Fecha de recepción: 31 de enero de 2014 / Fecha de aprobación: 28 de abril de 2014

Revista de Derecho Comunicaciones y Nuevas Tecnologías

Neutralidad tecnológica y función administrativa electrónica

Nelson Remolina Angarita

Artículo de reflexión

Universidad de los Andes
Facultad de Derecho
Revista de Derecho, Comunicaciones y Nuevas Tecnologías
No. 11, Enero - Junio de 2014. ISSN 1909-7786

Neutralidad tecnológica y función administrativa electrónica

Resumen

Este artículo de reflexión tiene como objetivo destacar la importancia del principio de neutralidad en el gobierno electrónico. Con un ejemplo, se destaca la necesidad de regular sobre gobierno electrónico garantizando que las normas sean neutrales desde el punto de vista tecnológico. Particular referencia se hace al caso de las alternativas de identificación electrónica (firma electrónica y firma digital) de los ciudadanos.

Si no se garantiza la neutralidad tecnológica se generan altos costos económicos. Estos costos pueden convertirse en una forma de excluir a la mayoría de los ciudadanos de los beneficios del gobierno electrónico.

Palabras clave: Principio de neutralidad tecnológica, gobierno electrónico, firma electrónica, firma digital, Internet, Tecnologías de la Información y la Comunicación (TIC), neutralidad tecnológica.

Technological neutrality and e-government

Abstract

This article aims to highlight the importance of the principle of neutrality in e-government. With an example, highlights the need to regulate electronic government ensuring that the rules are neutral from a technological point of view. Particular reference is made to the case of the alternative electronic identification (electronic signature and digital signature) of citizens.

If technological neutrality does not guarantee high economic costs are generated. These costs can become a way of excluding the majority of the citizens of the benefits of e-government.

Key words: Principle of technological neutrality, electronic government, electronic signature, digital signature, Internet, Information and Communication Technologies (ICT), technology neutrality.

Neutralidade tecnológica e função administrativa eletrônica

Resumo

Este artigo de reflexão tem como objetivo destacar a importância do princípio de neutralidade no governo eletrônico. Com um exemplo, se destaca a necessidade de regular sobre governo eletrônico garantindo que as normas sejam neutrais desde o ponto de vista tecnológico. Particular referência se faz ao caso das alternativas de identificação eletrônica (assinatura eletrônica e assinatura digital) dos cidadãos.

Se não se garante a neutralidade tecnológica se geram altos custos econômicos. Estes custos podem converter-se em uma forma de excluir à maioria dos cidadãos dos benefícios do governo eletrônico.

Palavras-chave: Princípio de neutralidade tecnológica, governo eletrônico, assinatura eletrônica, assinatura digital, Internet, tecnologias da informação e a comunicação (TIC), neutralidade tecnológica.

Sumario

Neutralidad tecnológica y función administrativa electrónica[1]

Nelson Remolina Angarita[2]

Introducción

Desde la década de los setenta se vienen utilizando las Tecnologías de la Información y la Comunicación (TIC) en ciertas cuestiones de la gestión estatal colombiana. No obstante, a finales del siglo pasado aumentó significativamente el uso de las TIC en la función administrativa. Pero quizá en la última década del siglo XXI se han expedido regulaciones que prácticamente irrigan el uso masivo de las TIC en toda la actividad estatal. Las normas básicas o vertebrales del tema ya existen pero la debida aplicación de las mismas es una tarea pendiente en ciertas cuestiones.

Si no se usan adecuadamente las TIC seremos testigos de pérdida de tiempo, dinero y oportunidades. Las TIC abren y cierran puertas. Pueden ser un medio de inclusión o de exclusión ciudadana. También pueden convertirse en una herramienta de protección o de amenaza y desprotección de los derechos de las personas. El que se obtenga uno y otro resultado depende de la revisión de algunas políticas y de su implementación.

En 2009 el Congreso de la República estuvo a punto de aprobar un proyecto de ley que decía lo siguiente: "Trámite administrativo electrónico: [...] cuando el trámite de las actuaciones administrativas se adelante por medios informáticos, las firmas autógrafas que la misma exija tendrán como equivalente la firma digital emitida por una entidad de certificación digital abierta"[3]

---

1 Cómo citar este artículo: Remolina Angarita, Nelson (Junio, 2014). Neutralidad tecnológica y función administrativa electrónica. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, 11.

2 Profesor asociado de la Facultad de Derecho de la Universidad de los Andes. Director del GECTI (Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática, http://gecti.uniandes.edu.co/). Correo: nremolin@uniandes.edu.co.

3 Este texto fue debatido en 2009 por el Congreso de la República de Colombia con ocasión de un proyecto de ley antitrámites (artículo 4). Finalmente no fue aprobado en los términos propuestos. Se modificó eliminando el requisito de exigir la firma digital emitida por una entidad de certificación abierta. Desde la academia se alertó al Congreso sobre las implicaciones de aprobar la norma en su redacción original. Ver: Remolina Angarita, N. *Imprecisiones y despropósitos de algunas propuestas de regulación*. Columna de opinión publicada el 27 de julio de 2009 en *Ámbito Jurídico*.

(Subrayamos). ¿Qué implicaciones tendrían este tipo de iniciativas regulatorias para las colombianas y los colombianos? ¿Por qué es importante que la regulación sobre el derecho administrativo sea neutral tecnológicamente? ¿De qué forma afectan las normas no neutrales tecnológicamente a la función pública, las empresas y los ciudadanos? ¿Por qué es importante que los funcionarios públicos sean "neutros" tecnológicamente en sus decisiones, en la fijación de políticas públicas y en su gestión frente a los ciudadanos?

El presente texto de reflexión pretende dar respuesta a los planteamientos propuestos y recalcar la importancia de la neutralidad tecnológica en la función administrativa. Particular referencia se hará al caso de los mecanismos de identificación electrónica frente al Estado. Procuramos señalar que la promulgación de políticas públicas y de normas que desconocen el principio de neutralidad tecnológica son inconvenientes para los ciudadanos porque eliminan la posibilidad de utilizar alternativas tecnológicas más económicas y sensatas para identificarse electrónicamente. Las normas no neutrales normalmente favorecen a algunos empresarios pero perjudican a los ciudadanos y se traducen en un desperdicio de recursos públicos.

Para el efecto, destacaremos la relevancia de las TIC como instrumentos para materializar algunos fines del Estado. Posteriormente nos centraremos en analizar la importancia de la neutralidad tecnológica en la gestión estatal. En este punto nos enfocaremos en el caso de las alternativas de identificación electrónica señalando algunos reparos frente a iniciativas que han pretendido imponer un determinado mecanismo para identificar las personas en el contexto digital, como lo son las firmas digitales de las entidades de certificación abierta. Previo a las conclusiones traeremos a colación la necesidad de una política de Estado sobre la identificación electrónica ciudadana.

