



Revista de
Derecho
Comunicaciones y
Nuevas Tecnologías

DOCUMENTO GECTI NRO. 10
¿PENSAR EN LAS NECESIDADES DEL PAÍS O
MANTENER A ULTRANZA UN STATU QUO PARA
LA FIRMA DIGITAL DE LAS ENTIDADES DE
CERTIFICACIÓN ABIERTA -ECA-?

Nelson Remolina Angarita¹
(Marzo de 2010)

Universidad de los Andes
Facultad de Derecho - GECTI
Revista N.º 4, junio de 2010. ISSN 1909-7786

Documento GECTI nro. 10

¿PENSAR EN LAS NECESIDADES DEL PAÍS O MANTENER A ULTRANZA UN STATU QUO PARA LA FIRMA DIGITAL DE LAS ENTIDADES DE CERTIFICACIÓN ABIERTA -ECA-?

Nelson Remolina Angarita¹

(Marzo de 2010)

SUMARIO

Introducción - I. GECTI - II. OBJETIVO DEL PRESENTE DOCUMENTO - III. NECESIDAD DE REPLANTEAR EL MARCO JURÍDICO DEL COMERCIO ELECTRÓNICO PARA SER MÁS COMPETITIVOS: EL CASO DE LA FIRMA ELECTRÓNICA - IV. ESTRATEGIAS DE POLÍTICAS PÚBLICAS PARA LA IDENTIFICACIÓN ELECTRÓNICA CIUDADANA - V. GREMIOS Y GOBIERNO NACIONAL EN PRO DE REVISAR EL MARCO JURÍDICO SOBRE MECANISMOS DE IDENTIFICACIÓN ELECTRÓNICA - A. *Opinión de la Asobancaria* . B. *Mandato del Conpes 3620 sobre comercio electrónico* - C. *La ONU y el fomento de la confianza en comercio electrónico* - VI. IMPRECISIONES SOBRE LA FIRMA DIGITAL - VII. DE LOS COMPROMISOS QUE HA ADQUIRIDO COLOMBIA EN ALGUNOS ACUERDOS DE COMERCIO - A. *TLC con Estados Unidos* - B. *TLC con Chile* - C. *TLC con Canadá* - VIII. DEL PROYECTO DE DECRETO SOBRE FIRMAS ELECTRÓNICAS - IX. DOING BUSINESS EN COLOMBIA - XI. CONCLUSIONES - XI. ANEXO: TEXTO PUBLICADO DEL PROYECTO DE DECRETO SOBRE FIRMA ELECTRÓNICA

I. GECTI

El Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática (GECTI) fue creado el 5 de octubre de 2001 en la Facultad de Derecho de la Universidad de los Andes. Busca fomentar el trabajo multidisciplinario y establecer un puente entre la Universidad y la sociedad para procurar reflexiones y acciones en materia de la Internet, la Sociedad de la Información y temas convergentes.

¹ Abogado y Especialista en Derecho Comercial de la Universidad de los Andes. Master of Laws del London School of Economics and Political Sciences. Doctorando en Ciencias Jurídicas de la Pontificia Universidad Javeriana. Profesor Asociado de la Facultad de Derecho de la Universidad de los Andes. Director de la Especialización en Derecho Comercial y del Gecti de la Facultad de Derecho de la Universidad de los Andes. <http://www.gecti.org/> o <http://gecti.uniandes.edu.co/>

Las opiniones expresadas en este documento sólo comprometen a su autor y no a la Universidad de los Andes ni a los miembros del GECTI.

II. OBJETIVO DEL PRESENTE DOCUMENTO

Justificar la necesidad de regular la firma electrónica como instrumento de identificación para ser más competitivos e incluyentes en el contexto digital, tanto en lo público (gobierno electrónico) como en lo privado (comercio electrónico).

III. NECESIDAD DE REPLANTEAR EL MARCO JURÍDICO DEL COMERCIO ELECTRÓNICO PARA SER MÁS COMPETITIVOS: EL CASO DE LA FIRMA ELECTRÓNICA

Desde varios espacios han surgido ideas en pro de pensar en las necesidades del país en el entorno electrónico para ser más competitivos.² Particularmente, se ha querido dar mayor fuerza regulatoria a las firmas electrónicas como alternativa al uso de las firmas digitales. De esta manera, se espera que todos tengamos una identificación electrónica, lo cual no se ha logrado masivamente en Colombia debido al alto costo de las firmas digitales de las Entidades de Certificación Abierta (ECA).

2 Cfr. Remolina Angarita, Nelson, "La protección de datos personales y las firmas digitales: dos temas para repensar y actuar", en Periódico Ámbito Jurídico, noviembre de 2009. Disponible en: <http://gecti.uniandes.edu.co/columna.php?Op=columna>. También consúltese: Rodríguez Turriago, Omar, "Diez años de la ley 527 de comercio electrónico: reflexiones sobre la necesidad de su modernización", Periódico Ámbito Jurídico, agosto 2009, p. 14.

