumos clave de los ciclos reales de negocios anteriores.

Al contrario del petróleo, cuyas reservas son limitadas y no renovables, la informática no enfrenta límites físicos de oferta. Su principal insumo material, el silicio, es muy abundante en la naturaleza. Hay oferta aparentemente ilimitada de esta materia prima a pesar de que se verifica una demanda creciente de estos recursos. En cuanto al insumo inmaterial de la informática, la inteligencia humana, su oferta, al menos aparentemente, es infinita. La Revolución Informática se ha caracterizado por una reducción de los precios de insumos y por la mejora del desempeño de todos los productos del complejo electrónico (Tigre, 1993).

Por lo anterior, las empresas, sobre todo las financieras, han tenido que utilizar la tecnología como punto fundamental y estratégico para captar el mercado y mantenerse vivo en él.

En este sentido, y en consideración al principio jurídico del necesario resguardo de la «*Fe Pública*» y para mantener el «*Orden Público Económico*» y la «*Buena Fe*» involucrados en las transacciones electrónicas, tecnológica y legalmente han surgido las denominadas «*Autoridades Certificadoras*» o, dicho más adecuadamente, los «*Proveedores de Servicios de Certificación*» de firmas digitales.

## 4. CERTIFICACIÓN ELECTRÓNICA: Régimen venezolano

En Venezuela la Ley de Transmisión de Mensajes de Datos y Firma Electrónica de fecha 28 de febrero de 2001, publicada en la *Gaceta Oficial*

N° 37.148, consagra en su capítulo VI, todo lo relativo a los «Proveedores de Servicios de Certificación».

Sin embargo, desde un punto de vista tecnológico, no cualquiera puede o está capacitado para ofrecer el respaldo de firmas digitales y el uso de mecanismos de encriptación. Es una función que no se le puede encomendar a personas naturales o a pequeños proveedores de *hardware* o *software* ajenos a las realidades y a los procedimientos técnicos de quienes intervienen en el comercio electrónico. Creemos que sería un gran error encomendar el trabajo de otorgar certificados digitales y de registrar los antecedentes personales de aquellos a quienes se refieran a entidades o funcionarios auxiliares de la administración de justicia como los notarios, que apenas manejan procesadores de textos o programas de bases de datos o de informática de registro (Jijena, 2001).

*Por tal razón, la ley nacional, antes referida, establece en su artículo 31 los requisitos para ser proveedor, entre los cuales destacan los siguientes:*

1. *La capacidad económica y financiera suficiente... En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.*
2. *La capacidad y elementos técnicos...*
3. *Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro...*
4. *Parafraseando al jurista Couture, la fe pública es una calidad particular de ciertos instrumentos que consiste o depende, no sólo en la autoridad moral y técnica de quien los ha otorgado sino también en una ficción legal de que lo aseverado por una entidad facultada para hacerlo es verdad.*
5. *Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios...*
6. *Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales...*
7. *En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen. Personal técnico adecuado con conocimiento especializado... y experiencia en el servicio...*

8. *Las demás que señale el reglamento de este Decreto-Ley.*

Pero es necesario dar un paso más allá y llegar al origen de la situación. Porque las personas jurídicas que presten servicios de Entidades Certificadoras a su vez también deben ser certificadas, validadas, autorizadas o acreditadas; o dicho de otra forma, porque la infraestructura de firma digital, o el sistema que la regule, tiene que posibilitar que también las llaves públicas de dichas Entidades Certificadoras puedan ser conocidas de forma segura por los suscriptores o signatarios que requieran de sus servicios, con el propósito de que ellos sepan fehacientemente que ha sido una Tercera Parte Confiable la que emitió un certificado válido y vigente que respaldará su identidad digital al firmar un documento. Se debe, por ende, considerar la existencia de un órgano público (y no privado), competente técnicamente, u *«órgano Acreditador o Licenciante de Certificadores»*.

En el caso de Venezuela se tiene a la Superintendencia de Servicios de Certificación Electrónica, cuya regulación está contemplada en la Ley de Transmisión de Mensajes de Datos y Firma Electrónica en su capítulo V.

Se señala como una ventaja el hecho de que la entidad de certificación sea pública (Martínez, 2000), ya que su objetivo es el beneficio de la comunidad y, por ende, un mejor servicio. Estas entidades de certificación pueden desempeñar funciones más importantes en el comercio electrónico de un país, como por ejemplo ser la entidad de certificación raíz del Estado, certificando a las entidades de certificación privadas e inclusive a las públicas de menor jerarquía. También podría certificar a los contribuyentes, o ciudadanos, en sus relaciones con la administración pública (Barzallo, 2001). En este sentido, en Venezuela el órgano competente, es decir, la Superintendencia de Servicios de Certificación Electrónica, tiene entre sus principales atribuciones las siguientes:

1. *Otorgar acreditación y correspondiente renovación a los Proveedores de Servicios de Certificación, una vez cumplidas las formalidades y requisitos...*
2. *Revocar o suspender la acreditación...*
3. *Mantener, procesar, clasificar, resguardar y custodiar el Registro de Proveedores...*
4. *Verificar que los Proveedores... cumplan con los requisitos...*
5. *Supervisar la actividad de los Proveedores...*
6. *Liquidar, recaudar y administrar las tasas establecidas en el artículo 24 de este Decreto-Ley...*