I. INTERNET Y LAS TIC COMO INSTRUMENTOS PARA ALCANZAR ALGUNOS COMETIDOS ESTATALES

Internet es la tecnología de información y comunicación (TIC) que más ha impactado el mundo en prácticamente todos los escenarios (social, político, económico, cultural, etc.). Se podría hablar del mundo antes y después de Internet. Particularmente de la "era digital y de la información" que ha cambiado y transformado muchas cosas en nuestra sociedad gracias a Internet.[4]

Internet[5] significa "entre redes" y desde 1995 Vinton G. Cerf planteó que Internet representa una infraestructura global de información jamás antes vista.[6] Vivimos en un mundo hiperconectado gracias a Internet, el cual se ha converti-

4 Sobre este aspecto consúltese el siguiente texto de Eric Schmidt y Jared Cohen (2014): *The new digital age. Transforming nations, businesses, and our lives*. Estados Unidos: Vintage books.

5 Según el Diccionario de la Lengua Española, Internet es una "red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación". Real Academia Española. Diccionario de la Lengua Española. Avance de la 23. ª edición. Recuperado de http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=internet

6 Cerf, V. 1995. Computer networking: global infraestructure for the 21st century. Computing Research Association (CRA). Recuperado de http://www.cs.washington.edu/homes/lazowska/cra/networks.html

do, entre otras, en un canal de comunicación, información y gestión. Son tantas las actividades públicas y privadas que se realizan en la red que se ha considerado Internet como el nuevo hábitat del siglo XXI.[7] Dentro de dicho hábitat se encuentran las relaciones entre el Estado y los ciudadanos.

A medida que crece el porcentaje de personas con acceso a Internet, aumentan las posibilidades para que más personas puedan beneficiarse de más y mejores servicios del Estado a través de Internet. Esto, desde luego, no es algo automático ni solo depende de incrementar la tasa de penetración de la población a Internet. También dependerá de tres cosas. En primer lugar, que el Estado haga un uso adecuado, estratégico e inteligente de Internet y las TIC para cumplir sus cometidos. En segundo lugar, que los funcionarios públicos se pongan a tono con el entorno tecnológico y se genere un cambio cultural respecto de la forma tradicional del obrar para cumplir los cometidos estatales. Finalmente, que los ciudadanos sean formados y capacitados para saber utilizar adecuadamente las TIC y sacar provecho legal y ético de las mismas.

Las cifras muestran el aumento importante del número de personas con acceso a Internet. A junio de 2012 la tasa mundial de penetración de usuarios fue del 34,3 %[8] y se ha establecido como meta que la misma sea del 60 % para 2015,[9] es decir, aproximadamente 4 200 millones de personas. En el caso de Latinoamérica y el Caribe el 42,9 %[10] de la población tiene acceso a Internet y Colombia cuenta con una tasa de penetración a Internet del 59,5 %[11] (aproximadamente veintisiete millones de colombianas y colombianos).

Nuestra constitución establece que la "función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad" y ordena a las autoridades administrativas "coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado".[12] Las Tecnologías de la Información y la Comunicación (TIC) son una herramienta que utilizada adecuada e inteligentemente ayudan a materializar los principios constitucionales citados.[13]

7 Teruel Lozano, M. (2013). Libertades y derechos de las personas en Internet: retos en materia de reconocimiento y la tutela de los derechos fundamentales ante el paradigma tecnológico de la sociedad del siglo XXI. En *Desafíos para los derechos de la persona ante el siglo XXI: Internet y nuevas tecnologías*. Aranzadi (España): Thomson Reuters, p. 39.

8 Cfr. Internet World Stats. 2012. Internet Usage Statistics. The Internet Big Picture. World Internet Users and Population Stats. 30 de junio de 2012. Recuperado de http://www.internetworldstats.com/stats.htm

9 Esta es una meta fijada por la Comisión de la Banda Ancha de la Unión Internacional de Telecomunicaciones. Véase: Unión Internacional de Telecomunicaciones. 2012. Medición de la Sociedad de la Información 2012. Sinopsis, p. 7. Recuperado de http://www.itu.int/ITU-D/ict/publications/idi/material/2012/MIS2012-ExecSum-S.pdf

10 Cfr. Internet World Stats. 2012. Internet Usage Statistics. The Internet Big Picture. World Internet Users and Population Stats. 30 de junio de 2012. Recuperado de http://www.internetworldstats.com/stats.htm

11 Cfr. Internet World Stats. 2012. Internet Usage Statistics. The Internet Big Picture. World Internet Users and Population Stats. 30 de junio de 2012. Recuperado de http://www.internetworldstats.com/stats2.htm#americas

12 Cfr. artículo 209 de la Constitución Política de Colombia de 1991.

13 Sobre procedimiento administrativo electrónico véase: Quintero Navas, G. A. (2011). Procedimiento administrativo electrónico: aportes

Señalan Montañés y Olier que "entre las claves del desarrollo de una administración eficaz está el uso de las tecnologías de la información y de las comunicaciones para facilitar las relaciones entre los administrados y la administración".[14] Las TIC pueden ser el factor determinante para mejorar la gestión del Estado frente a los ciudadanos siempre y cuando se utilicen de manera adecuada y no se conviertan en una nueva carga complicada para adelantar actuaciones administrativas o en una herramienta excluyente frente a los ciudadanos que no tienen cómo pagar los sobrecostos que genera acudir a las TIC para iniciar un trámite frente a una entidad pública.

El uso de las TIC debe centrarse en satisfacer las necesidades y garantizar los derechos y libertades de los ciudadanos que son, en últimas, la razón de ser del andamiaje estatal. Principios internacionales y nacionales del gobierno en línea[15] recalcan la necesidad de "incrementar la calidad de los servicios y productos públicos que el Estado tiene que suministrar a los ciudadanos al mejorar la eficiencia, la eficacia y una mayor transparencia de la gestión pública, aprovechando la utilización de las TIC en el Gobierno y en la Administración Pública".[16]

Las TIC no deben utilizarse porque están de moda sino porque realmente sumen valor agregado que transformen la función administrativa en una gestión más eficiente, transparente, económica, rápida, incluyente e imparcial. La gestión estatal a través de las TIC representa la "nueva gran oportunidad de aprovechar las tecnologías de la información para maximizar el servicio del Estado al ciudadano",[17] y lograr que este "sea más escuchado por los administradores y obtenga una máxima satisfacción".[18]

II. NEUTRALIDAD TECNOLÓGICA Y GESTIÓN ESTATAL

Desde hace tiempo el Estado colombiano está migrando hacia el uso masivo de las Tecnologías de la Información y la Comunicación (TIC) para, entre otras, "modernizar" su gestión y ser más eficiente. Existen varios caminos para lograrlo pero como la gestión pública es una tarea reglada, las normas van delineando el camino a seguir.

