Universidad del Rosario

COLOMBIA FINTECH

TRANSFORMACIONES EN EL COMERCIO ELECTRÓNICO

Un balance de los 20 años de la Ley 527 de 1999

EDITORES ACADÉMICOS:

Yira López Castro
Erick Rincón Cárdenas

TRANSFORMACIONES EN EL COMERCIO ELECTRÓNICO

Un balance de los 20 años de la Ley 527 de 1999

Patrocinado por:

Editores

UNIVERSIDAD DEL ROSARIO
COLOMBIA FINTECH

Patrocinadores

EXPERIAN
MASTERCARD

Editores académicos:

Erick Rincón Cárdenas
Yira López Castro

Autores:

Carlos Andrés Atuesta
Mario Fernando Ávila Cristancho
David Díaz
Pedro Novoa Serrano
Daniel Peña Valenzuela
Juan Sebastián Peredo
Rodrigo Puyo Vasco
Germán Realpe Delgado
Erick Rincón Cárdenas
Sergio Rodríguez Azuero
María Alejandra Soler Rangel
Daniel Villarroel
Andrés Felipe Umaña Chaux

.Puntoaparte bookvertising
www.puntoaparte.com.co

Director de arte

Andrés Álvarez
Maria Paula Leiva

Diagramación

Julieta Cruz
Angélica Villate

Coordinación Editorial

Andrés Barragán

ISBN (PDF)

978-958-784-371-2

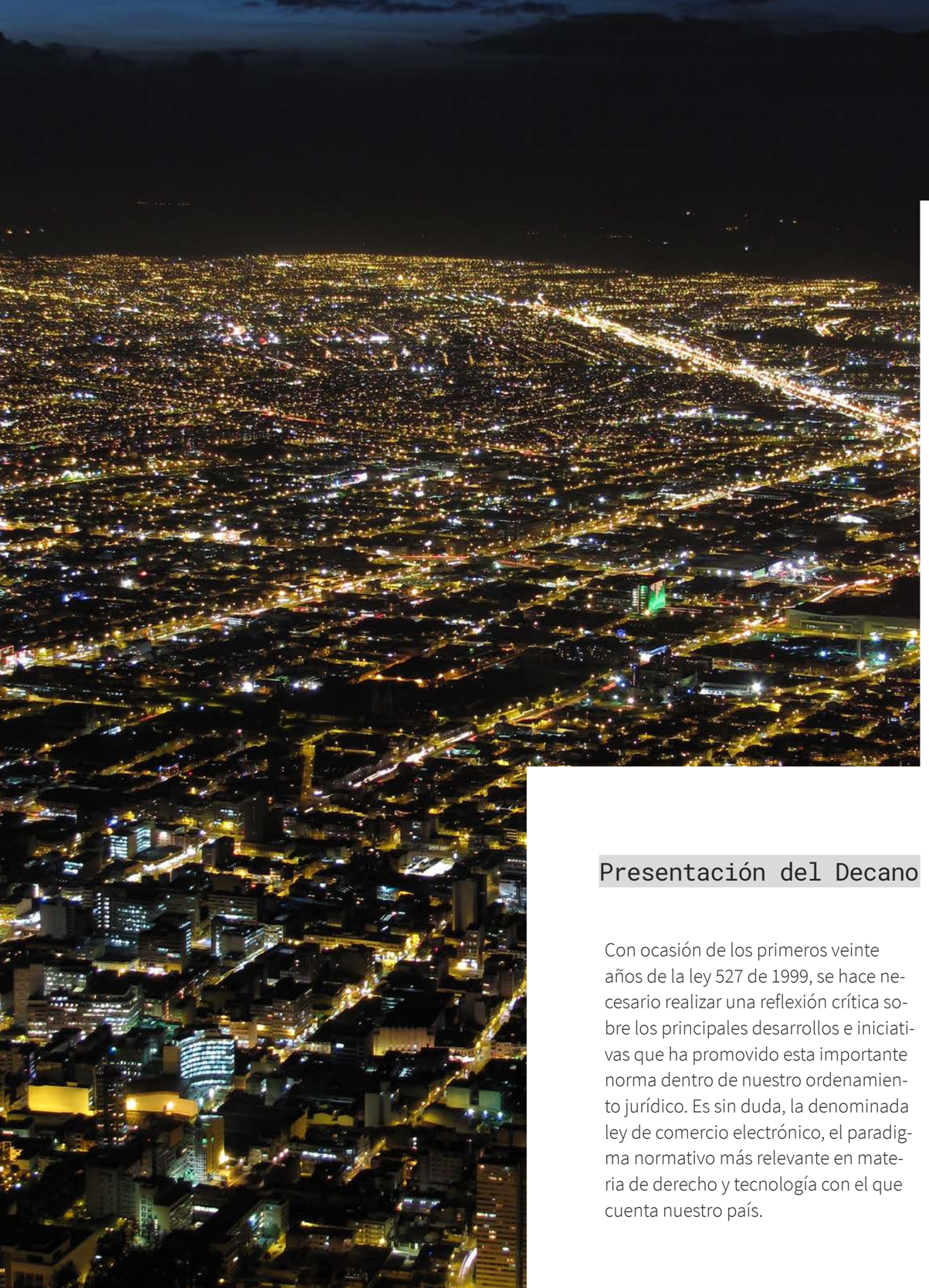
Presentación del Rector

Es para la Universidad del Rosario motivo de orgullo y satisfacción hacer parte de esta iniciativa académica que recoge las reflexiones de destacados profesionales del derecho alrededor de un evento de gran importancia para nuestro país, como es la celebración de los veinte primeros años de la Ley de Comercio Electrónico en Colombia.
En la Universidad del Rosario y en desarrollo de la Ruta UR-2025, nuestra bitácora estratégica de los siguientes seis años, estamos convencidos de que sólo a través de la innovación, la tecnología y el emprendimiento, nuestra sociedad tendrá una oportunidad para el desarrollo sostenido hacia el futuro en la mejora permanente de las condiciones de nuestros estudiantes, profesionales y en general de toda la sociedad.
En ese sentido, la Universidad ha contemplado dentro de sus diferentes estrategias el despliegue de importantes inversiones en el ámbito del uso de medios electrónicos, la conformación de nuevos laboratorios de formación, la constitución de grupos de investigación y estudio alrededor de la tecnología, y también se encuentra desarrollando programas académicos en diseño, arquitectura, así como en ingenierías. Todo esto para contribuir desde diferentes campos a los ya tradicionales en nuestra Universidad, al fomento del pensamiento creativo.

Nos unimos entonces a los esfuerzos del gobierno nacional por desarrollar industrias creativas. La economía naranja también es economía digital. El emprendimiento digital hace parte hoy de una destacadísima oportunidad ocupacional de nuestros estudiantes. Nuestro determinado compromiso es propociar escenarios de aprendizaje y formación para los estudiantes en estas materias, para que puedan enfrentarse a esa realidad que les impone un uso cada vez más intensivo de las tecnologías de la información.
El desarrollo legislativo que acá se celebra, ha sido un hito histórico en la modernización de de las instituciones públicas y privadas, fomentando el uso de las herramientas tecnológicas como insumo importante en todo tipo de actividad social y económica.
Aplaudimos el esfuerzo de los organizadores de esta iniciativa y nos ponemos a disposición para trabajar de manera conjunta en todos los retos que impone la virtualización en todos los ámbitos y actividades.

Gracias.

Alejandro Cheyne García
Rector
Universidad del Rosario



Presentación del Decano

Con ocasión de los primeros veinte años de la ley 527 de 1999, se hace necesario realizar una reflexión crítica sobre los principales desarrollos e iniciativas que ha promovido esta importante norma dentro de nuestro ordenamiento jurídico. Es sin duda, la denominada ley de comercio electrónico, el paradigma normativo más relevante en materia de derecho y tecnología con el que cuenta nuestro país.

Hasta la fecha diversas actuaciones y trámites, tanto de la administración pública, como del sector privado, se han virtualizado como consecuencia de la aplicación de principios jurídicos de gran relevancia, como son: la equivalencia funcional de los mensajes de datos, la neutralidad tecnológica, la inalterabilidad del derecho preexistente, la buena fe, y la libertad contractual. Principios que tienen transcendencia interpretativa en la aplicación de las tecnologías en Colombia. Tanto el Comercio como el Gobierno Electrónico han crecido y tienen un marco de referencia cada vez más estable y maduro, muestra de lo cual es precisamente el recientemente expedido decreto número 2106 del 22 de noviembre de 2.019. Esta Ley que es recipiendaria de la tradición jurídica de la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil, y que deviene directamente de la ley modelo sobre la misma temática del año 2006, constituye la principal manifestación de la modernización de los instrumentos jurídicos para el reconocimiento de la información electrónica que se gestó a partir de los albores del siglo enque nos encontramos. Se trata de una norma transversal en nuestro ordenamiento, de alcance probatorio que se despliega en todas las disciplinas del Derecho. La Ley en comento, más que proponer incentivos para el desarrollo de actividades por medios electrónicos, constituye una base fundamental para la validez jurídica y probatoria de los mensajes de datos en el desarrollo de todo tipo de disciplinas… De allí su importancia.

Se trata de un instrumento jurídico idóneo que ha habilitado el uso de las tecnologías en todo tipo de campos, ya que le debemos buena parte de los procesos de desmaterialización y virtualización en nuestra sociedad.
En este texto, que no podía tener otro tipo de desarrollo que una versión electrónica o digital, se presenta, de una parte, una revisión de lo que han sido los últimos veinte años en la aplicación de diversas temáticas jurídicas, como la contratación electrónica, la propiedad intelectual por medios electrónicos, la protección de datos personales, el valor jurídico y probatorio de la información electrónica. Por otra parte, el texto analiza lo que podrán ser los siguientes veinte años de desarrollo de tan importante disposición, en temáticas como la inteligencia artificial, el blockchain, el desarrollo de la tecnología financiera, la robótica y por supuesto también la analítica de datos, así como la computación cognitiva.
Nos acompañan en este texto conmemorativo alguno de los profesionales más destacados en el ejercicio profesional de este novedoso campo. A ellos el agradecimiento por participar en esta obra que pretende ser un referente de construcción colectiva sobre las diferentes iniciativas en el uso de medios electrónicos que ha tenido nuestro país. Se trata de una reflexión práctica desde el quehacer empresarial.

José Alberto Gaitán Martínez
Decano
Facultad de Jurisprudencia
Universidad del Rosario

CONTENIDO

I PARTE

II PARTE

I PARTE

APLICACIÓN DE LA LEY 527: 20 AÑOS DE DESARROLLO

VALIDEZ JURÍDICA DE LA INFORMACIÓN DIGITAL

LEGAL VALIDITY OF DIGITAL INFORMATION

Andrés Felipe Umaña Chaux
María Alejandra Soler Rangel

Resumen:

Este artículo repasa la aproximación de la Ley 527 de 1999 en su objetivo de otorgar validez jurídica a la información que reposa en medios digitales. El sustrato a esta validez jurídica es en esencia un asunto de confianza; este artículo analiza los criterios fundamentales que incorporó la ley para generar esta confianza, así como las novedades y algunas de las dificultades y discusiones que se han presentado en los últimos años, e introduce algunos de los futuros aspectos que necesariamente tendrán incidencia en la aplicación de la ley.

Palabras clave: derecho informático; mensajes de datos; firma electrónica; comercio electrónico.

Abstract:

This article reviews the approach taken by Law 527 of 1999 in granting legal validity to digital information. The substrate of this legal validity is a matter of trust. This article analyzes the fundamental criteria that this law incorporated to create trust, as well as the developments and some of the difficulties and discussions that has been presented over the last few years. It also introduces some of the future aspects that will impact the application of the law.

Key words: information law; data messages; e-sign; e-commerce.

Introducción: un problema de confianza

Entre el siglo XIX y mediados del XX, durante el paso de la moneda metálica al papel moneda, darle valor económico a un papel motivó la desconfianza en su uso. Para contrarrestarla, se implementó el patrón oro, un sistema que asignaba al papel moneda un valor equivalente en dicho metal, el cual fue desmontado tiempo después cuando el uso del papel moneda se afianzó. Como éste, nuestra historia jurídica posee muchos ejemplos de construcción de Nación en los que la desconfianza cultural ha impactado la implementación normativa. La adopción de la Ley 527 de 1999 (en adelante la "Ley 527"), que reguló expresamente la validez de la información en medios digitales1, no fue ajena al impacto de esa desconfianza cultural.

Aún hoy, tras 20 años de su expedición, la Ley 527 es el principal instrumento jurídico que el legislador colombiano ha desarrollado para superar esta desconfianza cultural. En este artículo abordaremos los principales elementos desarrollados en esta ley para cumplir con este objetivo. Sin embargo, aún enfrentamos dificultades en su implementación, a causa de las dudas que se alzan respecto de la validez de la información digital, al punto que nuestros más altos tribunales y entidades del Estado todavía tienen que conceptuar periódicamente respecto de la validez sustancial2 y procesal3 de los mensajes de datos4, en algunos casos ofreciendo interpretaciones disonantes. Según cifras de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones y el Observatorio de Comercio Electrónico de la Cámara Colombiana de Comercio Electrónico, tan sólo el 19% de los colombianos realiza compras y pagos electrónicamente5, dando cuenta del camino por recorrer en la masificación de las tecnologías de la información en el país.

1. La definición del Diccionario Jurídico de la Real Academia Española señala que la validez es la "Cualidad de lo que, por no estar afectado de causa alguna de nulidad, es válido y puede producir efectos jurídicos que le son propios", efectos que se predican tanto del ámbito procesal como sustancial.