Así como la tecnología abre puertas, también las cierra. Mientras la firma digital de las ECA sea costosa seguirá siendo un instrumento de lujo para pocos y una herramienta excluyente de muchos.

Para alcanzar una inmersión masiva de las TIC en todas las actividades, se debe evitar que encaezcan la realización de cualquier gestión. Es importante que los creadores de políticas públicas sobre la materia no creen ni trasladen costos adicionales a los ciudadanos para que puedan beneficiarse del uso las tecnologías.

Piénsese, por ejemplo, en el uso de las firmas digitales de las ECA para realizar negocios electrónicos o cualquier gestión ante una entidad estatal. Si su costo es alto, la gran mayoría de la población no podría acceder a sus beneficios. Tampoco crecerían significativamente las actividades de comercio electrónico que requieran de esta clase de firma, ni se masificaría el gobierno electrónico.

IV. ESTRATEGIAS DE POLÍTICAS PÚBLICAS PARA LA IDENTIFICACIÓN ELECTRÓNICA CIUDADANA

Sobre el particular existen varias opciones:

En primer lugar, el Estado debería proveer de manera gratuita³ un sistema de identifica-

3 Realmente no es gratuito porque todo se paga con impuestos (acá no se recomienda crear nuevos impuestos).

ción electrónica a cada ciudadano. Se trataría de incorporar un sistema único de identificación electrónica que sea económico, práctico, confiable y seguro para todos. En el caso de España, por ejemplo, el Real Decreto 1553/2005⁴, del 23 de diciembre, estableció las bases jurídicas para que el Documento Nacional de Identidad (DNI) constituya el mecanismo de identificación físico y electrónico de los españoles.⁵

En segundo lugar, el Estado podría convertirse en una ECA. Actualmente, la Dirección de Impuestos y Aduanas Nacionales (DIAN) es una entidad de certificación cerrada (ECC), pero sólo para efectos de las relaciones de dicha entidad y los ciudadanos.

En síntesis, debería crearse un único medio de identificación electrónica del ciudadano frente a todas las ramas del Estado y los particulares. Este mecanismo debe ser gratuito, confiable, seguro y de fácil uso para el ciudadano (no perder de vista que éste no es experto en tecnologías). Mientras ello sucede, en el corto plazo debería forjarse un ambiente legal propicio para el uso masivo de la firma electrónica.

4 “por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica”.

5 Según el artículo 1° de dicho decreto, el DNI “permite a los españoles [...] la identificación electrónica de su titular; así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, del 19 de diciembre, de firma electrónica”. La firma electrónica realizada a través del DNI “tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel”

V. GREMIOS Y GOBIERNO NACIONAL EN PRO DE REVISAR EL MARCO JURÍDICO SOBRE MECANISMOS DE IDENTIFICACIÓN ELECTRÓNICA

En el segundo semestre de 2009, aumentaron las voces que refuerzan la tendencia de replantear la regulación existente sobre los medios de identificación electrónicos. Veamos:

A. Opinión de la Asobancaria

La Asobancaria publicó el 23 de octubre de 2009 el documento: *Avances y desafíos para los instrumentos electrónicos en Colombia*. Allí se analizan varias cuestiones importantes para el país, dentro de las cuales se trae a colación el tema de la firma electrónica y digital.

Señala la Asobancaria que “no es posible establecer la superioridad técnica de uno de los dos tipos de firma sobre el otro (cada uno tiene sus fortalezas y debilidades)”. Adicionalmente, asevera que “la ley otorgó ventajas jurídicas injustificadas en materia probatoria a las firmas digitales, en particular a aquellas expedidas por entidades de certificación abiertas”. Esta situación ha sido reforzada, en palabras de dicha entidad, por el decreto 1747 del 2000 y por “prácticas de diferentes entidades públicas, que han dado preferencia al uso de la firma digital”. Recalca que

el “costo de la firma digital constituye una barrera de entrada para el público en general, además de que no respeta el principio de neutralidad tecnológica”.

Concluye la Asobancaria que es necesario contar con “soluciones prácticas y de bajo costo” para dinamizar el comercio electrónico. Así las cosas, sugiere “analizar si el uso de la firma digital es lo más adecuado para el país. O si, por el contrario, otras alternativas disponibles, como las firmas electrónicas [...] cumplen con los requisitos de seguridad para la acreditación y autenticación electrónicas”.

B. Mandato del Conpes⁶ 3620 sobre comercio electrónico

En el documento Conpes 3620⁷ se pone de presente que si bien la firma digital es “reconocida en la actualidad por sus altos estándares de seguridad, puede resultar limitada en el largo plazo de acuerdo a los cambios tecnológicos y su neutralidad”.

El Conpes resalta que en Colombia el precio de los certificados digitales emitidos por entidades de certificación abierta (ECA) “son considerados relativamente altos en comparación de otros países de América Latina, como por ejemplo Chile, lo cual puede representar un

costo de oportunidad en materia de utilización de esta herramienta para las mypimes”.