---

de la Ley 1437 de 2011. Capítulo de libro publicado en *Derecho & TIC 10.0*. Bogotá: Ediciones Uniandes-Editorial Temis, p. 75-108.

14 Montañés, P. y Olier E. (2006). *Corporate governance intelligence: desarrollando la corporación en web*. Madrid: Prentice Hall-Pearson Educación S.A., p. 182.

15 Cfr. Carta Iberoamericana de Gobierno Electrónico (aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado Pucón, Chile, 31 de mayo y 1 de junio de 2007). Este documento tiene como objetivo, entre otros, el de "servir como orientación para el diseño, regulación, implantación, desarrollo, mejora y consolidación de modelos nacionales de Gobierno Electrónico en la gestión pública"; y el Decreto 1151 de 2008. Sobre este texto y otros aspectos del proceso administrativo a través de medios electrónicos véase: Quintero Navas, G. (junio de 2011). Documento GECTI núm. 12 de 2011. Procedimiento administrativo electrónico: aportes de la Ley 1437 de 2011. *Revista de derecho, comunicaciones y nuevas tecnologías*. Faculta de Derecho de la Universidad de los Andes, 5. Recuperado de http://derechoytics.uniandes.edu.co

16 Carta Iberoamericana de Gobierno Electrónico, literal b), "De las finalidades" (numeral 2).

17 Srur, J. (agosto de 2002). E-goverment: el nuevo nombre del buen gobierno. *El Observador*, año 43 (513). Citado por Grecco y Vecchi en la obra señalada en la siguiente nota de pie de página.

18 Grecco, S. y Vecchi, S. (2004). Acciones participativas en el campo de la administración de justicia y tecnologías de información y comunicación (TIC). En *Internet y sistema judicial en América Latina: Reglas de Heredia*, coordinado por Carlos G. Gregorio y Sonia Navarro. Buenos Aires: Ad-Hoc, p. 63.

De haberse aprobado el proyecto de ley mencionado en la introducción los ciudadanos tendrían que acudir obligatoriamente a una Entidad de Certificación Abierta[19] (ECA) para adquirir los servicios de firma digital y certificación digital. Ello implica que una persona debe invertir por lo menos $400 000 anuales para identificarse digitalmente y cada año pagar una suma parecida. En otras palabras, para los ciudadanos la imposición legal de utilizar un medio de identificación digital se convierte en una barrera de entrada a los servicios del gobierno en línea. Barrera que prácticamente sería insuperable en el caso de colombianos(as) que sobreviven heroicamente con un salario mínimo legal mensual. ¿Lo anterior facilitaría las relaciones entre los administrados y la administración?

Normas como la propuesta en 2009 no están pensadas con el fin de acercar el Estado a los ciudadanos y las ciudadanas de escasos recursos económicos sino que están diseñadas para favorecer, entre otras, a las empresas que venden firmas digitales certificadas, como las Entidades de Certificación Abierta (ECA). Ese tipo de iniciativas aleja al ciudadano del Estado y no es consistente con lo planteado por la doctrina cuando afirma que "un ciudadano no tiene por qué ser experto en administración pública, por lo tanto hay que facilitarle la entrada a los servicios de gobierno electrónicos".[20]

La firma digital de las ECA sigue siendo muy costosa para el ciudadano común.[21] Se ha convertido en un artículo de lujo que no tiene cabida en la canasta familiar de millones de hogares. Pese a lo anterior sorprende cómo los proyectos de ley las acogen fácil y ciegamente pensando que es lo único jurídicamente válido en este país. Ha tenido más eco la estrategia publicitaria y comercial de ciertas ECA que las necesidades ciudadanas para maximizar el uso de las TIC en general.

¿Qué relación tiene todo lo anterior con la neutralidad tecnológica? Si se regula imponiendo a los ciudadanos los productos de ciertas empresas estamos frente a una norma subjetivamente tecnológica y no respecto de una neutral tecnológicamente. Veamos.

La ONU (2009), en su estudio sobre el fomento de la confianza en el comercio electrónico recalcó que la "neutralidad tecnológica reviste particular importancia habida cuenta de la rapidez de la innovación tecnológica y contribuye a garantizar que la legislación siga pudiendo dar cabida a las novedades futuras y no resulte anticuada muy pronto [...]".[22] Adicionalmente, la neutralidad tecnológica permite que las organi-

19 Las Entidades de Certificación Abierta (ECA) son aquellas entidades que "ofrecen, al público en general, servicios propios de las entidades de certificación, tales que: a) su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, y b) recibe remuneración" (Cfr. numeral 9 del artículo 3 del Decreto 333 de 2014).

20 Araya Dujisin, R. (2004). Tres perspectivas para observar el gobierno electrónico. En *América Latina Puntogob: casos y tendencias en gobierno electrónico*. Santiago (Chile): FLACSO, p. 35.

21 La primera Entidad de Certificación Abierta (ECA) fue creada en 2002. Durante siete años mantuvo un monopolio sobre los servicios de las entidades de certificación en el país. En 2009 y 2011 se crearon otras dos ECA. Con la incursión de estas últimas existen otras alternativas de precios más bajos por el mismo producto y servicio.

22 Organización de las Naciones Unidas (ONU) (2009). CNUDMI. Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas. Viena, p. 39.

zaciones y las partes utilicen "la tecnología que se ajuste a sus necesidades".[23]

En un artículo del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Universidad de los Andes, se recalcó que las normas que involucren tecnologías sean neutrales porque

> si la ley se casa con una tecnología en particular muy seguramente la norma quedará obsoleta rápidamente. Por eso, la Ley 527 exige algunos requisitos técnicos fundamentales pero no señala la tecnología específica que se deba utilizar. Así las cosas, si la ley requiere que se utilicen tecnologías confiables para garantizar la integridad de un mensaje de datos, el operador puede escoger la tecnología que desee siempre y cuando sea fiable a la luz del estado de la técnica y del momento histórico que se requiera.[24]

Varias razones destacan la importancia de mantener la primacía del principio de la neutralidad tecnológica, a saber:

- Garantiza que las normas perduren en el tiempo y no se esté cambiando permanentemente por cuestiones tecnológicas o por quedar obsoletas frente al cambiante estado del arte tecnológico.