2. Ver Concepto 08SE2019120300000023705 sobre la validez de los contratos laborales virtuales. Emitido por el Ministerio de Trabajo en junio de 2019. Allí se reitera lo que hace 20 años la Ley pretendió superar, esto es dar valor sustancial a los mensajes y sus efectos jurídicos no fueran denegados por el solo hecho de constar en un medio electrónico. También en el ámbito de la contratación estatal se ha requerido conceptuar sobre la materia, pues en las entidades estatales aún no se han afianzado en el uso de las nuevas tecnologías y la digitalización de sus procesos impactando el uso de los mensajes de datos en el marco de las relaciones sustanciales entre estas y terceros.

3. Las altas Cortes discutieron desde muy temprano la validez procesal de los mensajes de datos, centrando las discusiones de manera intensa en la admisibilidad o no de la copia impresa de un mensaje de datos en el marco de una contienda procesal, así como en la validez del documento no firmado. Respecto de lo anterior pueden consultarse los siguientes pronunciamientos:

- De la Corte Constitucional: Sentencia C-266 de 200, M.P. ; Sentencia C-662 de 2004, M.P. ; Sentencia C- 604 de 2016, M.P. Luis Ernesto Vargas Silva.
- De la Corte Suprema de Justicia: Sentencia de 4 de septiembre de 2000, Sala de Casación Civil, radicado: 5565; Sentencia del 1 de agosto de 2007, Sala Casación Civil, Expediente No. T -11001-02-03-000-2007-01087-00; Sentencia del 16 de diciembre de 2010, Sala de Casación Civil, Expediente No.11001 3110 005 2004 01074 01; Sentencia del 30 de julio de 2014, Sala De Casación Laboral. Radicación No. 58949; entre otras.
- Del Consejo de Estado: Sentencia del 5 de septiembre de 2013, Sección Cuarta, Rad. 11001-03-27-000-2011-00002-00(18635), C.P. Carmen Teresa Ortiz; Sentencia del 13 de noviembre de 2014, Sección Primera, Rad. 13001-23-31-000-2007-00814-01, C.P. Marco Antonio Velilla Moreno; Sentencia del 4 de diciembre de 2014, Sección Quinta, C.P. Alberto Yepes Barreiro, Rad. 11001-03-28-000-2014-00132-00; entre otras.

La discusión parece ya superada con el pronunciamiento del Consejo de Estado bajo el cual la copia impresa será tenida en cuenta en el proceso como válida, aunque el documento no se allega en la forma en la que fue creado, lo anterior toda vez que las partes de un proceso tendrán los mecanismos de tacha de falsedad o de repudio (sentencia del Consejo de Estado, 13 de diciembre de 2017. M.P. Stella Conto.

4. En este artículo usamos indistintamente las expresiones información digital, información electrónica y mensajes de datos. Si bien podrían hacerse algunas distinciones sobre estas, las mismas no son relevantes para los aspectos tratados en este artículo.

5. Ver: https://www.observatorioecommerce.com.co/wp-content/uploads/2019/03/estudio-consumo-ecommerce-colombia-observatorio-2019.pdf

01

La información electrónica a la luz de la Ley527: disposiciones y principios

Con la masificación de las tecnologías de la información y el advenimiento del comercio electrónico en la década de los noventa crecieron globalmente las inquietudes sobre el valor jurídico de la información que reposaba en medios electrónicos. Las legislaciones nacionales no tenían una regulación general para el comercio electrónico y usaban términos usualmente asociados a transacciones análogas, tales como "manuscrito", "original" o documentos "firmados"[6]. La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), consciente de las dificultades que esta obsolescencia jurídica podría traer para el crecimiento del comercio electrónico, desarrolló una "Ley Modelo de Comercio Electrónico" en 1996 (la "Ley Modelo de 1996"), que serviría de referencia para que los distintos países desarrollaran su propia legislación. Su objetivo principal no era otro que permitir el uso general de los medios electrónicos en las transacciones comerciales y jurídicas.
En Colombia la situación no era muy diferente. Si bien existían normas que hubieran permitido a los jueces y autoridades administrativas dar valor jurídico a los medios electrónicos[7], también había gran incertidumbre entre los empresarios y en general entre las autoridades sobre el uso y el alcance que les podían dar a dichos medios.

La Ley 527 de 1999, también denominada Ley de Comercio Electrónico, fue la respuesta directa a esta preocupación y al llamado de la CNUDMI. Esta perdura como la ley más importante para las tecnologías de la información porque, siguiendo de cerca la Ley Modelo de 1996[8], estableció principios generales para interpretar la totalidad del ordenamiento jurídico colombiano, los cuales aún hoy guían a todas las autoridades en el uso y análisis de los medios electrónicos.

6. CNUDMI, "Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996 - con el nuevo artículo 5 aprobado en 1998", página 16.

7. Por ejemplo, el artículo 95 de la Ley 270 de 1996, la Ley Estatutaria de la Administración de Justicia, estableció que "***Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y telemáticos, para el cumplimiento de sus funciones. Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales***". Este mismo artículo ordena al Consejo Superior de la Judicatura a "***propender por [sic] la incorporación de tecnología de avanzada al servicio de la administración de justicia***". Un artículo pionero que, como veremos más adelante, todavía sigue pendiente de ejecución. Por otra parte, el artículo 175 del derogado Código de Procedimiento Civil consagraba el principio de libertad de medios de prueba: "***Sirven como pruebas, la declaración de parte, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez. El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejantes o según su prudente juicio***".

8. Pero también, como veremos más adelante, separándose en importantes aspectos

1.1 La validez general de la información electrónica

El primer principio o regla fundamental que introduce la Ley 527 es la validez general de los mensajes de datos. En el artículo 5 se establece que *"no se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensajes de datos"*.

No es común que una norma, en lugar de otorgar efectos jurídicos, establezca la prohibición de negar efectos a una información o a un mecanismo particular para su procesamiento[9]. Sin embargo, bajo esta redacción inusual se revistió de valor jurídico, tanto sustancial como procesal, a los mensajes de datos. Esta fórmula surge del propósito de CNUDMI de garantizar un espectro amplio que diera cabida a nuevos desarrollos tecnológicos al servicio de las relaciones comerciales.

En el mismo sentido del artículo 5 se manifestó el artículo 14, a cuyo tenor se establecía que *"[e]n la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos"*. El artículo 15 refuerza lo anterior, refiriéndose esta vez al entorno o medio en el que se manifiesta la voluntad en el marco de una relación contractual u obligacional así: *"[e]n las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos"*.

9. Por ejemplo, la Cámara de Comercio Internacional y Reino Unido propusieron que se reconociera igual valor jurídico a algunas cláusulas incorporadas por vía de remisión dentro de un mensaje de datos. Ver documentos: Cámara de Comercio Internacional (A/CN.9/WG.IV/WP.65) y del Reino Unido de Gran Bretaña e Irlanda del Norte (A/CN.9/WG.IV/WP.66), en conjunto: A/CN.9/407, párrs. 100 a 105.

Ya en el ámbito eminentemente procesal, los artículos 10[10] y 11 dictan las pautas mínimas para la admisión y validez de los mensajes de datos en el marco de un proceso judicial o administrativo. Así, el artículo 10[11] señala que no se negará validez probatoria a una información electrónica: (i) por el hecho de estar en forma de mensaje de datos, o (ii) por no haberse presentado en su forma original. Por su parte, sobre el artículo 11, que será tratado en detalle líneas más adelante, basta decir que para la valoración probatoria de los mensajes de datos se reconocen las reglas de la sana crítica y los criterios generales de valoración de pruebas, y se enuncian algunos criterios que ampliaremos en otra sección del texto.

Además de los artículos transcritos, la Ley 527 incluyó capítulos que se ocupaban específicamente de la validez de la firma electrónica (género)[12] y de la firma digital (especie)[13], tema de particular relevancia en lo que respecta a las discusiones que se alzaron sobre la Ley 527 por su estrecho vínculo con la atribución y autenticidad de los documentos. Pese a lo anterior, este texto no se ocupará en detalle en la evolución de los conceptos de firma electrónica y digital, por cuanto otro capítulo del libro se dedicará enteramente al desarrollo de ese tema.

Así las cosas, el conjunto de normas enunciadas introdujo por primera vez en Colombia un marco jurídico transversal que amparaba el uso de los mensajes de datos e imponía algunos parámetros para darle fuerza legal. Sin embargo, sobre la validez procesal de los mensajes de datos, las altas Cortes han tenido posiciones divergentes, las cuales revisaremos a lo largo de este texto.

10. La primera discusión que tuvo lugar respecto de la validez jurídica de los mensajes de datos fue abordada por la Corte Constitucional en la Sentencia C-662 del 2000, en la que se resolvía una acción pública de inconstitucionalidad respecto de la Ley 527. Además de cuestionar la constitucionalidad de dotar a terceros diferentes de los notarios de la función de fe pública, otro cargo de la demanda cuestionaba la constitucionalidad de los artículos 9, 10, 11, 12, 13, 14, 15 y 28 de la Ley 527 por cuanto dar valor o validez probatoria a los mensajes de datos por vía de la ley desconocía el procedimiento especial de Ley Estatutaria que debía regir para la discusión legislativa, dado que la demandante alegaba que dicho cambio constituía una modificación al sistema de administración de justicia. Este alegato fue desestimado por la Corte Constitucional manteniendo la vigencia de la validez probatoria de la información electrónica.

11. El artículo 10 completo dice lo siguiente: "ARTICULO 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS. ***Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.***

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el solo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original".

12. La Ley 527 no habla expresamente de "firma electrónica", pero el Decreto 2364 de 2012, según expresamos más adelante, interpreta como "firmas electrónicas" a aquellas que cumplen con el equivalente funcional del artículo 7.

13. A partir del artículo 28 de la ley.

1.2 La neutralidad tecnológica

El segundo principio capital de la Ley 527 que soporta la validez general de los mensajes de datos es el que, siguiendo la denominación establecida en la Ley 1341 de 2009 (la "Ley 1341"), llamaremos principio de neutralidad tecnológica. Ni la Ley 1341 ni la Ley 527 definen este principio, pero la primera sí lo enuncia:

> *6. Neutralidad Tecnológica. 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.*

Por neutralidad tecnológica entendemos el derecho de los particulares a adoptar —y el deber de los servidores públicos a permitir— la "libre adopción" de tecnologías[14]. Es difícil considerar que una ley es neutral en su integridad; lo que sí podemos es afirmar es que la Ley 527 consagra muchas disposiciones que desarrollan el principio de neutralidad tecnológica, tal y como este se definió en la Ley 1341. Veamos algunos ejemplos:

- La definición de "mensaje de datos", cobija a todo tipo de información ***"generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares".*** Si consideramos lo "electrónico" como "la física, ingeniería la tecnología y sus aplicaciones que permiten manejar la emisión, flujo y control de electrones", resulta fácil concluir que toda la información procesada por las tecnologías de lo que hoy denominamos "Cuarta Revolución Industrial" debe ser considerada como mensajes de datos bajo legislación colombiana. Si bien, siendo puristas, podría afirmarse que la Ley 527 excluye otro tipo de tecnologías, como por ejemplo las "biológicas", lo cierto es que estas tecnologías alternativas para el procesamiento de información quedarían cobijadas bajo el concepto de "similares" incluido en la misma definición.

- Los artículos 6, 7, 8, 9, 12, entre otros, desarrollan los equivalentes funcionales de escrito, firma, original y conservación, sin prescribir el uso de una tecnología particular. Los particulares y los servidores públicos pueden usar cualquier tecnología disponible de procesamiento de información para escribir, firmar, almacenar o en general manejar información, cumpliendo con las condiciones establecidas en la norma, pero escogiendo las tecnologías que pueden utilizar para ello.

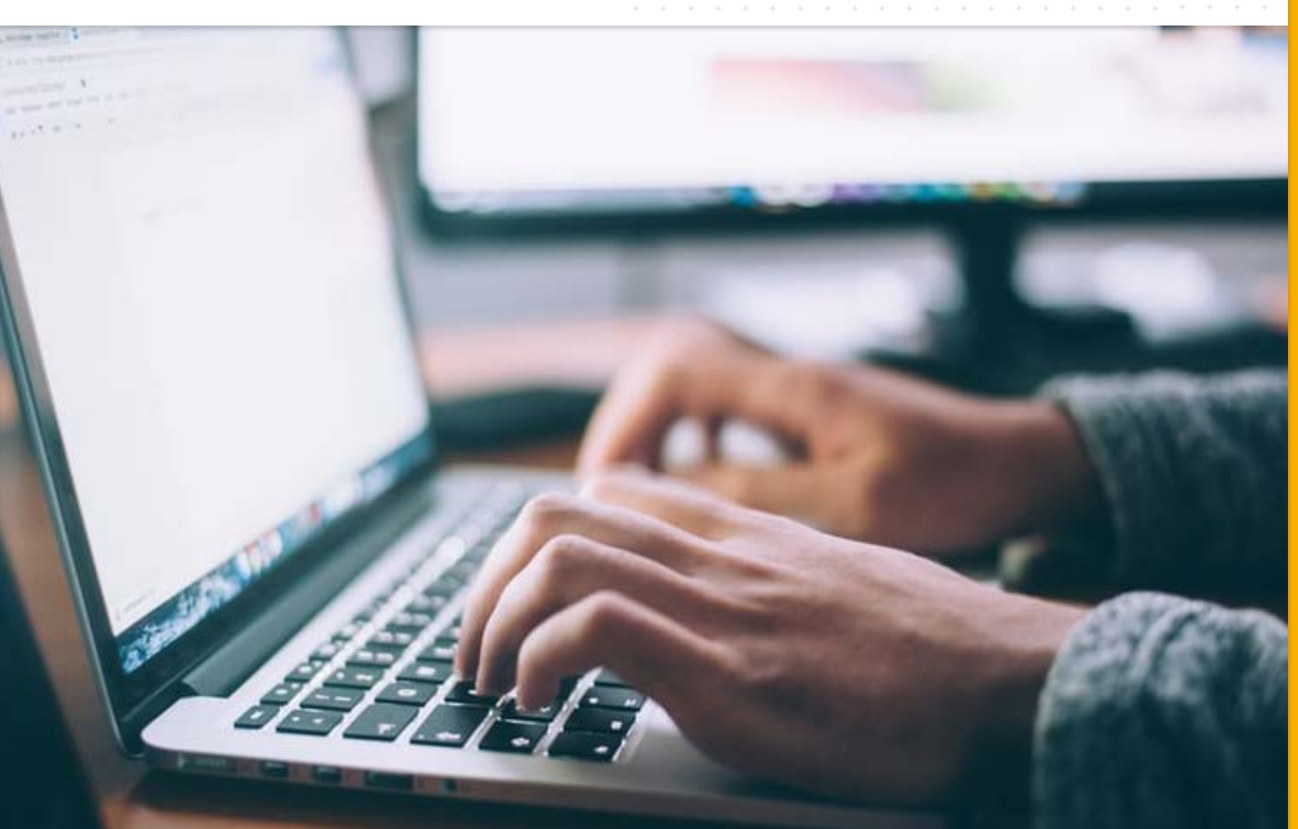
14. Existe todavía alguna discusión sobre si la Parte III de la Ley 527 es verdaderamente neutral. No afirmamos aquí que la Ley 527 de 1999 sea neutral en todos sus artículos, sino que sus artículos generales, particularmente los de la Parte II, sí permiten el uso de cualquier tecnología para su cumplimiento. Más adelante hacemos algunos comentarios sobre este asunto.