En virtud de lo anterior, el Conpes recomendó realizar una revisión integral de la ley 527 de 1999 que promueva el uso de la firma electrónica como esquema alternativo de la firma digital.⁸

C. La ONU y el fomento de la confianza en comercio electrónico

Vale la pena transcribir ciertos aspectos de un estudio realizado en el 2009 por la ONU titulado *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas*.⁹

Dice el estudio:

- “La definición de ‘firma electrónica’ en los textos de la CNUDMI es deliberadamente amplia, para que abarque todos los métodos de firma electrónica existentes o futuros”.¹⁰
- “Los métodos de autenticación y firmas electrónicas pueden clasificarse en tres categorías, a saber: los que se basan en lo que el usuario o el receptor sabe (por ejemplo, contraseñas,

6 Consejo Nacional de Política Económica y Social (Conpes)

7 Documento Conpes 3620 del 9 de noviembre de 2009, titulado Lineamientos de política para el desarrollo e impulso del comercio electrónico en Colombia.

8 Documento Conpes 3620 de 2009, p. 32.

9 Disponible en: http://www.uncitral.org/pdf/spanish/publications/sales_publications/Promoting_confidenceS.pdf

10 ONU/Uncitral, *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas*, Viena, 2009, p. 15.

números de identificación personal, NIP), los basados en las características físicas del usuario (por ejemplo, biometría) y los que se fundamentan en la posesión de un objeto por el usuario (por ejemplo, códigos u otra información almacenada en una tarjeta magnética). [...] Entre las tecnologías que se usan en la actualidad figuran las firmas digitales en el marco de una infraestructura de clave pública (ICP), dispositivos biométricos, NIP, contraseñas elegidas por el usuario o asignadas, firmas manuscritas escaneadas, firmas realizadas por medio de un lápiz digital y botones de aceptación de tipo 'sí' o 'aceptar' o 'acepto'. Las soluciones híbridas basadas en la combinación de distintas tecnologías están adquiriendo una aceptación creciente".¹¹

- "La firma digital funciona bien como un medio para verificar las firmas que se crean durante el período de validez de un certificado. Sin embargo, cuando el certificado caduca o se revoca la clave pública correspondiente pierde validez [...]. Por ello, todo mecanismo de ICP requeriría un sistema de gestión de la firma digital para asegurar que la firma siga disponible a lo largo del tiempo".¹²

- "Un volumen importante de operaciones comerciales electrónicas se lleva a cabo en redes cerradas, es decir, en grupos con un número limitado de participantes a los que pueden acceder únicamente personas o empresas previamente autorizadas".¹³ Un ejemplo que se cita de este tipo de redes son las instituciones financieras, las bolsas de valores, etcétera.

11 Ídem, p. 13.

12 Ídem, p. 26.

13 Ídem, p. 37.

Como corolario de lo anterior, contamos con otros medios electrónicos de identificación que pueden ser más seguros y ofrecer mayor certeza de origen que las firmas digitales. No podemos equivocarnos en sostener que la firma digital debe utilizarse para todo, si se trata de una cuestión de seguridad, pues con ese argumento todos los ciudadanos deberíamos movilizarnos en carros blindados y con escoltas. De la misma manera, pero en el campo de los documentos, todo lo que firmamos deberíamos autenticarlo ante notario. ¿Tiene esto sentido en todos los casos?

VI. IMPRECISIONES SOBRE LA FIRMA DIGITAL

El administrador de una entidad de certificación abierta ha sostenido sobre la firma digital algunas afirmaciones que no corresponden a la realidad de lo que dice la ley 527 de 1999.¹⁴

Es falso afirmar que el legislador estableció la firma digital como único equivalente de la firma manuscrita. Esta conclusión desconoce abiertamente el artículo 7º de la ley 527 de 1999. Tampoco es veraz aseverar que la

14 Esta persona afirma sobre la firma digital que: 1) "el legislador estableció la equivalencia con respecto a esta figura y no a la firma electrónica", 2) "para que la firma digital sea válida, requiere la intervención de un tercero de confianza, denominado entidad de certificación digital", 3) "a la luz de la legislación colombiana el equivalente idóneo de la firma manuscrita es la firma digital de una entidad de certificación abierta" (Rincón Cárdenas, Erick, "Discusiones alrededor de la firma digital", en Periódico Ámbito Jurídico, núm. 281, 2009, p. 13).

validez de una firma digital depende de la intervención de una entidad de certificación. Eso no lo dice la ley. Respecto de esta clase de firma, existen tres opciones:

- la digital (sin certificar pero verificable);
- la digital avalada por una Entidad de Certificación Cerrada (ECC); y
- la digital certificada por una ECA.

El artículo 28 de ley 527 de 1999 exige que la firma digital sea “susceptible de ser verificada”, pero en ninguna parte ordena que para que tenga validez deba ser certificada por una entidad de certificación (EC), pues ésta se puede realizar con la clave pública¹⁵ sin que sea necesaria la intervención de una EC.