- Permite el uso de todas las tecnologías que cumplan ciertos requisitos para alcanzar ciertos niveles de seguridad y autenticidad. Esto incentiva a que muchos productores de tecnologías participen en el mercado, compitan e innoven.

- Reduce costos tecnológicos a las entidades públicas.

- Impiden que al ciudadano se le trasladen costos muy altos por el uso de las TIC que se impongan mediante ley o actos administrativos.

- Tiene efectos incluyentes frente a los ciudadanos porque pueden acceder a esas tecnologías.

- Evita patrocinar monopolios u oligopolios de proveedores de tecnologías cerrando las puertas del mercado a otros sujetos que pueden ofrecer iguales o mejores tecnologías que logran los mismos fines o efectos que esperamos de las TIC.

Señala Mauro Ríos que

> el concepto de NT[25] reúne una serie de Principios que buscan describir un escenario libre y competitivo entre todas las soluciones técnicamente viables. Garantizando la libertad de optar y elegir de los individuos y las organizaciones, así como la no dependencia tecnológica de la información. La NT es [...] la libertad de los individuos y las organizaciones de optar por la tecnología más apropiada y conveniente a sus necesidades y requerimientos, para su desarrollo, adquisición, uso o comercialización.[26] (Subrayamos)

23 *Ibid.*

24 Remolina Angarita, N. (2006). Aspectos legales del comercio, la contratación y la empresa electrónica. *Revista de derecho, comunicaciones y nuevas tecnologías*, 2, 346.

25 Neutralidad Tecnológica.

26 Rios, M. D. (Enero de 2013). Technological Neutrality and Conceptual Singularity. Disponible en SSRN: http://ssrn.com/abstract=2198887 o en http://dx.doi.org/10.2139/ssrn.2198887

El mismo autor pone de presente los siguientes principios sobre neutralidad tecnológica (NT) que nos parece pertinente enunciar a continuación:

> - Principio 1: **Libertad de oportunidades de toda solución técnicamente viable**, para satisfacer un requerimiento tecnológico del sector público, privado, académico u otro.
>
> - Principio 2: **No dependencia de fabricantes, desarrolladores, proveedores o distribuidores** de productos o servicios tecnológicos.
>
> - Principio 3: Libertad de los individuos de relacionarse con una organización o institución pública o privada, por vías electrónicas, **sin que le sea impuesta, de facto o explícitamente, ningún tipo de tecnología específica**.
>
> - Principio 4: **Neutralidad de las normas** (Leyes, Decretos u otras) que enuncian derechos u obligaciones, **sin que refieran a tecnologías o medios tecnológicos necesarios obligatorios para que se cumplan dichas normas**.
>
> - Principio 5: Normalización de la información en archivos digitales, la que deberá generarse, almacenarse y transmitirse en al menos un formato estándar abierto certificado, sin perjuicio de que pueda hacerse además en otros.[27] (Subrayamos)

Las regulaciones no neutrales son de corta duración y tienden a oxidarse prontamente. Sus efectos son negativos y costosos para el país. Veamos un ejemplo.

La primera experiencia fue la regulación de la factura en la década de los noventa. Esas regulaciones fracasaron, entre otras, por no ser neutrales. La facturación electrónica no se masificó. Esto lo reconoció el legislador una década después cuando expidió la Ley 962 de 2005 y ordenó en el artículo 26 lo siguiente: "Para todos los efectos legales, la factura electrónica podrá expedirse, aceptarse, archivarse y en general llevarse usando cualquier tipo de tecnología disponible, siempre y cuando se cumplan todos los requisitos legales establecidos y la respectiva tecnología que garantice su autenticidad e integridad desde su expedición y durante todo el tiempo de su conservación". (Subrayamos)

Nótese cómo la Ley 962 no dice cuáles productos se deben usar (como sí lo hacía el proyecto de ley citado en la introducción) sino que menciona los requisitos que deben reunir los productos para expedir, aceptar y archivar facturas electrónicas. Esto es diferente y es neutral desde la perspectiva regulatoria. ¿Por qué imponer los productos de algunas empresas y no permitir que las organizaciones recurran a otras alternativas de identificación electrónica?

Con la Ley 1341 de 2009[28] se introdujo la neutralidad tecnológica como parte de los principios

27 Rios, *op. cit.*

28 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones". Según el artículo 1 de la ley, la misma tiene como objeto determinar "el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información".

orientadores de dicha norma en los siguientes términos:

> El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.[29]

Recientemente, algunas regulaciones están rescatando el principio de la neutralidad tecnológica. Un ejemplo a seguir es el artículo 2 del Decreto 2364 de 2012 sobre firmas electrónicas. Dicho artículo se titula "neutralidad tecnológica e igualdad de tratamiento de las tecnologías para la firma electrónica" y establece que ninguna parte de ese 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 artículo 7 de la Ley 527 de 1999". En esa misma línea se redactó el Decreto 2609 de 2012 (arts. 5, literal q, y 25).

En adición a lo anterior, mediante el Decreto 2693 de 2012[30] se actualizaron y ampliaron los lineamientos generales de la Estrategia de Gobierno en Línea para "garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado más eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad".[31] En dicho decreto se incorporó la neutralidad tecnológica como fundamento de dicha estrategia y para ello se utilizó la definición de Neutralidad Tecnológica del numeral 6 del artículo 2 de la Ley 1341 de 2009.[32]

Mediante el Decreto 333 de 2014 se derogó totalmente el Decreto 1747 de 2000, y con ello se eliminó un beneficio regulatorio no neutral que el Decreto 1747 de 2000 solo otorgaba a las Entidades de Certificación Abierta (ECA), dejando sin piso jurídico la labor de las Entidades de Certificación Cerrada[33] (ECC). Según el artículo 15 del derogado decreto, si un ciudadano deseaba utilizar una firma digital de una entidad de certificación, ese tipo de firma solo era válido si se utilizaba un certificado emitido por una ECA.[34]

29 Cfr. numeral 6 del artículo 2 de la Ley 1341 de 2009.

30 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones".

31 Cfr. artículo 1 del Decreto 2693 de 2012.

32 En efecto, el artículo 3 del Decreto 2693 de 2012 dice lo siguiente: "El Estado garantiza la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, emplear contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible".

33 Las Entidades de Certificación Cerrada son aquellas entidades que ofrecen "servicios propios de las entidades de certificación solo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello" (Cfr. numeral 8 del artículo 3 del Decreto 333 de 2014).