- El artículo 2 del Decreto 2364 de 2012, reglamentario de la Ley 527 e interpretando por tanto su sentido, consagró explícitamente el principio de neutralidad tecnológica respecto de los métodos de firma electrónica e incluyó varios criterios para determinar la admisibilidad de una firma de esa naturaleza.

- La Parte III, que se refiere a las firmas digitales y a las entidades de certificación y que suele esgrimirse como una razón para negar el carácter neutral de la Ley 527, no prescribe una tecnología, al menos en el sentido restringido de la palabra. Impone, sí, una serie de procedimientos, como el uso de un tercero de confianza para funciones de autenticidad e integridad, y supone en ocasiones el uso de un sistema criptográfico específico (criptografía asimétrica), para generar algunas obligaciones e imponer una serie de efectos jurídicos. Pero exigir estos procedimientos o incluso suponer estas técnicas criptográficas no exige un protocolo, dispositivo o software propietario particular para cumplir con dichas obligaciones o generar dichos efectos jurídicos, ni significa que dichos procedimientos no se puedan cumplir a través de distintas "tecnologías"[15].

A lo largo de este texto volveremos sobre este asunto, pero baste por ahora concluir que, al menos parcialmente y en muchos de sus preceptos, la Ley 527 desarrolla o aplica el principio de neutralidad tecnológica.

15. Sobre la necesidad de terceros de confianza para respaldar las firmas digitales y el crecimiento reciente de sistemas distribuidos nos pronunciamos más adelante. Sobre el concepto en sí de firmas digitales y si ellas mismas son un desarrollo o una excepción a la neutralidad tecnológica, puede verse el artículo sobre firmas en el libro en el que se publica este artículo.



1.3 El carácter contextual y relativo de la validez jurídica de la información electrónica

Hemos dicho que, de acuerdo con el artículo 5, no se le pueden negar efectos o valor jurídico a los mensajes de datos por el solo hecho de estar en un medio electrónico. ***Sin embargo, esto no significa que todos los mensajes de datos tengan efectos jurídicos, o que tengan el mismo valor o los mismos efectos***. El artículo 11, que regula el valor probatorio o validez procesal de la información electrónica, da pie para entender lo que denominaremos el "carácter contextual y relativo" de los mensajes de datos. Reza el artículo 11:

> *Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, 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, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.*

Este artículo no ha tenido en nuestro ordenamiento el desarrollo que merece. Como se puede apreciar, está ligando el valor probatorio de los mensajes de datos a tres criterios específicos de confiabilidad: (i) confiabilidad en la forma en que se haya generado, archivado o comunicado el mensaje; (ii) confiabilidad en la manera como se haya conservado la integridad de la información, y (iii) (confiabilidad en) la forma en que se identifique al iniciador del mensaje.

A diferencia del papel, tecnología que a grandes rasgos almacena la información con los mismos niveles de autenticidad, integridad y seguridad, los mensajes de datos pueden diferir sustancialmente en la manera como se manejan estos aspectos. Un mensaje de datos puede estar en un formato tal que pueda ser alterado sin que quede un registro de las modificaciones y sin dejar ninguna constancia de la persona que las ha realizado, pero también puede almacenarse en un sistema que, usando métodos de autenticación y técnicas criptográficas, permita identificar al iniciador de dicho mensaje con precisión y dejar un registro de cualquier modificación que se le realice. A esto nos referimos cuando hablamos del carácter ***relativo*** de la validez jurídica de la información electrónica: la validez jurídico-procesal de la información electrónica no es absoluta, sino que depende de la confiabilidad de los tres criterios mencionados por la norma en el artículo 11.

Estos tres criterios de confiabilidad dependen, a su vez, de los múltiples factores técnicos que rodeen al mensaje de datos. Un mensaje de este tipo, por regla general, no está ni puede analizarse aisladamente; es generado, comunicado, almacenado o transmitido a través de un conjunto de elementos físicos, lógicos, de personas y de procesos, que solemos denominar genéricamente como un "sistema de in-

formación”[16]. A esto nos referimos cuando afirmamos que la validez jurídica de la información electrónica tiene un carácter *contextual*: un mensaje de datos en sí mismo no tiene validez jurídica, o esta no puede determinarse ***ex ante***; su validez jurídica depende de la confiabilidad del sistema de información del que hace parte. También los metadatos resultan relevantes a fin de determinar el carácter contextual de los mensajes de datos.

Repasemos brevemente cada uno de estos dos criterios. “La forma en que se identifique a su iniciador” parece referirse a las cuestiones relacionadas con lo que hoy se denomina como “identidad digital” o “identificación electrónica” en la legislación comparada[17,18]. La firma manuscrita, aquella que por años permitió la identificación y la generación de certeza sobre el autor de un documento, da paso en el contexto digital a un conjunto amplio de tecnologías que permiten dicha identificación. Es importante anotar, sin embargo, que “identificación” o “identidad” y “autenticidad” no siempre se refieren a los mismos conceptos; en muchas ocasiones “identidad” se utiliza en un sentido más amplio para referirse al rasgo único e individual de todas las personas, mientras que la “autenticidad” se remite al acto o al hecho de tener certeza sobre la identidad de una persona en un contexto específico o de validar la identidad de esa persona en un sistema de información determinado.

¿Cuál método de identificación resulta apropiado para identificar al iniciador de un mensaje de datos? La Ley 527 no nos da una respuesta. Sin embargo, atendiendo nuevamente a su carácter internacional[19], podemos recurrir a la Guía para la Incorporación, que en su Considerando 58 establece, comentando el equivalente funcional de firma, algunos criterios no exhaustivos para determinar cuándo un método de firma es apropiado para una determinada transacción, criterios que podemos extrapolar para analizar de manera general la confiabilidad de los mensajes de datos en los términos del artículo 11:

> *Para determinar si el método seleccionado con arreglo al párrafo 1) es apropiado, pueden tenerse en cuenta, entre otros, los siguientes factores jurídicos, técnicos y comerciales: 1) la perfección técnica del equipo utilizado por cada una de las partes; 2) la naturaleza de su actividad comercial; 3) la frecuencia de sus relaciones comerciales; 4) el tipo y la magnitud de la operación; 5) la función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable; 6) la capacidad de los sistemas de comunicación; 7) la observancia de los procedimientos de autenticación establecidos por intermediarios; 8) la gama de procedimientos de autenticación que ofrecen los intermediarios; 9) la observancia de los usos y prácticas comerciales; 10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados; 11) la importancia y el valor de la información contenida en el mensaje de datos; 12) la disponibilidad de otros métodos de identificación y el costo de su aplicación; 13) el grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos; y 14) cualquier otro factor pertinente.*

Los otros dos criterios, “la confiabilidad en la forma en que se haya generado, archivado o comunicado el mensaje” y “confiabilidad en la manera como se haya conservado la integridad de la información” se refieren a lo que la misma Ley 527 denomina en su artículo 9 como integridad:

> *Para efectos del artículo anterior [que consagra el equivalente funcional de original], se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso”.*

Este artículo establece otra importante innovación jurídica que ha sido en la mayoría de las ocasiones ignorada. El concepto de original de los medios físicos está ligado usualmente a la primera versión o al momento de creación de un documento. El documento “original” es aquel que fue el primero en crearse, oponiéndose al concepto de “copia”, el cual persiste en el artículo 246 del Código General del Proceso[20], mientras que el artículo 9 de la Ley 527 rompe con él y crea atinadamente un concepto distinto de original para la información digital. A diferencia de la información en un medio análogo, la información digital se crea, se transmite y se almacena creando una copia cada vez que se interactúa con ella. No existe en realidad un “original”, una primera versión creada de un documento que luego se transmita o que el iniciador posea. Por esto, entre otras cosas, se habla de “iniciador”. Cada una de estas copias es exactamente igual a la anterior en cuanto a su contenido. Es por esto que el artículo 9 le da el mismo valor jurídico a la totalidad de las copias. Apenas hoy por vía jurisprudencial se ve reflejada y acogida tal innovación cuando los tribunales admiten la copia impresa como mecanismo de reproducción de ese primer mensaje creado en un entorno digital y señala mecanismos procesales como el repudio o la tacha de falsedad para atacar la veracidad de dichas copias.

16. Un sistema de información puede caracterizarse como un conjunto de hardware, software, datos, personas y procesos con los que se recolectan, almacenan, organizan y distribuyen datos y se transforman en información e incluso luego se convierten en conocimiento. Los mensajes de datos, en su sentido jurídico, representan uno de los componentes de los sistemas de información. Para una descripción pedagógica de lo que es un sistema de información, pueden consultarse los textos de Dave Bourgeois y David T. Bourgeois disponibles en este enlace: https://bus206.pressbooks.com/chapter/chapter-1/.

17. El Reglamento 910 de 2014 de la Unión Europea define la identificación electrónica en el numeral 1 del artículo 3 como *“el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica”*. Dicho reglamento se encuentra disponible en este enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

18. El artículo 244 del Código General del Proceso considera un documento 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”.*

19. El artículo 3 permite utilizar su carácter internacional como criterio de interpretación de su texto.

20. *“Artículo 246. Valor probatorio de las copias. Las copias tendrán el mismo valor probatorio del original, salvo cuando por disposición legal sea necesaria la presentación del original o de una determinada copia. Sin perjuicio de la presunción de autenticidad, la parte contra quien se aduzca copia de un documento podrá solicitar su cotejo con el original, o a falta de este con una copia expedida con anterioridad a aquella. El cotejo se efectuará mediante exhibición dentro de la audiencia correspondiente”.*

1.4 El principio del equivalente funcional

No existe una definición de lo que se conoce como el equivalente funcional, y la Ley 527 no menciona este concepto. Sin embargo, este es tal vez uno de los principios más importantes para entender el tratamiento que la Ley 527 y el ordenamiento jurídico colombiano les dan a los mensajes de datos. Ante la disyuntiva de adaptar el régimen probatorio existente a la realidad de los medios electrónicos o crear un nuevo régimen probatorio independiente para estos, el Legislador colombiano, siguiendo la tendencia internacional, optó por la primera opción. El principio del equivalente funcional es el mecanismo por el que se aplica el régimen probatorio existente a los medios digitales.

Parafraseando a la guía de la Ley Modelo de 1996, podemos enunciar este principio así:

Si un medio digital tiene los mismos objetivos y cumple las mismas funciones que las que una norma jurídica asigna a un medio físico o análogo de manejo de información, dicho medio digital tendrá los mismos efectos jurídicos que el medio análogo al que reemplaza[21].

La mejor manera de entender este principio es analizando su aplicación práctica. Las cuatro ejemplares aplicaciones del principio del equivalente funcional en la Ley 527 las encontramos en los artículos 6, 7, 8 y 12, que consagran los equivalentes de escrito, firma, original y conservación, respectivamente. La guía de la Ley Modelo de 1996 nos indica que estos artículos deben leerse en su conjunto y como una especie de "escala probatoria", de menor a mayor grado, para poder entender verdaderamente su significado. Sigamos, pues, este orden en nuestro análisis.

El artículo 6 establece que un mensaje de datos satisfará el requisito de escrito ***"si la información que este contiene es accesible para su posterior consulta"***. Si un medio digital permite esta consulta posterior de la información que declara y representa, tendrá efectos jurídicos "equivalentes" al documento escrito. Esto, que parece obvio, no lo es si se tiene en cuenta que el acceso a la información digital está mediado por dispositivos electrónicos que se hacen obsoletos con facilidad. A diferencia del papel, que nos permite ver la información declarada o representada en él sin la mediación de otro dispositivo y sin importar si el documento tiene, literalmente, miles de años, un medio digital puede "perder" su función de permitir el acceso a la información rápidamente. Piénsese que, si la información está en un cierto formato electrónico que ha caído en desuso, o para el que se necesita un dispositivo que ya no se encuentra en el mercado, esta probablemente y, para efectos prácticos, no podrá ser aportada a un proceso judicial como prueba o tendrá sendas dificultades para serlo.

De otro lado, el artículo 7 establece el equivalente funcional de fir ma así:

Artículo 7.º firma. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;

b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.[...]

Nótese que el artículo 7 hace expresa referencia a los criterios de autenticidad e integridad del artículo 11, mientras que el artículo 6 los ignora[22].