Verificar una firma no es lo mismo que certificarla, pues en este último caso es necesaria la presencia de una entidad de certificación (EC),¹⁶ pero, se repite, lo que la ley ordena es que la firma digital sea verificada.

La firma digital no es plena prueba de haber firmado una persona. Sólo nos dice que para

firmar se utilizó la clave privada de cierta persona (lo cual no es lo mismo). La firma digital de una entidad de certificación abierta puede ser un equivalente de firma manuscrita, pero no el único.

Actualmente, no sólo existen disposiciones que imponen el uso de la firma digital,¹⁷ sino que es evidente la presencia de una cruzada para minar la legislación colombiana de disposiciones que obliguen utilizar la firma digital avalada por una entidad de certificación abierta (ECA). Así, por ejemplo, en el texto del proyecto de la nueva ley antitrámites del 2009, el artículo 4º, denominado “Trámite administrativo electrónico”, establece que “todo documento electrónico expedido por servidor público en ejercicio de sus funciones y firmado digitalmente tendrá la connotación de documento público”. Concluye el párrafo diciendo que “cuando el trámite de las actuaciones administrativas se adelante por medios informáticos, las firmas autógrafas que la mis-

15 Recuérdese que a la luz del numeral 5 del artículo 1 del decreto 1747 de 2000, la clave pública es el “valor o valores que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador”.

16 En efecto, según el numeral 6 del artículo 1 del decreto 1747 de 2000, el “certificado en relación con las firmas digitales” es un “mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la clave pública de éste”.

17 Algunos ejemplos que corroboran esta afirmación, son las siguientes normas: ley 1350 de 2009, “por medio de la cual se reglamenta la Carrera Administrativa Especial en la Registraduría Nacional del Estado Civil y se dictan normas que regulen la Gerencia Pública”; decreto 852 de 2009, “por medio del cual se modifica parcialmente el decreto 159 de 2002, modificado parcialmente por el decreto 072 de 2005, y se dictan otras disposiciones”; resolución 1339 de 2008 del Ministerio de Transporte, “por la cual se adopta el uso de la firma digital para los sujetos obligados a reportar información al Ministerio de Transporte”; resolución 1448 de 2006 del Ministerio de la Protección Social, “por la cual se definen las condiciones de habilitación para las instituciones que prestan servicios de salud bajo la modalidad de telemedicina”; ley 1111 de 2006, “por la cual se modifica el estatuto tributario de los impuestos administrados por la Dirección de Impuestos y Aduanas Nacionales”, y circulares externas 003 de 2005 de la Superintendente de Industria y Comercio y 100-004 de la Superintendencia de Sociedades.

ma [sic] exija tendrán como equivalente la firma digital emitida por una entidad de certificación digital abierta”.

Esta propuesta está pensada en favorecer a las ECA, dejando de lado lo que han hecho algunas entidades públicas de certificación cerrada (la DIAN, por ejemplo) y obstruyendo la posibilidad para que el Estado utilice la firma electrónica del artículo 7º de la ley 527 de 1999. Este tipo de iniciativas es conveniente como estrategia de comercialización de dicha clase de firmas, pero no consulta los intereses de todos los ciudadanos y del país.

La ley 527 prevé opciones para que cada uno seleccione el medio de identificación electrónica más apropiado para determinadas gestiones. Insistimos en que existen escenarios en los cuales la firma electrónica es más pertinente que la digital, y lo contrario. Ésta debe ser una decisión libre por parte del empresario, pero no una imposición legal o un discurso propagandístico y mesiánico en pro de la firma digital de las ECA.

La firma digital no es mala; lo malo es imponerla por ley, a la fuerza, a las malas.

VII. DE LOS COMPROMISOS QUE HA ADQUIRIDO COLOMBIA EN ALGUNOS ACUERDOS DE COMERCIO

De la información publicada por el Ministerio de Comercio, Industria y Turismo (MCIIT) se puede constatar que en los acuerdos de comercio suscritos por Colombia con otros países, existen obligaciones contraídas en torno a la autenticación electrónica en el contexto del comercio electrónico.

Todos los convenios obligan a verificar si nuestra regulación está a tono con los compromisos adquiridos. Esto aplica no sólo al tema de firmas electrónicas, sino a otros de gran importancia como la protección de datos personales y la protección del consumidor

Lo pactado implica repensar, entre otros, si se debe mantener la legislación actual sobre firmas digitales. Indudablemente, por ser más neutral y universal, los acuerdos refuerzan la necesidad de dar vía libre a la firma electrónica y en ese sentido, el proyecto de decreto que anexamos al presente documento Gecti merece ser considerado.