34 Cfr. numeral 1 del artículo 15 del Decreto 1747 de 2000 (derogado por el Decreto 333 de 2014).

Finalmente es relevante mencionar que en noviembre de 2013 el Gobierno nacional publicó el proyecto de decreto "por el cual se establecen lineamientos generales en las entidades públicas en el uso de medios electrónicos, se reglamentan el capítulo IV de la Ley 1437 de 2011, y se dictan otras disposiciones".[35] Dicha iniciativa resultará crucial en la gestión pública a través de medios electrónicos. Infortunadamente, la misma no consagra el principio de neutralidad tecnológica, el cual resulta importante consagrarlo en este tipo de regulación que será referente en todo el Estado y que fija políticas cruciales para el futuro del país. Por eso sugerimos al Gobierno incorporar el siguiente numeral en el artículo 3 del proyecto de decreto:

> n) Principio de neutralidad tecnológica: Las entidades públicas y los particulares podrán utilizar cualquier tipo de tecnología disponible para comunicarse o realizar cualquier actividad de gestión documental, siempre y cuando la respectiva tecnología garantice autenticidad e integridad de los mensajes de datos desde su expedición y durante todo el tiempo de su conservación.
>
> Los ciudadanos están en libertad de relacionarse con una organización o institución pública o privada, por vías electrónicas, sin que le sea impuesta, de facto o explícitamente, ningún tipo de tecnología específica.[36]

III. AUTENTICACIÓN Y ALTERNATIVAS DE IDENTIFICACIÓN ELECTRÓNICA EN LA GESTIÓN ESTATAL

Uno de los retos para abordar en el derecho administrativo y los medios electrónicos consiste en establecer la identidad de quienes participan en las actuaciones administrativas mediante dichos mecanismos, y en establecer la autenticidad de los documentos electrónicos.

Señala el artículo 244 de la Ley 1564 de 2012 (nuevo Código General del Proceso) que un documento es auténtico "cuando existe certeza sobre la persona que lo ha elaborado, manuscrito, firmado, o cuando exista certeza respecto de la persona a quien se atribuya el documento". Esta definición replica la existente en el Código de Procedimiento Civil[37] y es, en lo fundamental, coincidente con la del Código de Procedimiento Penal.[38] Unas y otras tienen en común la firma[39] como factor determinante de la autenticidad de los documentos.

El sector privado ha sido pionero en el uso de las TIC en sus actividades. Sus buenas prácticas han sido replicadas en el sector público. Por

35 Publicado en la página http://www.programa.gobiernoenlinea.gov.co/foros.shtml?apc=gdx;x;x;x1-&x=81676

36 Esta propuesta fue sugerida por el autor y comunicada al Gobierno nacional, vía electrónica, mediante e-mail del 18 de noviembre de 2013.

37 Artículo 252.

38 Artículo 425 del Código de Procedimiento Penal. "Documento auténtico. Salvo prueba en contrario, se tendrá como auténtico el documento cuando se tiene conocimiento cierto sobre la persona que lo ha elaborado, manuscrito, mecanografiado, impreso, firmado o producido por algún otro procedimiento". A pesar de su importancia omitiremos tratar lo atinente a los aspectos probatorios de los documentos electrónicos, los cuales analizaremos en otro texto.

39 La firma tradicional del contexto análogo (no electrónico) es definida en el artículo 826 del Código de Comercio con el nombre "signo o símbolo empleado como medio de identificación personal".

eso, cuando hablamos de algunas instituciones del comercio electrónico, las mismas también tienen aplicación en la gestión estatal a través de medios electrónicos.

Así las cosas, resulta apropiado traer a colación ciertos aspectos del estudio realizado por la ONU a que nos referimos anteriormente sobre el "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas". Dice el estudio, entre otras, lo siguiente:

> • 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, 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.
>
> • 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.
>
> • 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.[40]

Esta última precisión hace que la adquisición de la firma digital de las ECA genere dependencia o se convierta en un servicio necesario para poder verificar la firma cuando caduca el certificado digital o se revoca la clave pública correspondiente. Esta dependencia significa más costos que deben asumir las organizaciones y las personas.

A. ¿Firmas digitales o firmas electrónicas?

La firma digital y la firma electrónica son alternativas de identificación en el contexto digital. La segunda se ha considerado como el género de las formas de identificación electrónica porque se refiere a cualquier medio electrónico para identificar las personas, mientras que la primera se cataloga como una especie de la primera, en la medida en que no se trata de cualquier medio sino de una forma de identificación basada en el uso de una clave privada para generar la firma de un mensaje de datos, y una clave pública para corroborar o verificar que un docu-

40 Organización de las Naciones Unidas (2009). Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas.

mento fue firmado con la clave privada asignada a una persona.[41]

La firma digital está definida en la Ley 527 de 1999[42] como

un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.[43]

La tecnología de la firma digital supone que un texto (mensaje de datos) se suscribe con una clave privada[44] y es verificado con una clave pública,[45] que permite establecer si, de una parte, el mismo fue creado con la clave privada del firmante.

Los dos tipos de firma son jurídicamente válidos pero se han generado afirmaciones sobre la firma digital que no se derivan de los que dice la norma. Así, por ejemplo, el administrador de una entidad de certificación abierta (ECA) afirmó en 2009 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" y 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".[46] Haciendo eco acrítico y "cuasiliteral" de lo anterior, el CIO del Consultorio de Tecnología y Derecho de Adalid Abogados concluyó en 2012 lo siguiente: "Para que una firma digital se entienda válidamente emitida en Colombia, se requiere de la intervención de un tercero de confianza denominado 'entidad de certificación'"[47] (subrayamos).

41 Las definiciones de clave privada y clave pública se encuentran en los numerales 5 y 6 del artículo 3 del Decreto 333 de 2014.

42 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

43 Cfr. literal c del artículo 2 de la Ley 517 de 1999. "El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:

1. Es única a la persona que la usa; 2. Es susceptible de ser verificada; 3. Está bajo el control exclusivo de la persona que la usa; 4. Está ligada a la información o mensaje, de tal manera que si estos son cambiados, la firma digital es invalidada; 5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional" (parágrafo del artículo 28 de la Ley 527).

44 La clave privada es definida en el numeral 5 del artículo 3 del Decreto 333 de 2014 como "valor o valores numéricos que utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos".

45 La clave pública es definida en el numeral 6 del artículo 3 del Decreto 333 de 2014 como "valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador".