Después de los menospreciados artículos 5 y 11, el artículo 7 es uno de los más novedosos e importantes de la ley. Por el objeto de este artículo no nos podemos extender sobre él; no obstante, dos comentarios vienen muy a lugar.

El primero es que la Ley 527 fue innovadora en asignar expresamente dos funciones primordiales a la firma: (i) "identificar al iniciador" de un mensaje de datos, y (ii) "indicar que el contenido cuenta con su aprobación [el iniciador]". La primera función, que llamaremos de "identificación",

21. El Considerando 15 de la Guía de la Ley Modelo de 1996 establece: *"La Ley Modelo se basa en el reconocimiento de que los requisitos legales que prescriben el empleo de la documentación tradicional con soporte de papel constituyen el principal obstáculo para el desarrollo de medios modernos de comunicación. En la preparación de la Ley Modelo se estudió la posibilidad de abordar los impedimentos al empleo del comercio electrónico creados por esos requisitos ampliando el alcance de conceptos como los de 'escrito', 'firma' y 'original' con miras a dar entrada al empleo de técnicas basadas en la informática"*.

22. Un escrito al parecer no necesita ser auténtico e íntegro para ser considerado como tal, lo que parece coincidir con la definición de documento que consagra el Código General del Proceso, al establecer en el artículo 243 que son documentos *"[…] los escritos… y, en general, todo objeto mueble que tenga carácter representativo o declarativo"*, sin hacer referencia a la autenticidad de estos, y en cierta medida se alinea con el artículo 252 del mismo estatuto, que permite la valoración de acuerdo con la sana crítica de los documentos rotos o alterados.

se asocia directamente con la necesidad procesal de que los documentos aportados a un proceso judicial sean "auténticos", es decir, que se tenga certeza de la persona a quien se pueden "atribuir"[23]. La segunda, que llamaremos de "integridad", consiste en poder asociar el contenido de un mensaje de datos con su iniciador, de tal manera que este no puedo desconocerlo o "repudiarlo". Ni el artículo 826 del Código de Comercio, ni el antiguo Código de Procedimiento Civil, ni el actual Código General del Proceso hacen expresa referencia a una función de integridad para la firma, y esta incluso pasó desapercibida en la definición incluida en el Decreto 2364 de 2012[24], reglamentario de la Ley 527.

El segundo es que el literal b) crea una importante diferencia entre los medios análogos y los medios digitales. Para determinar si una firma electrónica cumple con sus funciones, debemos analizar el método de firma utilizado y establecer si fue (i) confiable, y (ii) apropiado para el propósito del mensaje. Esto no ocurre en los medios análogos. Nuestro método de firma por excelencia, la firma manuscrita o autógrafa, es el mismo, independiente del tipo de documento que estamos firmando y del "propósito" para el que estamos firmando. Las firmas análogas no tienen grados de confiabilidad distintos según su propósito, pero este es el caso de las firmas electrónicas. Como mencionamos atrás, este es otro ejemplo del carácter contextual y relativo del valor probatorio de los medios digitales; su confiabilidad debe analizarse con base en el criterio de la sana crítica.

De acuerdo con el artículo 1 del Decreto 2364, las firmas que cumplen con los requisitos del artículo 7 se denominan de manera genérica "firmas electrónicas" y, siguiendo el principio de neutralidad tecnológica, no están asociadas a una tecnología particular. Empero, el artículo 28 de la Ley 527 establece una presunción para lo que denomina "firma digital":

Artículo 28. Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

La firma digital se define en el literal c) del artículo 2 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.

Finalmente, el artículo 28, en el parágrafo, establece una equivalencia entre la firma digital y la firma manuscrita[25] cuando se cumple, entre otras, con las reglamentaciones del Gobierno Nacional[26].

Como mencionamos atrás, se discute si la presunción consagrada en el artículo 28 de la Ley 527, en la cual se indica que "Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo", constituye o no una excepción al principio de neutralidad tecnológica. Tal interpretación tuvo cabida por vía jurisprudencial para denegar la validez de ciertos mensajes de datos[27], desdibujando la preponderancia de la autonomía de la voluntad como uno de los ejes centrales en la construcción de la ley, así como la existencia de otros medios que permiten acreditar la atribución de un documento.

En el ámbito institucional, el Consejo Superior de la Judicatura, mediante Acuerdo N.o PSAA06-3334 de 2006, se decantó en su momento por imponer un tipo de firma especial para dotar de valor procesal a un documento electrónico incorporado al proceso así:

los actos de comunicación procesal que se realicen por correo electrónico, así como los documentos que puedan ser presentados como mensajes de datos en los términos de la ley procesal, tendrán el mismo valor probatorio que la información que conste por escrito, siempre y cuando el firmante utilice una firma electrónica avalada por una entidad de certificación autorizada conforme a la Ley[28].

23. Cabe tener en cuenta en este punto la distinción que hace López Blanco sobre el requisito de autenticidad: *"La autenticidad es un requisito que debe estar cumplido para que el documento pueda ser apreciado y valorado por el juez en lo que intrínsicamente contenga, pero es asunto ajeno a su valor probatorio. En verdad, la autenticidad no tiene nada que ver con el efecto o poder demostrativo del documento"* (López Blanco, 2017, p. 457).

24. El numeral 3 del artículo 1 de este Decreto no menciona la integridad: *"3) Firma electrónica: 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".*

25. *"PARÁGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla 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 éstos son cambiados, la firma digital es invalidada.5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional"*.

26. Así lo ha reconocido la Sección Tercera del Consejo de Estado en sentencia del 13 de diciembre de 2017, proceso con número de radicación 25000-23-26-000-2000-00082-01(36321): *"En estas condiciones, la Sala considera que las copias impresas de correos electrónicos, no tachadas de falsas por la persona a quien se oponen, cuando permitan una mínima individualización, esto es, cuando ofrezcan certeza sobre quien los ha elaborado, a quien se ha dirigido y cuándo, pueden ser valoradas, en tanto la individualización da lugar a asociar el contenido, lo que implica, a la luz del principio de buena fe, aceptar su autenticidad. Eso sí, de ello no se sigue que el medio de prueba resulte* per se *idóneo para la demostración que se pretende, pues su valoración estará sujeto a valoración conjunta y en especial de las reglas de la sana crítica".*

27. Ver Sentencia del Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Quinta, 4 de diciembre de 2014. C. P. Alberto Yepes Barreiro. Rad. 11001-03-28-000-2014-00132-00. Allí se excluye un material probatorio por no contar con la firma digital en los correos electrónicos allegados como prueba en un proceso sobre nulidad electoral. Esta sentencia será abordada en mayor detalle en el apartado de discusiones jurisprudenciales sobre la validez de los documentos electrónicos.Consejo Superior de la Judicatura. Acuerdo N.o PSAA06-3334 de 2006.

28. Consejo Superior de la Judicatura. Acuerdo N.o PSAA06-3334 de 2006.

¿Cómo se interpretan estas normas a la luz del actual Código General del Proceso?

El artículo 244 considera 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". El mismo artículo, en su inciso segundo, establece una presunción de autenticidad para todos los documentos "en original o en copia, elaborados, firmados o manuscritos"; es decir, la presunción de autenticidad no es exclusiva para documentos firmados, sino que cobija otro tipo de documentos como los "elaborados". Finalmente, el quinto inciso del artículo refuerza esta presunción de autenticidad para todos los documentos que una parte aporte a un proceso, y hace una referencia expresa a la autenticidad de los documentos "en forma de mensaje de datos": "La parte que aporte al proceso un documento, en original o en copia, reconoce con ello su autenticidad y no podrá impugnarlo, excepto cuando al presentarlo alegue su falsedad. Los documentos en forma de mensaje de datos se presumen auténticos".

Hemos hablado extensamente en este artículo de los criterios de confiabilidad que consagró la Ley 527, particularmente en su artículo 11. Ahora bien, el artículo 244 parece ir en contra de estas disposiciones al establecer una presunción de autenticidad para todos los mensajes de datos, independientemente de su nivel de confiabilidad. ¿Existe una interpretación armónica de estas disposiciones? Así lo creemos. El artículo 244 es uno de los muchos ejemplos en los que el Legislador pretendió aliviar la carga probatoria a partir del principio de buena fe. Todos los documentos, incluyendo los mensajes de datos, se presumen auténticos, más allá de sus características técnicas o de su nivel de confiabilidad. Esto aplica, incluso, para las impresiones en papel de los mensajes de datos, tal y como lo menciona el mismo artículo 244 y como ha sido reconocido recientemente por vía jurisprudencial[29].

Para los mensajes de datos, los criterios de confiabilidad del artículo 11 entran a desempeñar un papel fundamental en el análisis probatorio en dos circunstancias: (i) cuando la parte en el proceso lo tache de falso en virtud del artículo 269 del Código General del Proceso, (ii) cuando el juez decida, en virtud del artículo 167 del Código General del Proceso, redistribuir y asignar la carga de la prueba a quien aportó el documento por las "circunstancias técnicas especiales" que tendría el mensaje de datos. El juez puede entonces considerar que la importancia del asunto amerita que la parte aportante de un proceso determine cómo en un mensaje de datos se puede identificar a su iniciador y establecer que el método de autenticidad es "confiable" y "apropiado" para el propósito del mensaje. Este asunto se ata y armoniza con lo dispuesto en el artículo 4 de la Ley 527, bajo la cual se concede un papel preponderante a la autonomía de la voluntad para determinar precisamente en qué circunstancias se estima confiable y apropiado un método preciso.

Finalmente, conviene hacer una breve referencia a otra de las grandes novedades de la Ley 527 en el equivalente funcional de original:

29. Así lo ha reconocido la Sección Tercera del Consejo de Estado en sentencia del 13 de diciembre de 2017, proceso con número de radicación 25000-23-26-000-2000-00082-01(36321): *"En estas condiciones, la Sala considera que las copias impresas de correos electrónicos, no tachadas de falsas por la persona a quien se oponen, cuando permitan una mínima individualización, esto es, cuando ofrezcan certeza sobre quien los ha elaborado, a quien se ha dirigido y cuándo, pueden ser valoradas, en tanto la individualización da lugar a asociar el contenido, lo que implica, a la luz del principio de buena fe, aceptar su autenticidad. Eso sí, de ello no se sigue que el medio de prueba resulte* per se *idóneo para la demostración que se pretende, pues su valoración estará sujeto a valoración conjunta y en especial de las reglas de la sana crítica"*.

Artículo 8.O original. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Como ya se mencionó, el concepto tradicional de original estaba asociado a la primera versión de un documento, aquella mediante la cual este era creado. En el mundo digital, esa "primera versión" no existe. Toda manifestación de un documento es en realidad una copia exacta de este. La información digital funciona de tal manera que todas las manifestaciones del documento son copias que el sistema de información crea para que la información digital pueda ser accedida y manipulada. Es por esto que el artículo 8, atinadamente, establece que todas estas "copias" podrán ser consideradas "originales", siempre y cuando haya una garantía de integridad de dicha información. Así pues, cualquier mensaje de datos que se aporte a un proceso deberá ser tenido como tal, siempre y cuando, de requerirse, la parte que lo aporte pueda probar que la información contenida en él no ha sido alterada desde el momento de creación de la primera "copia", incluso si la primera versión del mismo se creó en un medio físico o análogo y no en medio digital.

El artículo 247 del Código General del Proceso no habla específicamente del concepto de integridad, pero sin duda lo acoge y lo confirma como uno de los requisitos para su valoración:

Artículo 247. Valoración de mensajes de datos. Serán valorados como mensajes de datos los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que lo reproduzca con exactitud.

La simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos.

Para ser valorados como documentos, los mensajes de datos deben estar en un formato que permita probar su reproducción exacta.

Bajo las consideraciones previas, la consagración del "equivalente funcional" fue notoriamente innovadora, modificando incluso concepciones muy arraigadas como la del concepto de original. Es de resaltar que precisamente sobre ese tema se movieron las discusiones iniciales en los tribunales colombianos y hasta hace muy poco se superó la renuencia a admitir con plenas garantías la reproducción de un mensaje de datos en un medio impreso.

1.5 La autonomía de la voluntad en la Ley 527

Desde las discusiones previas a la formulación de la Ley Modelo de 1996, la CNUDMI resaltó la importancia de la autonomía de la voluntad respecto de las disposiciones del comercio electrónico. En 1991, mediante el informe ***Intercambio electrónico de datos***[30], antecedente de la Ley Modelo de 1996, este organismo concluyó que, pese a la conveniencia de establecer unas normas que ofrecieran un alto grado de certidumbre y armonización, se debía mantener un enfoque flexible respecto de ciertos temas y, en ese sentido, plantear cláusulas contractuales que sirvieran a las partes para abordar cuestiones concretas[31].

Esas recomendaciones fueron acogidas tanto en la Ley Modelo como parcialmente en la Ley 527, como queda en evidencia en el artículo 4, que establece la posibilidad de que algunas disposiciones de la Ley se puedan modificar por acuerdo[32]. Bajo esa premisa, el artículo 13 de la Ley Modelo, reproducido en el artículo 17 de la Ley 527, versa sobre la atribución de los mensajes de datos y consagra algunas fórmulas que les permiten a destinatario y a iniciador convenir previamente algunos procedimientos para asumir que un mensaje de datos es atribuible a alguna de las partes. Vale la pena mencionar que la norma no declara procedimientos específicos, así que bastaría que contractualmente las partes convinieran, por ejemplo, que siempre que se recibiera un mensaje de datos de un número determinado o de una cuenta de correo electrónico específica, los mensajes de datos podrían atribuirse de forma unívoca al iniciador sin que se requiera una firma (electrónica o digital) para acreditar el origen del mensaje.