Veamos la parte pertinente de los diferentes acuerdos de comercio suscritos por Colombia:

A. TLC con Estados Unidos¹⁸

En el artículo 15.6 (titulado *Autenticación*) se acordó que:

Ninguna Parte podrá adoptar o mantener legislación sobre autenticación¹⁹ electrónica que:

- a) prohíba a las Partes en una transacción electrónica determinar en forma mutua los métodos apropiados de autenticación para dicha transacción; o
- b) impida a las Partes tener la oportunidad de establecer ante las instancias judiciales o administrativas que la transacción electrónica cumple con cualquier requerimiento legal con respecto a la autenticación.²⁰

De mucha importancia resulta este acuerdo para el tema en estudio, porque reivindica la necesidad de garantizar el principio de libertad de las partes en seleccionar el medio de identificación que utilizarán en el contexto electrónico. En este sentido, podría inicial-

mente afirmarse que son inconsistentes con los compromisos del TLC las normas que impongan a los ciudadanos utilizar determinado sistema de identificación en las transacciones electrónicas.

Por otra parte, puede observarse que también se acordó un principio de libertad probatoria en materia de autenticación. Así, es muy importante que en Colombia se refuerce normativamente el uso de la firma electrónica, confiriéndole, entre otras, igualdad de tratamiento probatorio al que de manera privilegiada únicamente ha tenido por más de una década la firma digital de las ECA.

Gran parte del proyecto de decreto sobre firma electrónica, precisamente, recoge la idea de literales a) y b) del citado artículo 15.6.

B. TLC con Chile²¹

En el capítulo 12 sobre comercio electrónico se acordaron algunos aspectos relacionados con el tema en cuestión. Veamos:

Según el artículo 12.7 “ninguna parte podrá adoptar o mantener legislación sobre autenticación electrónica que impida a las Partes mantener la oportunidad de establecer ante

18 Cfr. ley 1143 de 2007 “por medio de la cual se aprueba el “Acuerdo de promoción comercial entre la República de Colombia y los Estados Unidos de América”, sus “Cartas Adjuntas” y sus “Entendimientos”, suscritos en Washington el 22 de noviembre del 2006”. (Declarada exequible por la Corte Constitucional en la Sentencia C-750 de 2008).

19 Según el artículo 15.8 (definiciones), “autenticación significa el proceso o el acto de establecer la identidad de una parte en una comunicación o transacción electrónica o asegurar la integridad de una comunicación electrónica”.

20 Este texto fue tomado de la página web del Ministerio de Comercio, Industria y Turismo. Cfr. <http://mincoweb1.mincomercio.gov.co/tlcmemorias/textotratado/15COMERCIO ELECTRONICO.pdf>. Consultado el: 8 de febrero de 2010.

21 Según la página web del Ministerio de Comercio, Industria y Turismo, el Acuerdo de Libre Comercio fue suscrito el 27 de noviembre de 2006 y entró en vigor el 8 de mayo de 2009. Ver: <http://www.mincomercio.gov.co/eContent/newsdetail.asp?id=2429&idcompany=7>. Consultado el: 8 de febrero de 2010)

las autoridades judiciales y administrativas que la transacción electrónica cumple con cualquier requerimiento legal con respecto a la autenticación”²². En el artículo 12.8 se establece que la autenticación es el “proceso o el acto de establecer la identidad de una parte en una comunicación o transacción electrónica o asegurar la integridad de una comunicación electrónica”.

Reiteramos en este punto lo planteado respecto del literal b) del artículo 15.6 del TLC de Colombia con los Estados Unidos.

C. TLC con Canadá

En el capítulo xv se fijaron los acuerdos sobre comercio electrónico. De la misma manera que el TLC con Chile, el artículo 1509 dispone que la autenticación es el “proceso o el acto de establecer la identidad de una parte en una comunicación o transacción electrónica o asegurar la integridad de una comunicación electrónica”.²³

No existe disposición explícita sobre los mecanismos de identificación electrónica, pero los dos países reconocen la importancia de:

1) evitar barreras innecesarias que dificulten el comercio realizado por medios electrónicos (numeral 4º del artículo 1502), y 2) “la claridad, transparencia y previsibilidad de sus marcos normativos nacionales para facilitar, en la mayor medida posible, el desarrollo del comercio electrónico”.²⁴

VIII. DEL PROYECTO DE DECRETO SOBRE FIRMAS ELECTRÓNICAS

En mayo del 2009, el Ministerio de Comercio, Industria y Turismo publicó el texto del proyecto de decreto “Por el cual se reglamenta la firma electrónica”²⁵ (anexo). Si bien esta iniciativa aún no ha sido convertida en decreto, merece algunos comentarios:

En nuestro país se está hablando hace más de diez años de firmas digitales, pero éstas no se han masificado. La firma electrónica, en cambio, se ha venido utilizando en el mundo desde la década de los sesenta en el contexto de los acuerdos EDI a que se refiere proyecto del decreto. En otras palabras, el tiempo se ha encargado de demostrar que desde los inicios del comercio electrónico la firma electrónica ha sido el instrumento empleado por los empresarios para identificarse y emitir

22 Tomado de la página web del Ministerio de Comercio, Industria y Turismo: <http://www.mincomercio.gov.co/eContent/documentos/negociaciones/Textos-def-colombiachile//12%20Capítulo.pdf>. Consultado el: 8 de febrero de 2010.