46 Cfr. Rincón Cárdenas, E. (2009). Discusiones alrededor de la firma digital. *Ámbito Jurídico*, (281), p. 13.

47 Cfr. *Ámbito Jurídico*, página 6 de la edición 356 (15-28 de octubre de 2012). Andrés Guzmán, CIO de Adalid Corp., en la página 15 de la edición 362 manifestó que de una lectura integral de las normas se puede concluir su afirmación.

No compartimos la argumentación ni la conclusión de dicha persona porque es notorio que Guzmán pretende aplicar como regla general una excepción. En efecto, él transcribió el artículo 15 del Decreto 1747 de 2000 pero le dio un alcance sustancialmente diferente al texto del mismo. Veamos: "Artículo 15. Uso del certificado digital. Cuando quiera que un suscriptor firme digitalmente un mensaje de datos con su clave privada, y la respalde mediante un certificado digital, se darán por satisfechos los atributos exigidos para una firma digital, en el parágrafo del artículo 28 de la Ley 527 de 1999, si: 1. El certificado fue emitido por una entidad de certificación abierta autorizada para ello […]" (subrayo).

No es cierto que el legislador colombiano estableció la firma digital como único equivalente de la firma manuscrita. Esa conclusión (*firma digital como único equivalente de firma*) desconoce el artículo 7 de la Ley 527 de 1999. Tampoco es veraz aseverar que la validez de una firma digital[48] 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 con la clave pública),
- la digital certificada por una Entidad de Certificación Cerrada (ECC), y
- la digital certificada por una ECA

El artículo 28 de la 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). La verificación se puede realizar con la clave pública[49] 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[50] (EC), 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. Solo 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.

Es alarmante que no solo existan disposiciones que imponen el uso de la firma digital,[51] sino la notoria cruzada por parte de algunos

Ese artículo solo es aplicable cuando alguien utiliza un certificado para respaldar una firma digital, pero no establece la obligatoriedad de que la firma digital sea certificada. Ese es el error de Guzmán y por eso es incorrecta su afirmación de la página 6 de la edición 356 de 2012 de *Ámbito Jurídico*: "Para que una firma digital se entienda válidamente emitida en Colombia, se requiere de la intervención de un tercero de confianza denominado 'entidad de certificación'".

48 Nótese que la firma digital está basada en la tecnología PKI. Esta tecnología comprende un modelo de arquitectura que incluye varios componentes. Uno de ellos es la Certification Authority (CA). Esta CA no es la entidad de certificación de que trata la Ley 527 de 1999, aunque tecnológicamente puedan cumplir funciones similares, pues es la misma tecnología. La función principal de las CA es emitir certificados, los cuales son generados automáticamente; en otras palabras, son autogestionados y forman parte del modelo de infraestructura PKI. Para ello no se requiere las EC de la Ley 527 de 1999. Ver: 1) Kiran S., Lareau, P. y Lloyd, S. (noviembre de 2002). PKI basics. A technical perspective, Shashi Kiran, Patricia Lareau y Steve Lloyd, en *PKI Note*, PKI Fórum, p. 5. Disponible en http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf; 2) La arquitectura PKI. Disponible en http://www.webtaller.com/maletin/articulos/arquitectura_pki.php

49 Recuérdese que a la luz del numeral 6 del artículo 3 del Decreto 333 de 2014, 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".

50 En efecto, según el numeral 1 del artículo 3 del Decreto 333 de 2014, el "certificado en relación con las firmas" 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 este".

51 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 Superintendencia de Industria y Comercio y 100-004 de la Superintendencia de Sociedades.

empresarios, asesores y consultores para minar la legislación colombiana de disposiciones que obliguen a utilizar la firma digital de las Entidades de Certificación Abierta (ECA). Un ejemplo que corrobora lo anterior es el proyecto de ley con que iniciamos este texto.

No es conveniente para el país vender las firmas digitales de las entidades de certificación imponiendo su uso vía leyes, decretos, circulares, etcétera. Tampoco es sensato que algunos funcionarios públicos crean que lo único válido y útil es la firma digital. La firma digital no es mala, lo malo es imponerla a las malas, cerrando las puertas a otras alternativas de identificación electrónica a costa del bolsillo de los colombianos.

*B. **Firma electrónica***

Mediante el Decreto 2364[52] del 22 de noviembre de 2012 el Gobierno nacional reglamentó la firma electrónica[53] del artículo 7 de la Ley 527 de 1999. Con este se deja en manos del país una alternativa de identificación electrónica diferente a la firma digital.

Con dicho decreto desaparece cualquier duda sobre la validez jurídica de la firma electrónica al expresar en el artículo 5 que "la firma electrónica tendrá la misma validez y efectos jurídicos que la firma", siempre y cuando la misma sea confiable y apropiada para los fines con los cuales se generó o comunicó un mensaje de datos. El decreto es aplicable en el sector público y privado de manera que debería considerarse en todas las actividades englobadas bajo el término *gobierno en línea*.

La norma en comento incorpora explícitamente los "acuerdos sobre uso de mecanismos de firma electrónica" (acuerdos EDI) mediante los cuales el Estado y las empresas pueden pactar con la ciudadanía y sus clientes la forma como se identificarán los unos y los otros cuando realicen actividades a través del uso de las TIC. El artículo 7 presume, salvo prueba en contrario, "que los mecanismos o técnicas de identificación personal o autenticación electrónica, según el caso, que acuerden utilizar las partes mediante acuerdo, cumplen los requisitos de firma electrónica".

Estos acuerdos han sido acogidos explícitamente por el Gobierno nacional para efectos de impuestos. En efecto, mediante el Decreto 2926 de 2013[54] se facultó al director general de Impuestos y Aduanas Nacionales para que defina las personas naturales que podrán utili-

52 Algunos antecedentes del decreto pueden consultarse en: Remolina Angarita, N. (junio de 2010). Documento GECTI núm. 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—? *Revista de derecho, comunicaciones y nuevas tecnologías* de la Facultad de Derecho de la Universidad de los Andes, 4. Recuperado de https://derechoytics.uniandes.edu.co/. Se puede consultar en:

https://derechoytics.uniandes.edu.co/index.php?option=com_content&view=article&id=59%3Adocumento-gecti-nro-10-ipensar-en-las-necesidades-del-pais-o-mantener-a-ultranza-un-statu-quo-para-lafirma-digital-de-las-entidades-de-certificacion-abierta-eca-&lang=es

53 Definida como: "Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente" (numeral 3 del artículo 1 del Decreto 2364 de 2012).