De hecho, el artículo 7 en su numeral b) permite un buen grado de flexibilidad en torno a la firma al consagrar que basta que ***"el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado"***, sin imponer un método específico. Resulta desafortunado que la Ley 527 se haya apartado de la Ley Modelo de 1996 y no haya aclarado expresamente la posibilidad de determinar contractualmente la confiabilidad de los métodos de firma. No obstante, dada la especial redacción abierta de la norma, consideramos que los jueces eventualmente llegarán a aceptar que las partes puedan establecer si un determinado método les parece confiable en una determinada transacción o que, por ejemplo, la costumbre certificada pueda determinar dicha confiabilidad.

Sin embargo, lo que es cierto es que la flexibilidad referida reconoce los límites de las cláusulas contractuales para enervar normas imperativas de derecho interno —como es el caso de las normas procesales—, así como la inviabilidad de regular contractualmente los derechos y obligaciones de terceros. En virtud de lo anterior, la Ley 527 planteaba unos requisitos mínimos aceptables, los cuales, tal y como señala la guía de aplicación de la Ley Modelo, no comportan una invitación a establecer requisitos de forma más estrictos[33].

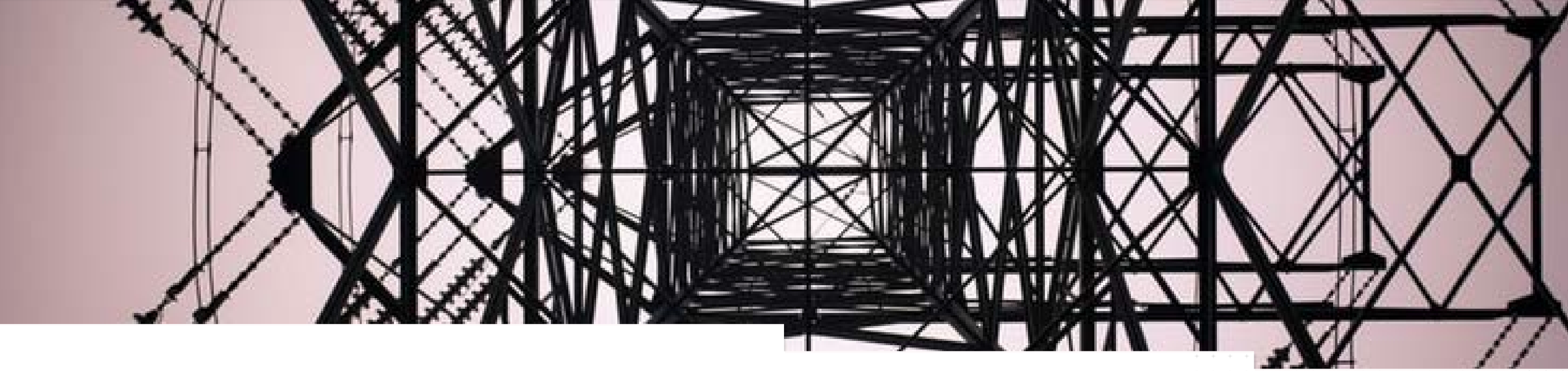
Pese a lo anterior, en Colombia no se afianzó la preponderancia de la autonomía de la voluntad para dar contenido a ciertas normas. Por ejemplo, la jurisprudencia nacional se decantó en su momento por inadmitir las copias de los mensajes de datos por no encontrarse en versión original, y por exigir la firma digital como mecanismo preponderante para garantizar la confiabilidad de la atribución en el marco de las actuaciones ante la administración de justicia. Esto se derivaba indispensablemente de la desconfianza cultural en torno a las particularidades técnicas de la información electrónica.

30. <?>

31. CNUDMI, (A/CN.9/ 350), fecha 1991. "Intercambio electrónico de datos". Párr. 130.

32. La Ley en todo caso distingue entre normas de orden público dentro de la misma ley y otras que se sujetan a un amplio grado de autonomía.

33. La guía señala lo siguiente: *"Debe considerarse que las disposiciones del capítulo II enuncian el requisito mínimo aceptable en materia de forma de los actos jurídicos, por lo que deberán ser consideradas como de derecho imperativo, salvo que se disponga en ellas expresamente otra cosa. La indicación de que esos requisitos de forma han de ser considerados como el 'mínimo aceptable' no deberá ser, sin embargo, entendida como una invitación a establecer requisitos de forma más estrictos en el derecho interno que los enunciados en la Ley Modelo"*



1.6 Ley 527: una implementación mediada por la desconfianza cultural

Como se ha ilustrado, bajo las disposiciones de la Ley 527 se pretendió consagrar una amplia gama de efectos a los mensajes de datos. Sin embargo, otras normas posteriores reiteraron la habilitación del uso de los medios electrónicos, dando cuenta de que la Ley 527 no bastó para extender culturalmente la confianza en el uso de estos[34].

El Consejo de Estado reconoce esta situación, desde la perspectiva de las instituciones jurídicas, señalando que

> *Los adelantos tecnológicos no son de fácil recepción o aceptación por parte de la comunidad jurídica e incluso su implementación no es tan rápida, como ha sucedido con la entrada en operancia* [sic] *del expediente electrónico. Pues bien, ha de tenerse cuenta que el documento electrónico, como medio de probanza, es un tema que sigue generando polémica y algo de inseguridad tanto para quien le interesa obre en el proceso, para quien se opone a él incluso para el operador jurídico al momento de decretar la prueba e incluso de practicarla, pues en varias de las veces se requiere apoyo, en mayor o menor escala, del soporte de sistemas o de personas profesionales en el manejo los medios electrónicos*[35].

34. Algunos ejemplos de la reiteración sobre la validez de los mensajes de datos son los siguientes:

- El artículo 19 de la ley 594 de 2000, la Ley General de Archivo, estableció que ***"Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de su archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos [...] PARÁGRAFO 1.***° Los documentos reproducidos por los citados medios gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por las leyes procesales y se garantice la autenticidad, integridad e inalterabilidad de la información". Hay que señalar en todo caso que esta provisión se acompasa con el requisito que pesa sobre las autoridades de contar con los mecanismos de archivo idóneos para mantener la integridad de la evidencia electrónica.

Los artículos 55 y 216 del CPACA que admiten lo que ya había admitido la Ley 527: la validez probatoria de los mensajes de datos en el marco de las actuaciones administrativas.

El capítulo IV del Decreto 2170 de 2002 dedicado exclusivamente al uso de medios electrónicos en la contratación estatal.

35. Ver Sentencia N.° 76001-23-33-000-2015-01577-02 de Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Quinta, de 24 de noviembre de 2016.

La desconfianza normativa e institucional hacia el uso de estos medios refleja una desconfianza cultural, que es más profunda y difícil de erradicar. Pese a lo anterior, las realidades de hoy han ido construyendo una narrativa y unas necesidades diferentes: por ejemplo, como se menciona en la introducción del artículo, la permeabilidad del comercio electrónico en el país cada vez crece más y los mecanismos de autenticación y atribución a fin de obligarse en el marco de esas relaciones comerciales se hacen cada vez más flexibles. El número de teléfono como mecanismo de autenticación de usuarios es muestra de lo anterior.

También en el ámbito procesal es cada vez más común la incorporación de evidencia electrónica, de la cual el 60 % corresponde a correos electrónicos, y 35 %, a chats de WhatsApp, y de estos 23 % son mensajes de voz; el resto son páginas de internet y otro tipo de documentos[36]. Bajo esta transformación o aceptación social creciente de los medios electrónicos, las Cortes también han modulado las discusiones permitiendo mejores condiciones, menos restrictivas, respecto del uso de medios electrónicos en el ámbito sustancial y probatorio[37].

No obstante lo anterior, queda mucho por lograr para afianzar lo pretendido por la Ley 527, particularmente en el sector público. Por ejemplo, es momento de que la contratación estatal admita plenamente, en la práctica, la valía de los mensajes de datos y de la firma electrónica en los procesos estatales, en vez de dar cabida a interpretaciones diferenciadas por cada institución respecto del uso de dichos medios.

36. Informe de Adalid Corp, citado en: https://www.enticconfio.gov.co/audios-whatsapp-prueba-judicial.

37. Ver por ejemplo el caso de la admisión de notas de voz como medios de prueba en el marco de un proceso penal, que condujo a que una jueza de control de garantías impusiera medida de aseguramiento.

La Corte Suprema de Justicia colombiana aprueba la legalidad de este tipo de conversaciones realizadas por la víctima: *"una grabación hecha por un particular sin orden judicial tendrá validez en un proceso penal si se realiza directamente por la víctima o con su aquiescencia, si capta el momento de la comisión del delito y si su finalidad es pre constituir prueba del mismo.* ***No es viable grabar conversaciones propias con terceros y usarlas en beneficio de intereses particulares"***. Ver Sentencia 41790 de 2013.

02

La Ley 527 y las tecnologías emergentes: Lo que viene

2.1 Inteligencia artificial y la atribución de los mensajes de datos

La inteligencia artificial (IA) plantea retos en el ámbito de la validez jurídica de la información electrónica, así como en muchos otros ámbitos. Explicar las características de esa tecnología desborda el alcance de este artículo, por lo que basta con dejar esbozada la discusión respecto de la atribución de los mensajes de datos cuando estos se realizan de forma automatizada a través de un sistema de información que, al menos en teoría, carece de acción humana.

La Ley 527 funda la atribución en la relación que vincula al iniciador y al destinario[38], como lo precisa el artículo 16 de la Ley al señalar que se podrá atribuir a un iniciador determinado mensaje de datos cuando ha sido enviado por: (i) el iniciador, (ii) una persona facultada por él y/o (iii) lo envía un sistema de información programado por el iniciador o en su nombre para que opere automáticamente[39]. Este último criterio de atribución, anuncia la guía para la implementación de la Ley Modelo de 1996, implica que *"los mensajes de datos generados automáticamente en una terminal informática sin intervención humana directa deberán ser considerados como 'iniciados' por la persona jurídica en cuyo nombre se haya programado la terminal informática"*.

De lo anterior se pueden mencionar dos retos para el uso de la IA en el marco de la Ley 527: (i) la definición de "sistema de información" en los términos de la ley, que parece limitarse a medios técnicos de transmisión, recepción y archivo, y (ii) que la atribución de los mensajes de datos generados automáticamente solo se predique de personas jurídicas, conforme a lo que señala la guía. Dado que la IA es mucho más que un medio técnico de transmisión y que su gestión

38. Conforme a lo que indica la guía de implementación de la Ley Modelo de 1996, los vocablos "iniciador" y "destinatario" hacen referencia a personas, sin que ello implique que se refiera únicamente a personas naturales. Tales vocablos abarcan sociedades legalmente constituidas y demás personas jurídicas.

39. Textualmente el artículo 16 señala:

- "ARTICULO 16. ATRIBUCION DE UN MENSAJE DE DATOS. *Se entenderá que un mensaje de datos proviene del iniciador, cuando este ha sido enviado por:*
- *1. El propio iniciador.*
- *2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje, o*
- *3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente".*

puede comprometer y ser atribuible también a una persona natural, ambos asuntos deberían ser revisitados a la luz de la nueva realidad tecnológica, ampliando la definición de "sistema de información" y el alcance de dicha atribución.

A pesar de lo anterior, la amplitud de la Ley 527 da cabida para que, aún 20 años después de la expedición de esta, se pueda alzar una interpretación favorable respecto de la atribución de los mensajes de datos creados y enviados a través de mecanismos que usan IA, sin comprometer la confiabilidad que exige el artículo 11 de la Ley.

2.2 Blockchain y la Ley 527

Otro capítulo del libro en que se publica el presente artículo trata extensamente de las implicaciones jurídicas de la tecnología conocida como ***blockchain*** o cadena de bloques. A nosotros nos compete solamente hacer un breve comentario. Tal vez la principal prueba de la neutralidad de la Ley 527 y de la visión del Legislador de 1999 es que esta tecnología se está masificando sin necesidad de modificar el ordenamiento jurídico. La información almacenada y compartida a través de una cadena de bloques puede ser utilizada en transacciones de todo tipo en virtud del artículo 5 de La Ley 527, puede ser analizada según los criterios de confiabilidad del artículo 11 y puede ser aportada en procesos judiciales aplicando los equivalentes funcionales de escrito, firma y original que discutimos atrás. Si bien la Ley 527 regula extensamente la utilización de terceros de confianza, denominados entidades de certificación, la neutralidad tecnológica y el principio del equivalente funcional no exigen la intervención de un tercero para garantizar la autenticidad e integridad de la información. La Ley 527 es el marco jurídico por el que todavía, 20 años después, podemos adoptar una tecnología revolucionaria y no imaginada.

03

Comentario final: La Ley 527 y la inclusión digital

Hemos visto que la validez de la información digital depende de manera directa de criterios de confiabilidad como la autenticidad y la integridad. También mencionamos el camino accidentado que hemos recorrido en los últimos años para aplicar estos conceptos a las transacciones jurídicas. Cabe preguntarse ahora: ¿cuál es la importancia de estos temas hoy, 20 años después de la expedición de la Ley 527? ¿Tienen vigencia —ya no jurídica sino práctica— las directrices que nos dio la Ley 527?

Son muchas las respuestas que se pueden dar a esta pregunta, y hoy podemos ver el impacto de la autenticidad e integridad de la información digital en todos los ámbitos de nuestra economía, pero para cerrar quisiéramos destacar el rol que desempeña la validez de la información digital en un área con la que no se suele asociar: la inclusión digital.

Hoy en día aproximadamente un millardo de personas carece de alguna forma de identificación y 3,4 millardos tienen alguna forma de identificación legal pero no pueden usarla en medios digitales. Las consecuencias de esto son devastadoras. Para hablar solo de inclusión financiera, el 18 % de los adultos excluidos económicamente no pueden acceder a servicios financieros porque carecen de los documentos necesarios para probar su identidad.