23 Texto tomado de la página del Ministerio de Comercio, Industria y Turismo <http://www.mincomercio.gov.co/eContent/documentos/negociaciones/canada/TLC-Canada/Espanol-Cap13-23.pdf>. Consultado el: 8 de febrero de 2010)

24 Cfr. numeral 2º del artículo 1502 del Acuerdo de Libre Comercio entre Canadá y la República de Colombia.

25 El texto fue publicado en <http://www.mincomercio.gov.co/eContent/NewsDetail.asp?ID=6835>. Consultado el: 25 de mayo de 2009).

documentos electrónicos, mensajes de datos auténticos, etcétera.

Es muy positiva, entre otras, la consagración en el proyecto de lo atinente a los acuerdos EDI, pues actualmente un porcentaje importante de los negocios electrónicos se realiza en mercados electrónicos cerrados (*e-marketplaces*) cuyo soporte jurídico son dichos acuerdos.

El decreto abre los ojos a los neófitos al respecto para que también exploren la firma electrónica como medio de identificación masivo en el contexto digital. Adicionalmente, pone a Colombia a tono con los países o bloques económicos con los que está suscribiendo tratados de libre comercio. En Estados Unidos y en Europa las leyes se refieren a la firma electrónica.

Es positiva y saludable la iniciativa para el país porque es neutral tecnológicamente, no concede privilegios y, sobre todo, es consistente con estándares internacionales y la misma ley 527 en lo pertinente. Nótese cómo el precitado proyecto de decreto sigue muy de cerca los siguientes documentos: 1) Ley Modelo de la ONU sobre Firmas Electrónicas con la guía para su incorporación al derecho interno, 2001; y 2) Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, 2005.

Otro aspecto favorable del proyecto de decreto es que deja intacta toda la regulación

sobre firmas digitales. De esta manera, se reabre al país una baraja de posibilidades de identificación tecnológica y se permite a las empresas y a los consumidores seleccionar el mecanismo más apropiado para cada necesidad particular.

Como era de esperarse, esta propuesta no ha sido bien recibida por el representante legal de una entidad de certificación abierta (ECA), quien se opone a que se conceda a las firmas electrónicas los mismos privilegios probatorios que tienen las firmas digitales certificadas por las entidades de certificación abierta (ECA).²⁶ Esta posición es entendible en la medida que si se confiere igual valor probatorio a una firma electrónica que a una firma digital certificada por una ECA se afectaría el negocio de dichas empresas, pero ello no significa que la propuesta de decreto sea mala o inconveniente para el país.

Los cambios son bienvenidos si realmente suman al escenario legal y favorecen a la sociedad en general. No se debe cerrar jurídicamente la puerta al uso de la firma electrónica ni avalar un monumento ciego, acrílico y de adoración perpetua a la firma digital.

Nos parece mesiánico pretender definir qué es lo bueno o malo para el país, sobre todo desde una posición donde claramente brota

²⁶ Cfr. Rincón Cárdenas, Erick. "Sobre el proyecto de reglamentación de firmas electrónicas". Periódico *Ámbito Jurídico*, núm. 289, 2010, pp. 14-15.

un conflicto de intereses entre quien opina y la empresa que representa. No es sensato mantener a ultranza un statu quo a las firmas digitales que certifican las ECA.

Colombia merece cambios de verdad, no meros retoques estéticos. Por eso el proyecto de decreto busca ampliar los privilegios probatorios que vía artículo 15 del decreto 1747 del 2000 se confirieron únicamente a las entidades de certificación abierta.

IX. DOING BUSINESS EN COLOMBIA

El proyecto Doing Business procura establecer qué favorable es la regulación de un país para realizar negocios. Se trata de un reporte del Banco Mundial y la Corporación Financiera Internacional que compara 183 países en cuanto a la normatividad sobre algunas áreas. Respecto al conjunto de aspectos regulatorios de nuestro país que facilitan hacer negocios, los resultados actuales de Colombia frente a 2009 son los siguientes:

TABLA 1. Cuadro comparativo de Colombia en el ranking 2009-2010. Proyecto Doing Business del Banco Mundial (marzo de 2010)

Tema	Ranking 2010	Ranking 2009	Cambio
Hacer negocios	37	49	+12
Apertura de un negocio	74	82	+8
Manejo de licencias de construcción	32	47	+15
Contrato de trabajadores	63	59	-4
Registro de propiedades	51	78	+27
Obtención de crédito	61	59	-2
Protección de los inversores	5	25	+20
Pago de impuestos	115	148	+23
Comercio transfronterizo	97	96	-1
Cumplimiento de contratos	152	149	-3
Cierre de una empresa	32	32	0

Fuente: tomado de <http://espanol.doingbusiness.org/ExploreEconomies/?economyid=46> (última consulta: 1° de marzo de 2010)

Aunque en el informe no se incluye explícitamente lo atinente a los sistemas de identificación electrónica, creemos que la propuesta de reglamentación anexa contribuirá a crear un mejor ambiente legal que ayudará a fomentar la aplicación del principio de neutralidad tecnológica en el contexto digital.