54 Por el cual se reglamenta el artículo 19 de la Ley 1607 de 2012 y el artículo 579-2 del Estatuto Tributario.

zar la firma electrónica[55] "para el cumplimiento de las obligaciones tributarias sustanciales y formales a través de los servicios informáticos electrónicos".[56] Pero el uso de dicha firma queda sujeto a lo que establece el artículo 2 de dicho decreto, a saber: "Previo al uso de la firma electrónica, sin uso de mecanismo digital, el usuario deberá suscribir un documento de acuerdo, en el cual se definirán las reglas que regirán las comunicaciones electrónicas confiables entre el usuario y la UAE, Dirección de Impuestos y Aduanas Nacionales (DIAN)". Ese "documento de acuerdo" es una especie de contrato o acuerdo EDI utilizado desde hace varias décadas en el mundo.

La seguridad no la otorga la ley por obra de magia. Esta dependerá, como mínimo, de dos cosas: (i) El producto o tecnología que se utilice como firma —grado de seguridad tecnológica intrínseca— y (ii) la diligencia, custodia y cuidado que tenga el usuario de los datos de creación de la firma electrónica. El firmante debe cumplir las obligaciones señaladas en el artículo 6 del decreto pues no puede olvidarse que en ciertas ocasiones las fallas de seguridad obedecen a factores humanos.

Los acuerdos EDI pueden ser la herramienta jurídica para sacar adelante todo el plan de justicia digital y las gestiones de gobierno electrónico. Ya han mostrado ser útiles en grandes proyectos mundiales de desmaterialización e inmaterialización.[57]

En síntesis, ahora todas las organizaciones cuentan con otra alternativa de identificación electrónica. Como tal, en cada caso es necesario establecer si es conveniente o no utilizarla. Es esencial que quien suministre mecanismos de firma electrónica asegure que los mismos tengan altos niveles de seguridad que permitan, entre otros, mitigar cualquier cuestionamiento técnico sobre la autenticidad e integridad de los mensajes de datos.

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 un asunto 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?

Finalmente, el decreto es consistente con el principio de neutralidad tecnológica[58] en la me-

55 De conformidad con el artículo 3 del Decreto 2926 de 2013, "la firma electrónica a que se refiere el presente decreto tendrá la misma validez y efectos jurídicos de la firma autógrafa".

56 Cfr. artículo 1 del Decreto 2926 de 2013.

57 La desmaterialización supone que un documento se creó físicamente y luego se reemplaza por mecanismos electrónicos. La inmaterialización se refiere a documentos que nacen electrónicamente, como lo son los mensajes de datos.

58 El artículo 2 ordena que "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 artículo 7 de la Ley 527 de 1999".

dida en que no dice cuál producto debe utilizarse como firma electrónica sino que deja al Estado, las empresas y los ciudadanos definir el mecanismo más confiable y apropiado.

Lamentablemente, normas posteriores al Decreto 2364 ya han dado reversa al tema y han regresado al emporio de la firma digital. El nuevo Estatuto de Registro de Instrumentos Públicos (Ley 1579 de 2012), por ejemplo, volvió a imponer la firma digital en los artículos 9 (radicador de documentos), 14 (para la radicación exige firma digital de las notarías, despachos judiciales o entidades públicas) y 15 (radicación de documento o título vía electrónica en las notarías, despachos judiciales o entidades estatales).

Esto pone en evidencia la falta de una política coherente del Estado sobre identificación electrónica. Estamos en un mundo digital, global e hiperconectado en el que nos seguimos identificando con cédulas de ciudadanía plásticas.

Es urgente que el Estado repiense y actúe teniendo en cuenta la neutralidad tecnológica en sus decisiones.

IV. ¿NEUTRALIDAD TECNOLÓGICA EN LAS REGULACIONES RESPECTO DE ORGANIZACIONES PRIVADAS QUE CUMPLEN FUNCIONES PÚBLICAS?

El Decreto 805 del 24 de abril de 2013[59] reglamentó, entre otras, la inscripción en el registro mercantil de los libros de registro de socios o accionistas y los de actas de asamblea y juntas de socios. Allí se definen los libros de comercio en medios electrónicos como aquellos en forma de mensaje de datos en los cuales los comerciantes registran sus operaciones mercantiles. Para su registro, las Cámaras de Comercio deberán contar con plataformas electrónicas o sistemas de información apropiados para prestar adecuadamente este servicio "registral virtual".

Dichos libros pueden llevarse en archivos electrónicos y para su inscripción se deben cumplir, entre otros, los siguientes requisitos: a) Inclusión de un mecanismo de firma digital o electrónica a elección del comerciante en el archivo electrónico enviado para registro; b) Firma digital o electrónica por parte de la Cámara de Comercio competente.

Aunque existe libertad de firmar electrónica o digitalmente, el comerciante no tendrá opción de escoger el tipo de firma digital que prefiera porque el artículo 5 dice que cuando este firme digitalmente "deberá hacerlo mediante uso de un certificado digital emitido por una entidad de certificación digital autorizada o acreditada en Colombia". En otras palabras, el comerciante que opte por utilizar este tipo de identificación solo podrá emplear la firma digital certificada, acudiendo inevitablemente a las entidades de certificación.

El citado artículo reitera que en Colombia es jurídicamente válida la firma digital con o sin la intervención de las entidades de certificación. Regulatoriamente no son lo mismo la firma digital y los certificados digitales. Estos últimos son

59 "Por el cual se reglamenta el artículo 173 del Decreto 019 de 2012".

"mensajes de datos firmados por una entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor, y contiene la clave pública de este" (núm. 1 del art. 3 del Decreto 333 de 2014). Dicho certificado debe contener lo que indica el artículo 35 de la Ley 527 de 1999.

Las regulaciones que imponen la obligación de acudir a las entidades de certificación crean nuevos costos que deben asumir los ciudadanos y las organizaciones. Por eso es necesario evaluar la creación de una entidad de certificación pública que ofrezca gratuitamente sus servicios. Si ello se hace se favorece al ciudadano y se le dan herramientas para que acuda masivamente a utilizar todos los servicios del gobierno electrónico.

Si no se crea la entidad de certificación pública, los ciudadanos seguirán asumiendo los costos de las normas que los obligan a acudir a las entidades de certificación privadas.

V. ESTRATEGIAS DE POLÍTICAS PÚBLICAS PARA LA IDENTIFICACIÓN ELECTRÓNICA CIUDADANA

De manera preliminar sugerimos las siguientes dos opciones para fomentar una actividad estatal electrónica e incluyente desde la perspectiva de los mecanismos de identificación electrónica:

En primer lugar, el Estado debería proveer de manera gratuita[60] un sistema de identificación electrónica a cada ciudadano. Se trataría de incorporar un sistema único de identificación electrónica que sea económico, práctico, confiable y seguro para todas y todos. En el caso de España, por ejemplo, el Real Decreto 1553/2005[61] de 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.[62]

Lo ideal sería que todos tuviésemos una cédula de ciudadanía electrónica como medio de identificación de las colombianas y los colombianos en el contexto digital. Sobre esto ya existen esfuerzos en otros países que deberían replicarse en Colombia.