Colombia ya está en el camino hacia la conversión de su economía en una economía digital. Estamos desarrollando iniciativas en campos tan variados como los servicios ciudadanos inteligentes, la historia clínica electrónica, la factura electrónica, la justicia digital, la alfabetización digital, entre muchos otros. En todos ellos, el primer obstáculo por superar es el de garantizar los efectos jurídicos de las transacciones que se hacen a través de estos proyectos, trascendiendo la eventual desconfianza que susciten los medios digitales. Sin la seguridad jurídica de la validez de estas transacciones, estos proyectos no llegarán a feliz término.

Un requisito necesario para esta seguridad jurídica es la garantía de la autenticidad e integridad de las transacciones. Los sistemas de identidad digital son los que permitirán autenticar a las personas en sus actividades digitales con el Estado, con el sector financiero, y con todos los ámbitos de la economía digital. Los sistemas de identidad digital son la llave para lograr la inclusión digital, y la Ley 527 es el marco jurídico que permite la implementación y masificación de estos sistemas de identidad digital. No podremos desaprovechar la oportunidad de revisitar las disposiciones de la Ley y evitar que las discusiones al respecto se compliquen de forma tal que obstruyan la adecuada implementación de los sistemas de identidad digital. En igual medida deberá considerarse la necesidad de promover lineamientos de seguridad digital que preserven los valores que con mayor celo cuidan los ciudadanos, para así combatir los rezagos de la desconfianza cultural que todavía permea la aplicación de normas innovadoras. La importancia de este marco jurídico, pues, no puede ser mayor para la inclusión digital de los colombianos.

Bibliografía

Cruz Tejada, Horacio (agosto de 2015). ***Nuevas tendencias del derecho probatorio.*** Segunda edición ampliada. Edición Uniandes. ISBN: 978-958-774-184-1.

López Blanco, Hernán Fabio (2017). ***Código General del Proceso (pruebas).*** Dupre Editores Ltda. ISBN 978-958-56408-0-1.

Jurisprudencia

Sentencia de Corte Suprema de Justicia, Sala de Casación Laboral, N.º 49043 de 25 de abril de 2018.

Sentencia de Corte Suprema de Justicia, Sala de Casación Civil y Agraria, N.º 5397 de 12 de septiembre de 2000.

Sentencia N.º 25000-23-36-000-2013-01082-01 de Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, de 13 de noviembre de 2018.

Sentencia N.º 11001-03-26-000-2013-00149-00 de Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, de 19 de septiembre de 2016.

COMUNICACIÓN ELECTRÓNICA Y CONTRATOS ELECTRÓNICOS

ELECTRONIC COMMUNICATION AND ELECTRONIC CONTRACTS

Daniel Peña Valenzuela[40]

Resumen

Los mensajes de datos y las comunicaciones electrónicas son los ejes de las normas sobre comercio electrónico en el modelo de la CNUDMI. La existencia y la validez de los documentos electrónicos permiten la utilización efectiva de la prueba digital. Respecto de las declaraciones de voluntad por medios electrónicos, son la base para la oferta y aceptación en el entorno digital, así como para los contratos inteligentes, en los cuales la fase de ejecución es automatizada.

Abstract

Data messages and electronic communications are the axes of the rules on electronic commerce in the Uncitral model. The existence and validity of electronic documents allows the effective use of digital evidence. Regarding declarations of will by electronic means, they are the basis for the offer and acceptance in the digital economy as well as for smart contracts in which the execution phase is automated.

40. Profesor titular de la Universidad Externado de Colombia de las Facultades de Derecho, Finanzas y Administración de Empresas. Con maestría en leyes (LLM) de la UCL-Universidad de Londres. Máster en Propiedad Intelectual, Contratos y Derecho de las Nuevas Tecnologías (DESS), de la Université Pierre Mendès-France (Grenoble 2). Árbitro de la Cámara de Comercio de Bogotá y de la Cámara de Comercio de Medellín. Árbitro de la Organización Mundial de la Propiedad Intelectual (OMPI). Socio de la firma Peña Mancero Abogados en Bogotá. Director de investigación en comercio electrónico del Departamento de Derecho de los Negocios de la Universidad Externado de Colombia.

Agradezco la colaboración brindada por Juan Sebastián Alarcón Castillo y Natalia Sofía Miranda Gómez, monitores de la línea de investigación de comercio electrónico del Departamento de Derecho de los Negocios de la Universidad Externado de Colombia por la revisión editorial de este artículo.

Introducción

Con motivo de los veinte años de vigencia de la Ley 527 de 1999, Colombia debe llevar a cabo un balance del efecto que ha tenido el trasplante en el ordenamiento jurídico nacional del modelo de comercio electrónico de la Comisión de las Naciones Unidas del Derecho Mercantil Internacional (CNUDMI). Entre los ejes fundamentales de ese modelo, las nociones de comunicación electrónica y contrato electrónico despuntan como aportes conceptuales a las categorías jurídicas tradicionales, en particular, en el derecho probatorio y en la teoría del negocio jurídico.

La CNUDMI, en especial el Grupo de Trabajo IV, ha desarrollado en su labor de casi cuatro décadas un corpus normativo integrado por distintos instrumentos relacionados con la temática del comercio electrónico tales como convenciones, leyes modelo, guías legislativas y recomendaciones, así como textos explicativos y guías de implementación. Dichos instrumentos han contribuido a definir el alcance, la interpretación y la aplicación práctica de los mensajes de datos y de los contratos por medios electrónicos.

En Colombia, con la entrada en vigencia de la Ley 527 de 1999 se inició un desarrollo paulatino de los conceptos incorporados por esta a partir de estudios doctrinales, decisiones judiciales y práctica comercial. En el actual entorno de transformación digital de las empresas y del gobierno electrónico se aprecia una mayor apropiación por parte de los comerciantes respecto de la validez y eficacia jurídica de las comunicaciones electrónicas, así como de su utilización en el ámbito contractual.

La relación entre las categorías tradicionales del derecho —documento y contrato— y las nuevas nociones —mensaje de datos y contrato electrónico— surgidas de la utilización de la tecnología justifica el modelo de la CNUDMI. Los principios de interpretación o principios puente entre los cuales se destaca el principio de equivalencia funcional facilitan la aplicación práctica de los mensajes de datos y de la contratación electrónica en un entorno cada vez más proclive al uso de medios digitales.

En este escrito se abordará la historia y la evolución de los conceptos de comunicaciones electrónicas y contratos electrónicos, su interrelación y los vasos comunicantes entre las dos figuras, así como una visión prospectiva sobre el futuro de la contratación web y de la contratación inteligente como nuevo paradigma tecnológico y legal surgido a raíz de las aplicaciones prácticas de la cadena criptográfica de bloques blockchain. Las controversias jurídicas fundamentales en estas temáticas giran en torno a la validez, eficacia y legalidad de los mensajes de datos y su alcance probatorio, tales como la validez del consentimiento a los contratos web y la calificación de los contratos inteligentes como contratos en el sentido jurídico del término, así como la automatización que traen consigo en la fase de ejecución o cumplimiento.

01

El mensaje de datos y la comunicación electrónica

El Comité de Ciencia y Tecnología de la Asociación Americana del Derecho (ABA) introdujo por primera vez en una legislación sobre firmas digitales y comercio electrónico el concepto de ***electronic record*** con el fin de conceder valor jurídico pleno al registro electrónico, que es el elemento propio de las bases de datos. Aún en ese momento no era claro que internet, con su dinámica en la transmisión de paquetes de información, crearía la necesidad de ampliar el alcance de registro electrónico a la categoría legal de mensaje de datos, núcleo central de la nueva visión de la evidencia digital.

En los trabajos de la CNUDMI respecto de comercio electrónico, firmas electrónicas y digitales se introduce el ***electronic message*** o mensaje de datos, más dinámico y asociado a la transmisión de información, es decir, comunicaciones electrónicas en la red global. Internet, como una red digital de transmisión de información y no un mero repositorio de datos, permitía el acceso y circulación de contenidos digitales ente servidores, redes y dispositivos.

En la Ley 527 de 1999 se incorporó la noción de mensaje de datos en el ordenamiento colombiano como categoría jurídica que incorpora la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares: entre otros, el intercambio electrónico de datos (EDI), internet, el correo electrónico, el telegrama, el télex o el telefax. Esta enumeración de ejemplos coincide con una noción más común y tradicional: el documento electrónico.

El mensaje de datos puede ser ***inmaterializado*** en el evento en que haya sido generado de manera original por medios digitales o ***desmaterializado*** si, luego de haber sido creado por medios tradicionales, es convertido a medios electrónicos, por ejemplo, mediante escaneo. En las pantallas de los dispositivos en los que se visualiza la interfaz del sistema de información al usuario le aparece una imagen o una representación del mensaje de datos que tiene metadatos, los cuales permiten determinar características como el autor, fecha de creación, cambios, modificaciones sucesivas, entre otras. También es representativo cuando incorpora imágenes o textos que acreditan la ocurrencia de un hecho en circunstancias de tiempo, modo y lugar determinables. El mensaje de datos es declarativo cuando su contenido se refiere a una declaración de voluntad en la que se expresa la intención de la parte, por ejemplo, de contraer obligaciones.

El modelo de regulación del comercio electrónico de la CNUDMI incluye además los métodos de autenticidad e integridad: la firma electrónica y la firma digital, y los documentos electrónicos transferibles, cuyos efectos se irradian a todo el ordenamiento jurídico colombiano. Este modelo abarca también tecnologías emergentes como los registros electrónicos que componen ***blockchain***, la cadena de bloques cifrada y descentralizada, es decir, una tecnología disruptiva que corresponde a un sistema de información a la luz del derecho uniforme creado por la CNUDMI. Los registros de la cadena de bloques son mensajes de datos localizados y localizables en su generación, transmisión y almacenamiento, con la posibilidad de combinar criterios geográficos de la información como tal; por ejemplo, el lugar en que se encuentran los equipos que soportan el registro original o en los cuales los efectos de la transmisión de la información tienen lugar.

1.1 El mensaje de datos como documento sin soporte material como tal

En sentido *lato*, documento es el soporte material o *"diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos. Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo"*[41]. Esta noción tradicional de documento incorpora la idea de "materialización" y "corporeidad" que acompaña el entendimiento natural del término.

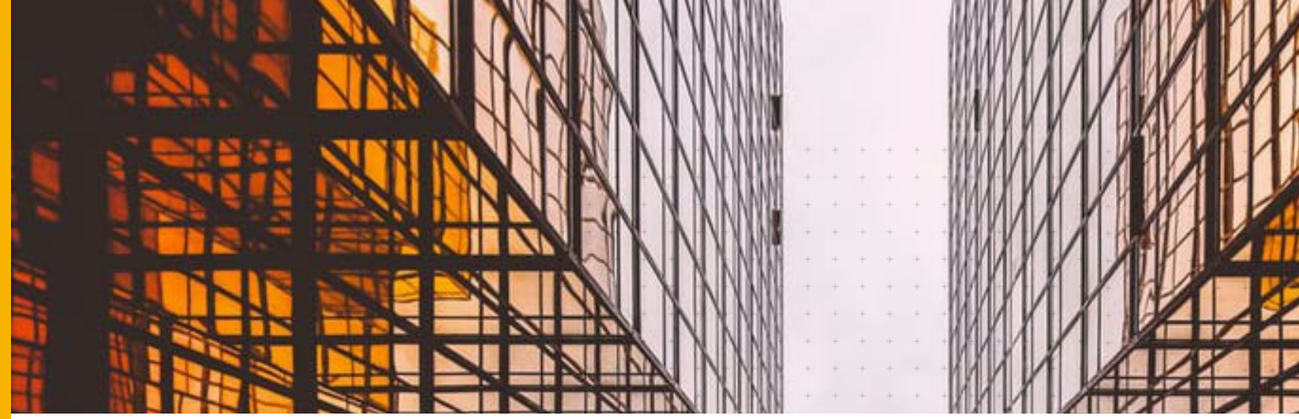
En sentido estricto desde el punto de vista jurídico, y en particular de los procedimientos judiciales, el documento es un medio probatorio que se enmarca dentro de la libertad general probatoria[42]. El Código General del Proceso, en el capítulo de pruebas, define el documento como "todo objeto mueble que tenga carácter representativo o declarativo" y se incluyen ejemplos de las distintas clases de documentos. De acuerdo con el Código, pueden considerarse documentos, entre otros "los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, los mensajes de datos y a las videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos, las inscripciones en lápidas, monumentos, edificios o similares"[43].

En el Código General del Proceso, los documentos electrónicos o en formato electrónico se considerarán "documentos" por cuanto la enumeración dada por el ordenamiento los incluye expresamente. La "materialidad" o soporte físico no es un requisito esencial de la noción de "documento". El Código hace referencia a "objeto mueble", que bien podría ser intangible o desmaterializado, o existir como un registro o entrada en un sistema de información o base de datos, entre otros. Esta noción no se refiere necesariamente a documentos compuestos de números y letras. Por ejemplo, las imágenes de videovigilancia pública y privada que utilizan videograbaciones digitales son mensajes de datos en su origen, almacenamiento y eventual transmisión.

41. Diccionario de la Real Academia de la Lengua Española. Recuperado de: http://www.rae.es/.

42. El artículo 165 del Código General del Proceso establece *"Medios de Prueba. Son medios de prueba, la declaración de parte, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial,* los documentos*, los indicios, los informes y* cualesquiera otros medios que sean útiles para la formación del convencimiento del juez" (negrilla fuera de texto).

43. El artículo 243 del Código General del Proceso reza: "Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares [...]".



1.2 El mensaje de datos como documento privado y público

La noción amplia de documento prevista en la Ley 527 de 1999 y en el Código General del Proceso no hace distinción en relación con los documentos electrónicos por la naturaleza de su creador o emisor, es decir, la diferencia entre documentos públicos o privados. En efecto, "en toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el solo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original"[44].