Lo anterior facilitará la realización de trámites y la firma de documentos que, por ejemplo, tengan relación con los pasos para formar una empresa en Colombia (creación electrónica de documentos de constitución y registros en línea de éstos ante las cámaras de comercio). Lo propio sucederá con muchas actividades que se pueden realizar ciento por ciento en línea, siempre y cuando se eliminen formalismos medievales innecesarios y contemos con sistemas de registro electrónicos prácticos, efectivos, seguros, económicos y competitivos.

La iniciativa también es provechosa porque dejará en manos de los empresarios y del Estado un instrumento de identificación electrónica más económico.

XI. CONCLUSIONES

Para el ciudadano los costos cobran mucha relevancia, a tal punto que podrían determinar el éxito o fracaso de la puesta en marcha de las políticas y actividades del sector público y privado en el campo de la identificación electrónica.

Lo ideal sería que todos tuviésemos una cédula de ciudadanía electrónica como medio de identificación de los colombianos en el contexto digital. Sobre esto ya existen esfuerzos en otros países que deberían replicarse en Colombia. Pero mientras ello sucede, resulta sensato pensar en fortalecer un escenario legal para otorgarles a los ciudadanos un medio de identificación más económico e incluyente que, en ciertos casos, puede ser más seguro y confiable que las firmas digitales de las Entidades de Certificación Abierta (ECA).

La firma digital no es el único medio jurídicamente válido para suplir la firma tradicional en el contexto digital. La ley no exige que la firma digital sea siempre certificada por una Entidad de Certificación (EC); esta puede ser verificada sin necesidad de la intervención forzosa de las EC. El uso de la firma digital o la firma electrónica debe ser una decisión de los empresarios y no una imposición legal.

Es positivo, necesario y saludable el proyecto de decreto sobre firmas electrónicas (anexo) porque es neutral tecnológicamente, no concede privilegios a nadie y, sobre todo, es incluyente, consistente con estándares internacionales y la misma ley 527 en lo pertinente.

Imponer el uso de la firma digital de las ECA y no dar luz verde a una buena reglamentación sobre firmas electrónicas no parece ser una medida sensata ni alineada con el propósito de expedir regulaciones modernas y tecnológicamente neutrales. Tampoco es una

decisión consistente con los compromisos internacionales de Colombia en los diferentes TLC suscritos a la fecha, ni contribuirá a crear un ambiente legal propicio para realización de negocios y actividades a través de las TIC.

XI. ANEXO: TEXTO PUBLICADO DEL PROYECTO DE DECRETO SOBRE FIRMA ELECTRÓNICA

República de Colombia
Ministerio de Comercio, Industria y Turismo
Decreto número () de 2009
“Por el cual se reglamenta la firma
electrónica”

El Presidente de la República de Colombia,

en uso de sus facultades constitucionales y legales, especialmente de las que le confiere el numeral 11 del artículo 189 de la Constitución Política,

Considerando:

Que se ha considerado al comercio electrónico como motor de crecimiento de la economía del siglo XXI y factor que contribuye a fomentar la competitividad empresarial de las pymes y mipymes a través del uso de las tecnologías de información y comunicación.

Que para impulsar el desarrollo del comercio electrónico, internacionalmente se [ha] recomendado promover enfoques apropiados para

el reconocimiento legal de firmas electrónicas bajo principios de neutralidad tecnológica.

Que la firma electrónica representa un medio de identificación electrónico flexible y tecnológicamente neutro que se adecua [sic] a las necesidades de los particulares, las empresas y el Estado.

Que ante la evolución de las innovaciones tecnológicas, es necesario establecer criterios para el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología utilizada.

Que en documento Conpes 3419 del 17 de abril de 2006 se destacó que la falta de legalización de la firma electrónica presenta un obstáculo al crecimiento de los canales virtuales.

Que es indispensable, tanto en el comercio como en el gobierno electrónico y todas las demás actividades que se realizan a través del uso e intercambio de mensajes de datos o documentos electrónicos, avalar jurídicamente el uso de las nuevas tecnologías de identificación personal.

Que en el artículo 7° de la ley 527 de 1999 se consagró la firma electrónica como equivalente funcional de la firma.

Que se hace necesario reglamentar la firma electrónica para generar mayor entendimiento sobre la misma [sic], dar seguridad jurídica a los negocios que se realicen a través de medio electrónicos y facilitar el uso masivo de la

firma electrónica en todo tipo de transacciones entre particulares y frente al Estado.