7. *Liquidar y recaudar las multas establecidas en el presente Decreto-Ley...*
8. *Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones...*
9. *Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de este Decreto-Ley...*
10. *Inspeccionar y fiscalizar la instalación, operación y prestación de servicios...*
11. *Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativo a presuntas infracciones a este Decreto-Ley...*
12. *Requerir de los Proveedores... o sus usuarios, cualquier información que considere necesaria...*
13. *Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores y los usuarios, cuando ello sea solicitado por las partes...*
14. *Seleccionar los expertos técnicos o legales que considere necesario...*
15. *Presentar un informe anual al Ministerio de su adscripción...*
16. *Tomar las medidas correctivas y preventivas que considere...*
17. *Imponer las sanciones establecidas en este Decreto-Ley...*
18. *Determinar la forma y alcance de los requisitos para ser Proveedor...*
19. *Las demás que establezca la ley y los reglamentos.*

### 4.1. **Certificados Electrónicos:** ***Noción y Tipos***

Los certificados son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten la verificación de que una clave pública dada pertenece fehacientemente a una determinada persona.

Los certificados ayudan a evitar que alguien utilice una clave falsa haciéndose pasar por otro.

En su forma más simple, contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del certificado y la firma digital del que otorga el certificado. Los certificados se inscriben en un registro (*repository*), considerado como una base de datos a la que el público puede acceder directamente en línea (*on line*) para conocer acerca de la validez de los mismos. Los usuarios o firmantes (*suscribers*) son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de manera que quien pretenda verificar una firma digital, con la clave pública que surge de un certificado, tenga la seguridad de que la correspondiente clave privada es detentada por el firmante.

La Autoridad Certificante puede emitir distintos tipos de certificados. Los certificados de identificación simplemente identifican y conectan un nombre a una clave pública. Los certificados de autorización, en cambio, proveen otro tipo de información correspondiente al usuario, como dirección comercial, antecedentes, catálogos de productos, etc. Otros certificados colocan a la Autoridad Certificante en el rol de notario, pudiendo ser utilizados para la garantía de la validez de un determinado hecho, o que un hecho efectivamente ha ocurrido. Otros certificados permiten determinar día y hora en el que el documento fue digitalmente firmado (*Digital time – stamp certificates*).

El interesado en operar dentro del esquema establecido por la ley, luego de crear el par de claves deberá presentarse ante la autoridad certificante (o funcionario que ella determine) a efectos de registrar su clave pública, acreditando su identidad y/o cualquier otra circunstancia que le sea requerida para obtener el certificado que le permita «firmar» el documento de que se trate. Por ejemplo, para realizar una operación financiera de importancia con un banco, éste puede requerir del interesado un certificado del que surja, además de la constatación de su identidad, el análisis de sus antecedentes penales o financieros. Esto quiere decir que la firma digital del interesado sólo será aceptada por la otra parte si cuenta con el certificado apropiado para la operación a realizar.

## 5. LA REGULACIÓN SUPRANACIONAL: UNA ALTERNATIVA DE SOLUCIÓN PARA EL INTERCAMBIO DE DATOS VÍA INTERNET

Ahora bien, la pregunta obligatoria es: ¿son seguros los medios por donde viaja la información?, porque el mayor interés por parte de las empresas en su desarrollo por el *e-commerce bussines to bussines* es buscar medidas de seguridad para evitar que la información que viaja electrónicamente pueda ser interceptada por extraños y puedan conocer y alterar el contenido del mensaje (Useche, 2001).

De allí que se hable de un seguro informático que debe involucrar un sistema técnico-jurídico integrado por la firma electrónica y los certificados electrónicos, pero donde indudablemente serán los actores sociales (proveedores de servicios de certificados y los controladores del servicio) los terceros llamados a garantizar la seguridad y confidencialidad en la transmisión de los datos por la Web, mientras que los usuarios serán responsables de exigir un servicio eficiente, como lo exige cualquier consumidor de un producto o servicio.

Ésto lleva a plantearse vías de solución que van desde la puesta en marcha de una complicada plataforma tecnológica hasta la creación de organismos públicos o privados en pro de garantizar una transformación cada vez más segura, lo cual crea obstáculos ante el riesgo que por sus importantes consecuencias conviene tener perfectamente controlado. Esto nos lleva a la necesidad de crear no sólo elementos teóricos sino prácticos en pro de la consolidación de las diferentes actividades que pueden desarrollarse a través de la red, especialmente el comercio electrónico.