De esta manera, el documento público electrónico es el otorgado por el funcionario público en ejercicio de su cargo o con su intervención utilizando medios electrónicos o mediante mensaje de datos; es el caso, por ejemplo, del acto administrativo por medios electrónicos o una sentencia judicial que se profiera y notifique por medios digitales. Así mismo se considera el documento otorgado por medios digitales por un particular en ejercicio de funciones públicas o con su intervención[45].

El Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA) refuerza la regla de validez plena de la Ley 527 al establecer que "Los documentos públicos autorizados o suscritos por medios electrónicos tienen la validez y fuerza probatoria que le confieren a los mismos las disposiciones del Código General del Proceso. Las reproducciones efectuadas a partir de los respectivos archivos electrónicos se reputarán auténticas para todos los efectos legales"[46]. El CPACA considera que la duplicación, copia o imagen de un registro electrónico original en una base de datos del Estado se considera como auténtica.

44. Artículo 10 de la Ley 527 de 1999: "Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original" (negrilla fuera de texto).

45. Artículo 243 del Código General del Proceso, inciso 2: "Los documentos son públicos o privados. Documento público es el otorgado por el funcionario público en ejercicio de sus funciones o con su intervención. Así mismo, es público el documento otorgado por un particular en ejercicio de funciones públicas o con su intervención. Cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumento público; cuando es autorizado por un notario o quien haga sus veces y ha sido incorporado en el respectivo protocolo, se denomina escritura pública".

46. Artículo 55 de la Ley 1437 de 2011, Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

1.3 El expediente electrónico: haz de mensajes de datos

En un trabajo conjunto con el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), el Archivo General de la Nación (AGN) presenta la Guía técnica para la gestión de documentos y expedientes electrónicos, la cual es el resultado de un proceso de revisión y aclaración de conceptos relacionados con los documentos y expedientes electrónicos, realizado por un grupo de profesionales de las dos entidades en mención.

Esta guía ha sido creada con el fin de brindar parámetros que permitan a las entidades públicas y privadas que cumplen funciones públicas comprender la importancia del documento electrónico de archivo, su estructura y sus características, así como las etapas para su gestión durante todo su ciclo vital, la conformación de los expedientes electrónicos y los elementos que lo integran, incluyendo la gestión de los metadatos mínimos obligatorios.

Es además una herramienta que se rige bajo Ley 594 de 2000 y está dirigida a la administración pública, a las áreas de gestión documental, calidad, tecnologías de la información y las comunicaciones, así como a todas aquellas entidades que desarrollan procesos para la planeación, producción, gestión y trámite, organización, transferencia, disposición, preservación y valoración de los documentos electrónicos de archivo, y en general a cualquier organización pública o privada que gestione documentos y expedientes electrónicos de archivo.

De igual manera, es un documento que pretende servir de referencia para la construcción de expedientes y documentos electrónicos con características de archivo que busca estandarizar la producción documental en entornos electrónicos y facilitar la interoperabilidad, independientemente de la tecnología utilizada. El documento público electrónico es oponible erga omnes respecto a la fecha y lugar de su otorgamiento, al otorgamiento mismo, a quienes intervinieron en el acto y a lo que declararon en él. Tiene fuerza de plena prueba respecto de las declaraciones emitidas por las partes, pero en todo caso podrá demostrarse que su contenido no corresponde a la realidad sin que se puedan afectar los derechos de terceros que de buena fe hayan confiado y actuado con base en lo expresado en el documento. Frente a terceros ajenos a la elaboración del documento, los documentos públicos constituyen plena prueba respecto de lo que les favorezca, mientras que respecto de lo que lesione sus intereses deberán aplicarse las reglas de la sana crítica.

El Gobierno Nacional y las altas Cortes han puesto en marcha el piloto Expediente Electrónico Judicial, uno de los primeros esfuerzos concretos por encaminar al país hacia un panorama de justicia digital. La herramienta piloto, que permitirá litigar en línea, gestionará cinco tipos de procesos judiciales a través de una plataforma unificada.

La iniciativa reúne esfuerzos de la Comisión de Justicia en Línea del Consejo de Estado, el Ministerio de Justicia, el Ministerio de TIC, la Alta Consejería Presidencial para la Transformación Digital, la Corte Suprema de Justicia, la Corte Constitucional y el Consejo Superior de la Judicatura. El proyecto piloto arrancará con procesos judiciales como: trámites de nulidad de propiedad industrial, nulidad en asuntos tributarios, acción pública de inconstitucionalidad, trámites de selección, revisión y acción de tutela y execuátur.

Según resulte la primera fase, se espera que la digitalización del litigio llegue a todos los procesos adelantados por la rama judicial. Para una segunda etapa, la herramienta daría soluciones a solicitudes de jueces para la ejecución de penas y permitiría trámites de medidas cautelares, títulos judiciales y otros procesos. También llegaría a comisarías de familia, inspecciones de policía y superintendencias.

1.4 Legalidad de la prueba electrónica

El valor probatorio del mensaje de datos tiene como supuesto básico la legalidad de la prueba, es decir, que la información del contenido digital objeto de la evidencia no hubiere sido obtenida como resultado de la intromisión abusiva o indebida en el sistema de información, de la interceptación ilegal en el proceso de transmisión de esta, de la violación de datos personales o de la infracción al secreto empresarial o industrial. Por ende, la admisibilidad de la prueba está vinculada a la legitimación que tenga su tenedor, la cual se expresa en términos de custodia, posesión o propiedad legítimo.

Por ejemplo, el emisor de un mensaje de datos puede legalmente presentar la prueba en el proceso porque fue su creador y tiene la posesión legítima de este. En caso de que se haya violado el derecho de un tercero o su intimidad o la protección a los datos personales para obtener un documento, no solamente es una prueba inválida e ineficaz, sino que además quien la presente en un proceso podría estar incurso en un hecho punible[47].

47. La detentación ilegal e ilegítima de un mensaje de datos puede ser consecuencia del acceso abusivo a un sistema de información o la violación de datos personales de un tercero (Ley 1273 de 2009). Como ejemplo podrían mencionarse correos electrónicos o mensajes de texto de terceros, y comunicaciones interceptadas sin orden judicial y obtenidas ilícitamente.

1.5 Valoración probatoria de los mensajes de datos

El documento electrónico tiene un formato digital y electrónico que debe conservarse con sus características técnicas propias y originales, como cualquier otro documento. La condición de original del documento electrónico implica que no debe ser convertido a un soporte físico so pena de perder sus atributos técnicos y, por ende, perder la fuerza y el valor probatorio previsto para los mensajes de datos en el ordenamiento jurídico. De acuerdo con el Código General del Proceso,

> *"serán valorados como mensajes de datos los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que lo reproduzca con exactitud. La simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos"*[48].

Los documentos en forma de mensaje de datos se presumen auténticos[49],pero esta presunción no abarca integridad del contenido. El documento electrónico original debe presentarse en la misma forma en que fue creado, por ejemplo, para el decreto de un mandamiento ejecutivo. Las partes deberán aportar el original del documento cuando estuviere en su poder, salvo causa justificada. Cuando se allegue copia, el aportante deberá indicar en dónde se encuentra el original; por ejemplo, en qué sistema de información o base de datos, si tuviere conocimiento de ello[50].

Cuando se quiera reivindicar la presunción de autenticidad de los mensajes de datos, no es admisible la impresión de una copia en papel, ya que deben ser valorados como mensajes de datos solamente los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados o recibidos, o en algún otro formato que los reproduzca con exactitud. La simple impresión en papel de un mensaje de datos es valorada de conformidad con las reglas generales de los documentos. En este último caso, dicha impresión es la simple copia de otro documento original que fue generado, almacenado o trasmitido por medios electrónicos, y deberá ser apreciada con tal valor probatorio y sujeta a la contradicción respectiva.

Para la valoración de la fuerza probatoria de los mensajes de datos, según la Ley 527 de 1999, se deben tener en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. De manera particular, se debe tener en cuenta: ***"la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente"***[51]. El criterio técnico de la confiabilidad abarca al método que vincula la identidad del emisor del mensaje y la generación del mensaje de datos. El valor probatorio de un mensaje de datos depende de las características técnicas de los sistemas de información que han permitido y habilitado su generación, creación, almacenamiento y transmisión.

Para la Corte Suprema de Justicia, la confiabilidad está vinculada a los atributos técnicos del mensaje de datos que garanticen su integridad, inalterabilidad, recuperabilidad y rastreabilidad así:

48. Artículo 247 de la Ley 1564 de 2012, Código General del Proceso.

49. Artículo 244 de la Ley 1564 de 2012, Código General del Proceso.

50. El artículo 245 de la Ley 1564 de 2012, Código General del Proceso, señala: ***"Los documentos se aportarán al proceso en original o en copia.***

Las partes deberán aportar el original del documento cuando estuviere en su poder, salvo causa justificada. Cuando se allegue copia, el aportante deberá indicar en dónde se encuentra el original, si tuviere conocimiento de ello".

51. Artículo 11 de la Ley 527 de 1999

la integralidad de la información tiene que ver con que el texto del documento transmitido por vía electrónica sea recibido en su integridad por el destinatario, tarea que puede cumplirse técnicamente utilizando el procedimiento conocido como "sellamiento" del mensaje, mediante el cual aquel se condensa de forma algorítmica y acompaña al mensaje durante la transmisión, siendo recalculado al final de ella en función de las características del mensaje realmente recibido; de modo, pues, que si el mensaje recibido no es exacto al remitido, el sello recalculado no coincidirá con el original y, por tanto, así se detectará que existió un problema en la transmisión y que el destinatario no dispone del mensaje completo. Incluso, la tecnología actual permite al emisor establecer si el receptor abrió el buzón de correo electrónico y presumiblemente leyó el mensaje. Esa característica guarda una estrecha relación con la "inalterabilidad", requisito que demanda que el documento generado por primera vez en su forma definitiva no sea modificado, condición que puede satisfacerse mediante la aplicación de sistemas de protección de la información, tales como la criptografía y las firmas digitales.

La "rastreabilidad" del mensaje de datos consiste en la posibilidad de acudir a la fuente original de creación o almacenamiento del mismo con miras a verificar su originalidad y su autenticidad. La "recuperabilidad", o sea la condición física por cuya virtud debe permanecer accesible para ulteriores consultas; y la "conservación", pues de ella depende la perduración del instrumento en el tiempo, siendo necesario prevenir su pérdida, ya sea por el deterioro de los soportes informáticos en que fue almacenado, o por la destrucción ocasionada por "virus informáticos" o cualquier otro dispositivo o programa ideado para destruir los bancos de datos informáticos. Una óptima conservación de la información puede lograrse mediante la aplicación de protocolos de extracción y copia, como también con un adecuado manejo de las reglas de cadena y custodia[52].

El criterio de la confiabilidad vinculada al valor probatorio de un mensaje de datos, sobre todo si existe controversia entre las partes sobre el contenido o la autoría, necesita la consideración de las características técnicas de la prueba documental[53]. La determinación del grado de confiabilidad puede eventualmente, en caso del ejercicio de la contradicción, requerir de la prueba pericial, cuyo objeto son las características técnicas y no el contenido del documento. En ese orden de ideas, la pericia no reemplaza la naturaleza de documento propia de los mensajes de datos, pero la definición, determinación o análisis de las características propias de la información digital puede exigir conocimientos especializados en informática y seguridad tecnológica. Los sistemas de información y las herramientas informáticas utilizadas en la generación, transmisión y almacenamiento de los mensajes de datos pueden ser explicados al juez de manera clara y sencilla por las partes procesales con el fin de evitar que el análisis del documento requiera necesariamente la intervención del perito.

La utilización de la inspección judicial en relación con los mensajes de datos también encuentra limitaciones en su eficacia ya que este medio probatorio solo se puede utilizar *"cuando sea imposible verificar los hechos por medio de videograbación, fotografías u otros documentos, o mediante dictamen pericial, o por cualquier otro medio de prueba"*. El juez puede aceptar que un documento electrónico aportado se complemente con una inspección judicial para demostrar el lugar donde se encuentra almacenado o archivado (por ejemplo, en un servidor o en un dispositivo). La originalidad y la autenticidad de un mensaje de datos se encuentran en las características técnicas inherentes a este, a sus funcionalidades, a la forma de su creación y no al lugar donde se encuentre ubicado.

La disponibilidad de la evidencia digital y su valor jurídico dependen en gran medida de buenas prácticas y estrategias de seguridad de información en su creación, transmisión y almacenamiento, todas las anteriores con un respaldo técnico.

52. .Corte Suprema de Justicia, Sala de Casación Civil, 16 de diciembre de 2010, Sentencia 2004-01074. M. P. Pedro Octavio Munar.

53. En el artículo 4.° del Decreto 2364 de 2012 se establecen los criterios de confiabilidad de la firma electrónica: "la firma electrónica se considerará confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si: 1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante. 2. Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma. Parágrafo. Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona: 1. Demuestre de otra manera que la firma electrónica es confiable; o 2. Aduzca pruebas de que una firma electrónica no es confiable".

La primera fase para establecer políticas de manejo seguro y confiable de los documentos electrónicos es la identificación de la información digital dentro de la organización con el fin de que se puede acceder a ella cuando se requiera su utilización y eventual presentación a terceros, incluyendo las autoridades que lo exijan. Así pues, la información relevante se debe preservar, retener y almacenar, para lo cual es importante establecer criterios determinados de retención de datos como la clase, la localización y la fuente de la información digital. El propósito de esto es evitar la destrucción involuntaria o provocada de la información digital que traiga consigo sanciones legales si existía el deber de retención documental o la pérdida de una prueba importante respecto de un hecho que podría sustentar un argumento jurídico a favor.