DECRETA:

Artículo 1°. *Definiciones.* Para los fines del presente decreto se entenderá por

a) *Acuerdo EDI.* Acuerdo de voluntades mediante el cual se estipulan las condiciones legales a que se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos (EDI).

b) *Datos de creación de la firma electrónica.* Datos únicos y personalísimos, tales como códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

c) *Firma electrónica.* De conformidad con el artículo 7° de la ley 527 de 1999, se entenderá como firma electrónica cualquier procedimiento, método o dispositivo electrónico, óptico o similar tales como, entre otros, códigos, contraseñas, datos biométricos o claves criptográficas privadas que el firmante utiliza para suscribir documentos electrónicos o mensajes de datos y que:

I) Permite identificar al firmante de un mensaje de datos o un documento electrónico y para indicar que el contenido cuenta con su aprobación;

II) Sea tanto confiable como apropiado para el propósito por el cual el mensaje o documento electrónico fue generado o comunicado, aten-

didadas todas las circunstancias del caso, inclusive todo acuerdo EDI aplicable entre las partes.

d) *Firmante.* Persona que posee los datos de creación de la firma y que actúa en nombre propio o por cuenta de la persona a la que representa.

Artículo 2°. *Neutralidad tecnológica e igualdad de tratamiento de las tecnologías para la firma electrónica.* Ninguna de las disposiciones del presente decreto será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método, procedimiento, dispositivo o tecnología para crear una firma electrónica que cumpla los requisitos señalados en el literal c) del artículo 1° de este decreto.

Artículo 3°. *Confiable de la firma electrónica.* La firma electrónica se considerará confiable si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración no autorizada de la firma electrónica hecha después del momento de la firma.

Parágrafo. Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona:

- a) demuestre de otra manera que la firma electrónica es confiable y apropiada para los fines que suscribió un documento electrónico o se generó o comunicó un mensaje de datos; o
- b) aduzca pruebas de que una firma electrónica no es confiable.

Artículo 4°. *Atributos jurídicos de la firma electrónica.* Cuando una firma electrónica haya sido fijada en un mensaje de datos o en un documento electrónico se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos o documento electrónico y de ser vinculado con el contenido del mismo [sic].

El uso de una firma electrónica tendrá la misma fuerza y efectos que el uso de la firma, la firma manuscrita u otros tipos de firma diferentes a la firma digital, si aquélla incorpora los siguientes atributos:

- a) Es única a la persona que la usa.
- b) Es susceptible de ser verificada por cualquier medio útil para la formación del convencimiento del juez, los particulares o las entidades públicas.
- c) Está bajo el control exclusivo de la persona que la usa.
- d) Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma electrónica es invalidada.

Artículo 5°. *Obligaciones del firmante.* El firmante debe:

- a) mantener control y custodia sobre los datos de creación de la firma;
- b) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;
- c) Dar aviso oportuno a cualquier persona que posea, haya recibido o va a recibir documentos o mensajes de datos firmados electrónicamente por el firmante, si:
 - I) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o
 - II) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.

Parágrafo. Se entiende que los datos de creación del firmante han quedado en entredicho cuando éstos, entre otras, han sido conocidos ilegalmente por terceros, corren peligro de ser utilizados indebidamente, o el firmante ha perdido el control o custodia sobre los mismos [sic] y en general cualquier otra situación que ponga en duda la seguridad de la firma electrónica o que genere reparos sobre la calidad de la misma [sic].

Artículo 6°. *Firma electrónica pactada mediante acuerdo EDI.* Salvo prueba en contrario, se presume que los mecanismos o técnicas de identificación personal o autenticación electrónica que acuerden utilizar las partes mediante acuerdo EDI, cumplen los requisitos de firma electrónica.

Las partes que suscriban acuerdos EDI en el que pacten utilizar la firma electrónica como medio de identificación personal no negarán a la misma admisibilidad y valor probatorio entre sí o ante terceros [sic].

Artículo 7º. Admisibilidad y valor probatorio. La firma electrónica será admisible como prueba en toda actividad de naturaleza pública o privada frente a particulares, las autoridades públicas, la administración de justicia y en general frente a todas las ramas del poder público, los órganos de control y la organización electoral.

De conformidad con el artículo 11 de la ley 527 de 1999, para la valoración de la fuerza probatoria de la firma electrónica, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado la firma electrónica y conservado la integridad de la información, y cualquier otro factor pertinente.

Artículo 8º. Criterios para establecer el grado de seguridad de las firmas electrónicas. Para determinar si los procedimientos, métodos o dispositivos electrónicos que se utilicen como firma electrónica son seguros, y en qué medida lo son, podrán tenerse en cuenta los siguientes factores:

- a) El grado de cumplimiento de los estándares establecidos para el efecto por la Superintendencia de Industria y Comercio.

- b) El concepto técnico emitido por un órgano independiente y especializado.

- c) La existencia de una auditoría especializada, periódica e independiente sobre los procedimientos, métodos o dispositivo electrónicos que una parte suministra a sus clientes o terceros como mecanismo electrónico de identificación personal.

- d) Cualesquiera otros factores pertinentes.

Artículo 9º. El presente decreto rige a partir de su publicación en el *Diario Oficial* y deroga todas las normas que le sean contrarias.

Publíquese y cúmplase.

Dada en Bogotá, D. C., a los [...]

El Ministro de Comercio, Industria y Turismo
Luis Guillermo Plata Páez