La expansión y difusión que la red ha alcanzado en países como Inglaterra, Alemania o Estados Unidos es considerable, y producto de ello, en estos países existe un marco legal acorde a las exigencias del cambio informático. Marco normativo que no sólo puede limitarse a establecer mecanismos de seguridad, confidencialidad e integridad y no de repudio, hacia los mensajes transmitidos por la red de redes, sino que es necesario, además, la existencia de un organismo supranacional que vigile la repercusión de la *Web* en las sociedades de cada uno de los países hacia los que esta red se extiende, a fin de establecer las bases de una regulación jurídica adaptada a las necesidades políticas y económicas de la realidad de cada uno de esos estados; y aun cuando Internet alberga cientos de instituciones de carácter internacional que velan por determinados aspectos teleológicos de sus funciones, desarrollo y expansión, surgen elementos que sirven de agentes controladores y supervisores de la información, que se extiende sin límites ni fronteras por Internet.

Desde el punto de vista mercantil, lo más importante es que la red crezca en el plano extremo, favoreciendo y controlando el desarrollo de sistemas y plataformas homologadas para todo el planeta; y desde un punto de vista interno, a través de la utilización únicamente de determinados lenguajes de programación o *software* análogo. De esta forma ambos tipos de expansión quedan controlados por esas instituciones supranacionales de marcado carácter mercantil creadas *ad hoc* (Lagares, 2000).

Por otra parte, en principio será la Buena Fe de las partes la que prevalecerá ante las interrogantes de una jurisdicción y competencia en Internet.

## 7. REFLEXIONES FINALES

Aunque se han desarrollado importantes avances en materia de seguridad informática, partiendo de contratos contra riesgos, firma electrónica, certificados electrónicos, proyectos y leyes que regulan de alguna manera el

nuevo desafío que impone el uso de las «nuevas tecnologías», especialmente de la información y de la comunicación, aún es mucho el camino por recorrer. Los expertos consideran que la implementación de tales mecanismos, o elementos de seguridad y confidencialidad, también originan nuevos desafíos para su auditoria, seguridad y control.

No obstante, debe procurarse que todos participen (entidades públicas y privadas) en procura de consolidar una política nacional, en principio, e internacional a mediano plazo, que establezca las bases para mitigar los efectos del abuso del contenido nocivo que puede haber en Internet; y aprovechar este medio global interactivo para promover, por ejemplo, la democracia, la libertad y el desarrollo de las sociedades civiles.

En definitiva, no basta crear dispositivos de seguridad ajenos a la realidad política, económica y social de nuestros pueblos; por ello es conveniente ir divulgando el contenido de nuestras disposiciones en torno al tema y compararlas, a fin de extraer de ellas lo más favorable, y crear organismos y acuerdos supranacionales que permitan que bien sea la firma electrónica, o los certificados digitales que le otorgan a estos últimos validez, o cualquier otro elemento para la seguridad y confidencialidad informática, ejecutables sin problemas.

## BIBLIOGRAFÍA


BARON, D. *Digital Technology and the implications for intellectual property.* Publicación OMPI sobre el Simposio en Hardvard University, Cambrige, Massachusetts, p. 131.

BARZALLO, J. (2001). «Los terceros de confianza en el comercio electrónico». En REDI.

CASTRO, J. (1995). «El habeas data en Costa Rica». En Carrascosa (Coordinador), *Informática y Derecho.* Actas del III Congreso Iberoamericano de Informática y Derecho (Mérida-España, 24-28 de abril 1995). Mérida, Aranzadi, 1996, p. 1.482.

FONT, A. (2000). *Seguridad y Certificación en el Comercio Electrónico.* España. Biblioteca Fundación Retevisión, p. 165.

JIJENA, R. (2001). «Impuestos, Firmas y Certificados Digitales». En REDI.

KALT, H. (1996). Europa prepara-se para mercados livres nas telecomunicacoes: a Telekom, a concorréncia e o mercado mundial. En *Deutschland.* N° 3, junio.

LAGARES, D. (2000). *Nuevas Tecnologías Internet y el Derecho.* España, Ediciones Carena, p. 145.

MARTÍNEZ, A. (2000). *Comercio Electrónico, firma digital y autoridades de certificación.* España. Civitas.

NEFF, R. (1997). *El Derecho de Autor en el espacio cibernético: una protección universal invita al desarrollo nacional. Ejemplos Teóricos y Prácticos.* Publicación OMPI

sobre el III Congreso Iberoamericano sobre Derecho de Autor y Derechos Conexos, tomo I. Montevideo, p. 521.
RIBAS, J. (1999). *Aspectos Jurídicos del Comercio Electrónico en Internet*. Navarra (España). Aranzadi, p. 294.
TIGRE, P. (1993). «Informática como bases técnica do novo paradigma». En *Sao Paulo en perspectiva*. Nº 4. Octubre-diciembre.
URDANETA, Y. (1996). «Las redes telemáticas: un nuevo paradigma para las revistas científicas de LUZ». En *Memorias Gerencia de Tecnología para las Comunicaciones en el siglo 21*. Maracaibo, del 17 al 20 de septiembre de 1996, p. 27-48.
USECHE, O. (2001). «Intercambio de datos vía Internet». En *PC WORLD*. Año: III. Nº 48, etapa III. Caracas, agosto.

Texto Legal:
Decreto-Ley: «*Ley de Transmisión de Mensajes de Datos y Firma Electrónica*». 28 de febrero de 2001. G. O. No. 37.148