En segundo lugar, el Estado podría convertirse en una ECA. Actualmente la DIAN y el Banco de la República son Entidades de Certificación Cerrada (ECC), pero solo para efectos de las relaciones de dichas entidades y los ciudadanos. Si el ministro de Hacienda pregunta a todas las entidades públicas cuánto dinero invierten en firmas digitales, automáticamente se dará cuenta de que se están despilfarrando recursos en ese tema y en cuestiones de tecnología. Por eso, sería bueno que el Estado asuma el rol de una entidad de certificación para todos.

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

61 "Por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica".

62 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, de 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".

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 el ciudadano no es experto en tecnologías).

VI. CONCLUSIONES

La regulación sobre TIC debe ser neutral tecnológicamente. No debe recetar productos específicos sino establecer los requisitos mínimos que deben cumplir los medios tecnológicos para garantizar seguridad, autenticidad e integridad.

Para alcanzar una inmersión masiva de las TIC en todas las actividades se debe evitar que las mismas encarezcan 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 de las tecnologías.

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. Piénsese, por ejemplo, en el caso del proyecto de ley a que nos referimos en la introducción de este texto. Si se le impone al ciudadano el uso de las firmas digitales de las ECA para iniciar una actuación administrativa, muchos no podrían acceder a los beneficios del gobierno electrónico y serían excluidos del mismo. 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.

En las iniciativas regulatorias sobre TIC es necesario garantizar la neutralidad tecnológica. Si el Estado no es capaz de garantizar la neutralidad tecnológica en los mecanismos de identificación electrónica, debería crear una entidad de certificación pública y abierta para todos(as), de manera que la firma digital no sea un mecanismo de identificación excluyente (por su costo).

Las regulaciones no neutrales tecnológicamente pueden ser excluyentes porque afectan a personas que no tienen cómo pagar los altos costos que implica, por ejemplo, recurrir a una entidad de certificación privada. Si esto es así, dicho tipo de normas serían inconsistentes con los claros mandatos del artículo 53[63] de la Ley 1437 de 2011 en la medida en que no garantizarían, entre otras, la igualdad de acceso de los ciudadanos a la administración porque los citados costos serían un elemento de exclusión de las personas de pocos recursos económicos, es decir, a la mayoría de las colombianas y los colombianos.

63 El artículo 53 ordena lo siguiente: "Procedimientos y trámites administrativos a través de medios electrónicos. Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.

"En cuanto sean compatibles con la naturaleza de los procedimientos administrativos, se aplicarán las disposiciones de la Ley 527 de 1999 y las normas que la sustituyan, adicionen o modifiquen" (artículo 53 de la Ley 1437 de 2011, "por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo).

Referencias

Araya Dujisin, R. (2004). Tres perspectivas para observar el gobierno electrónico. En *America Latina Puntogob: casos y tendencias en gobierno electrónico*. Santiago de Chile (Chile): FLACSO.

Cerf, V. (1995). Computer networking: global infrastructure for the 21st century. Computing Research Association (CRA). Recuperado de http://www.cs.washington.edu/homes/lazowska/cra/networks.html

Grecco, S. y Vecchi, S. (2004). Acciones participativas en el campo de la administración de justicia y tecnologías de información y comunicación (TIC). En *Internet y sistema judicial en América Latina: Reglas de Heredia*, coord. Carlos G. Gregorio y Sonia Navarro. Buenos Aires: Ad-Hoc.

Montañés, P. y Olier E. (2006). *Corporate governance intelligence: desarrollando la corporación en web*. Madrid: Prentice Hall-Pearson Educación S.A.

Organización de las Naciones Unidas (ONU) 2009. Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas. Viena.

Quintero Navas, G. A. (2011). Procedimiento administrativo electrónico: aportes de la Ley 1437 de 2011. En *Derecho & TIC 10.0*. Bogotá: Ediciones Uniandes-Editorial Temis.

Remolina Angarita, N. (2006). Aspectos legales del comercio, la contratación y la empresa electrónica. *Revista de derecho, comunicaciones y nuevas tecnologías*, 2.

— (2010). Documento GECTI núm. 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—? *Revista de derecho, comunicaciones y nuevas tecnologías*, 4. Bogotá: Facultad de Derecho de la Universidad de los Andes.

Rios, M. D. (2013). Technological Neutrality and Conceptual Singularity. Recuperado de http://ssrn.com/abstract=2198887 o http://dx.doi.org/10.2139/ssrn.2198887

Shashi Kiran, P. L. y Lloyd S. (2002). PKI basics. A technical perspective. En *PKI Note, PKI Fórum*. Recuperado de http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf

Srur, J. (2002). E-goverment: El nuevo nombre del buen gobierno. *El observador*, año 43, (513).

Schmidt, E. y Cohen, J. (2014). *The new digital age. Transforming nations, businesses, and our lives*. Estados Unidos: Vintage books.

Teruel Lozano, M. (2013). Libertades y derechos de las personas en Internet: retos en materia de reconocimiento y la tutela de los derechos fundamentales ante el paradigma tecnológico de la sociedad del siglo XXI. En *Desafíos*

para los derechos de la persona ante el siglo XXI: Internet y nuevas tecnologías. Aranzadi (España): Thomson Reuters.

Otros documentos y columnas de opinión

Carta Iberoamericana de Gobierno Electrónico. Aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado Pucón, Chile, 31 de mayo y 1 de junio de 2007.

Internet World Stats (2012). Internet Usage Statistics. The Internet Big Picture. World Internet Users and Population Stats. Junio 30 de 2012. Recuperado de http://www.internetworldstats.com/stats.htm.

Guzmán, A. (octubre de 2012). Las diferencias entre firma electrónica y firma digital. Consultorio de Tecnología y Derecho. Sección patrocinada por Adalid. *Ámbito Jurídico*.

Remolina Angarita, N. (2009). Imprecisiones y despropósitos de algunas propuestas de regulación. *Ámbito Jurídico* (278).

Rincón Cárdenas, E. (2009). Discusiones alrededor de la firma digital. *Ámbito Jurídico* (281).

Unión Internacional de Telecomunicaciones (2012). Medición de la Sociedad de la Información 2012. Sinopsis. Recuperado de http://www.itu.int/ITU-D/ict/publications/idi/material/2012/MIS2012-ExecSum-S.pdf