Para aportar la prueba digital es necesario clasificar la información específica mediante el filtro que permita determinar el fin o el requerimiento en particular. En ese momento se debe tomar la decisión sobre qué medio probatorio es el más adecuado para la presentación de la evidencia digital ante los jueces o autoridades. En caso de que las características técnicas de confiabilidad sean suficientes, basta con la presentación del archivo digital que contiene la información digital. De lo contrario, se deben explicar o reforzar tales características con un experto forense tecnológico.

Para la exhibición del documento electrónico que reposa en los sistemas de información de terceros es preciso tener en cuenta que el solicitante debe identificar el sistema de información en el cual se encuentra el mensaje de datos y todos los datos pertinentes como el equipo o dispositivos en los que está almacenado, su titular, los usuarios, entre otros. El juez, por su parte, debe definir e identificar el nombre del archivo y sus características técnicas, así como cualquier especificación o funcionalidad adicional con el fin de determinar el momento de creación y su presunta autoría. Luego, el documento debe ser extraído y copiado utilizando las herramientas que permitan mantener el formato electrónico y evitar que sea alterado o modificado.

En el campo de la investigación criminal, el recaudo y la cadena de custodia aplicable a la información digital y los mensajes de datos es definida en su alcance y características:

> *con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los c ambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos. La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente*[54].

Estas normas del ordenamiento penal pueden ser aplicadas a los procedimientos civiles, disciplinarios, contencioso-administrativos y, en general, a las inspecciones y diligencias judiciales y administrativas que tengan como objeto el recaudo de evidencia digital que ha sido generada, almacenada o transmitida por medios digitales.

54. Artículo 254 de la Ley 906 de 2004, Código de Procedimiento Penal.

1.6 La autoría y autenticidad del mensaje de datos

El documento, sea original o copia, es auténtico cuando existe certeza sobre la persona que lo ha elaborado, manuscrito o firmado, o cuando exista certeza respecto de la persona a quien este se atribuya[55], es decir, cuando no exista duda alguna respecto de quién generó o creó el documento ni de la aceptación a su contenido. También es auténtico el documento inscrito en un registro público[56]. En el caso del registro mercantil, cuando el documento no sea público, debe ser presentado por sus otorgantes de manera personal ante el secretario de la cámara respectiva[57]. Los libros de comercio debidamente registrados se presumen auténticos[58]; la formalidad de la inscripción de los libros ante las cámaras se eliminó[59].

En el campo mercantil, con la entrada en vigencia del Código de Comercio, se estableció que cuando la Ley exija que un acto o contrato conste por escrito, bastará el instrumento privado con las firmas autógrafas de los suscriptores[60].

En relación con la atribución o autoría de un mensaje de datos requerida en la norma procesal, la Ley 527 de 1999 estableció que se entenderá que un mensaje de datos proviene del iniciador cuando ha sido enviado por: el propio iniciador, alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje o un sistema de información programado por el iniciador o en su nombre para que opere automáticamente[61]. Adicionalmente, el mensaje de datos se presume enviado por el iniciador cuando: haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador para establecer que el mensaje de datos provenía efectivamente de este, o el mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación

55. El artículo 244 del Código General del Proceso reza: ***"Es auténtico un documento 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 […]"***.

56. El artículo 252, numeral 2, del Código de Procedimiento Civil señaló: "[…] El documento privado es auténtico en los siguientes casos: […] 2. Si fue inscrito en un registro público a petición de quien lo firmó".

57. El artículo 40 del Código de Comercio regula: "Todo documento sujeto a registro, no auténtico por su misma naturaleza ni reconocido por las partes, deberá ser presentado personalmente por sus otorgantes al secretario de la respectiva cámara".

58. El artículo 252 del Código de Procedimiento Civil estableció: ***"[…] Se presumen auténticos los libros de comercio debidamente registrados y llevados en legal forma, el contenido y las firmas de pólizas de seguros y recibos de pago de sus primas, certificados, recibos, bonos y títulos de inversión en establecimientos de crédito y contratos de prenda con*** éstos, cartas de crédito, contratos de cuentas corrientes bancarias, extractos del movimiento de ***éstas y de cuentas con aquellos establecimientos, recibos de consignación y comprobantes de créditos, de débitos y de entrega de chequeras, emitidos por los mismos establecimientos, y los títulos de acciones en sociedades comerciales y bonos emitidos por estas, títulos valores, certificados y títulos de almacenes generales de depósito, y demás documentos privados a los cuales la ley otorgue tal presunción […]"***.

59. Decreto 019 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".

60. Artículo 826 del Código de Comercio.

61. Artículo 16 de la Ley 527 de 1999.

con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio[62].

De acuerdo con el Código General del Proceso, *"los documentos en forma de mensajes de datos se presumen auténticos"*[63]. La presunción de autenticidad se refiere a todas las características del mensaje de datos que se puedan establecer por el sujeto procesal que aporte la prueba. Es decir, la presunción puede abarcar los atributos de autenticidad, integridad y no repudiación siempre y cuando el formato de mensaje de datos se conserve original e incluya las características técnicas relacionadas con los mencionados atributos.

En el Código General del Proceso se establece que la simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos. Asimismo, dicho código complementa las reglas de interpretación establecidas en la Ley 527 de 1999 —en particular, el artículo 11— en relación con los criterios de valoración probatoria de los mensajes de datos. Esta norma permite al juez interpretar, bajo el criterio de la sana crítica, los medios de prueba allegados por las partes al proceso.

La conservación del formato original es la manera más técnica para allegar un mensaje de datos; no obstante, no es la única posible (ni debe serlo de manera obligatoria). Como supuesto fáctico se debe reconocer que en nuestro país la mayor parte de la población no tiene acceso a medios tecnológicos que permitan acudir a técnicas de computación forense para hacer valer sus pruebas en el ámbito judicial y arbitral. Frente a esta realidad evidente, el Legislador tomó partido en la norma demandada por referirse al formato específico del mensaje de datos cuando este es impreso.

Así pues, si bien la impresión de un mensaje de datos trae consigo una transformación del documento electrónico, esta alteración debida al cambio de formato no puede tener como consecuencia que el mensaje pierda el valor probatorio propio de los mensajes de datos ni tampoco debe afectar la equivalencia funcional con los documentos tradicionales. De ser así, sí se estarían modificando los artículos 5 y 10 de la Ley 527 de 1999 en cuanto al reconocimiento jurídico de los mensajes de datos y a la admisibilidad y fuerza probatoria de los mensajes de datos, respectivamente. Se debe recordar que el principio cardinal que establece la equivalencia funcional de los mensajes de datos con los documentos tradicionales es reconocido en nuestro ordenamiento jurídico desde la entrada en vigencia de la Ley 527 de 1999[64] y luego ratificado en las normas reglamentarias sobre firma electrónica y firma digital.

El Código General del Proceso reconoce que el mensaje de datos original, cuando es transformado a un formato impreso, debe ser valorado como cualquier otro documento. Es decir, la norma acusada no omite la obligatoriedad de valoración probatoria del documento electrónico por el juzgador ni desconoce que el mensaje de datos impreso constituye una transformación del original. Más aún, la redacción de la norma demandada habilita el uso de uno de los formatos del documento electrónico (el impreso) sin desconocer la obligación (propia del derecho constitucional del debido proceso) que tiene el juzgador de establecer su valor probatorio de acuerdo con las normas de interpretación procesal pertinentes.

62. El artículo 17 de la Ley 527 de 1999 reza: *"Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:*

- *Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o*
- *El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio".*

63. Inciso final del artículo 244 del Código General del Proceso.

64. Artículos 5, 6, 7 y 8 de la Ley 527 de 1999.

Cuando los comerciantes utilizan los mensajes de datos para sus actividades mercantiles, estos dejan de ser documentos comunes y corrientes y, al ser utilizados en el giro de actividades mercantiles, deben obligatoriamente conservarse; tal es el caso de la correspondencia y demás documentos relacionados con los negocios y las actividades mercantiles[65]. La Ley 527 de 1999 también hace referencia a que los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta[66]. Así pues, entre los papeles del comerciante se encuentra su correspondencia profesional, comercial, con fines mercantiles y de sus negocios. Evidentemente, no es el caso del uso de mensajería electrónica para propósitos privados o familiares que lleve a cabo un hombre o mujer de negocios.

En Colombia, el comerciante debe entonces dejar copia fiel de la correspondencia que dirija en relación con los negocios por cualquier medio que asegure la exactitud de la copia. Asimismo, se requiere que conserve la correspondencia que reciba en relación con sus actividades comerciales, con anotación de la fecha de contestación o de no haberse dado respuesta. Esta obligación proviene de la Ley Mercantil y abarca las actividades del comerciante respecto de su correspondencia[67].

La mencionada obligación legal de los comerciantes debe ser cumplida con el apoyo de los sistemas de información que permitan el almacenamiento y la retención de la correspondencia comercial. Ahora bien, la ley comercial no distinguió el formato o el medio en el que la correspondencia de actividades comerciales se lleva a cabo; lo importante es la finalidad mercantil y el uso en el giro de negocios por parte de los comerciantes. Es una carga de responsabilidad y diligencia en las actividades mercantiles y de negocios.

La correspondencia de los comerciantes puede ser examinada por las entidades que ejerzan supervisión, vigilancia y control (como las Superintendencias)[68], y su exhibición puede ser ordenada por

65. El artículo 19 (4) del Código de Comercio reza: "Es obligación de todo comerciante: 1) Matricularse en el registro mercantil; 2) Inscribir en el registro mercantil todos los actos, libros y documentos respecto de los cuales la ley exija esa formalidad; 3) Llevar contabilidad regular de sus negocios conforme a las prescripciones legales; 4) Conservar, con arreglo a la ley, la correspondencia y demás documentos relacionados con sus negocios o actividades; 5) Denunciar ante el juez competente la cesación en el pago corriente de sus obligaciones mercantiles, y 6) Abstenerse de ejecutar actos de competencia desleal".

66. El artículo 12 de la Ley 527 de 1999 reza: *"Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones: 1. Que la información que contengan sea accesible para su posterior consulta. 2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y 3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento. No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos. Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta".*

67. El artículo 54 del Código de Comercio reza: *"obligatoriedad de conservar la correspondencia comercial: El comerciante deberá dejar copia fiel de la correspondencia que dirija en relación con los negocios, por cualquier medio que asegure la exactitud y duración de la copia. Asimismo, conservará la correspondencia que reciba en relación con sus actividades comerciales, con anotación de la fecha de contestación o de no haberse dado respuesta".*

68. El artículo 61 del Código de Comercio reza: *"excepciones al derecho de reserva: Los libros y papeles del comerciante no podrán examinarse por personas distintas de sus propietarios o personas autorizadas para ello, sino para los fines indicados en la Constitución Nacional y mediante orden de autoridad competente. Lo dispuesto en este artículo no restringirá el derecho de inspección que confiere la ley a los asociados sobre libros y papeles de las compañías comerciales, ni el que corresponda a quienes cumplan funciones de vigilancia o auditoría en las mismas".*

autoridades judiciales o administrativas con funciones jurisdiccionales (de oficio o a petición de parte) de acuerdo con el Código General del Proceso y las demás áreas en que se aplican las normas probatorias establecidas en aquel.

En el campo penal, los mensajes de datos se consideran de manera expresa como elemento material probatorio[69]. De manera que, así como el ocultamiento, alteración o destrucción de un elemento probatorio es un delito de acuerdo con el Código Penal, lo mismo aplica para la mensajería electrónica. Para que exista este delito, además de la destrucción, alteración u ocultamiento como conductas materiales, el comerciante debe estar buscando evitar que el mensaje electrónico se utilice como medio cognoscitivo durante la investigación o como elemento probatorio durante el juicio[70].

Es decir que si la intención del comerciante es evitar que cierto mensaje de datos se utilice en una investigación penal, se podría constituir el delito sin importar que tal mensaje ya haya sido allegado o no como elemento material probatorio en el proceso. Los sistemas de información, archivo y retención de documentos deben tener en cuenta estas reglas y principios para evitar que directivos, empleados y contratistas incurran en responsabilidad civil, mercantil e incluso penal en caso de que por cualquier razón, de manera intencional o incluso involuntaria, modifiquen, alteren o destruyan la correspondencia comercial que sus empresas han llevado a cabo por medios electrónicos utilizando mensajes de datos y mensajería digital.

Los métodos de autenticidad e integridad contemplados por la Ley 527 de 1999, es decir, la firma electrónica y la firma digital, permiten a un mensaje de datos gozar de esos atributos más allá del ámbito procesal. La firma electrónica, en particular, tendrá la misma validez y efectos jurídicos que la firma si cumple con los requisitos establecidos en el artículo 3 del Decreto 2364 de 2012[71]. Esta clase de firmas son métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas, los cuales permiten identificar a una persona en relación con un mensaje de datos, siempre y cuando este 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[72].

Por otro lado, de acuerdo con la Ley 527 de 1999, la firma digital fijada en un mensaje de datos hace presumir la autenticidad y la integridad del contenido de este. El uso de una firma de este tipo tendrá la misma fuerza y efectos que el de una firma manuscrita si incorpora los siguientes atributos: 1. Unicidad o garantía de uso exclusivo por el firmante. 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.

69. Artículo 275, literal g, del Código de Procedimiento Penal.

70. Artículo 454, literal b, del Código Penal.

71. El artículo 5 del Decreto 2364 de 2012 reza: *"Efectos jurídicos de la firma electrónica. La firma electrónica tendrá la misma validez y efectos jurídicos que la firma, si aquella cumple con los requisitos establecidos en el artículo 3 de este decreto".*

72. El artículo 1 del Decreto 2364 de 2012 reza: *"[…] 3) Firma electrónica: 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".*

02

Contratos electrónicos e inteligentes

2.1. La contratación electrónica, entre el Código de Comercio y la Ley 527 de 1999

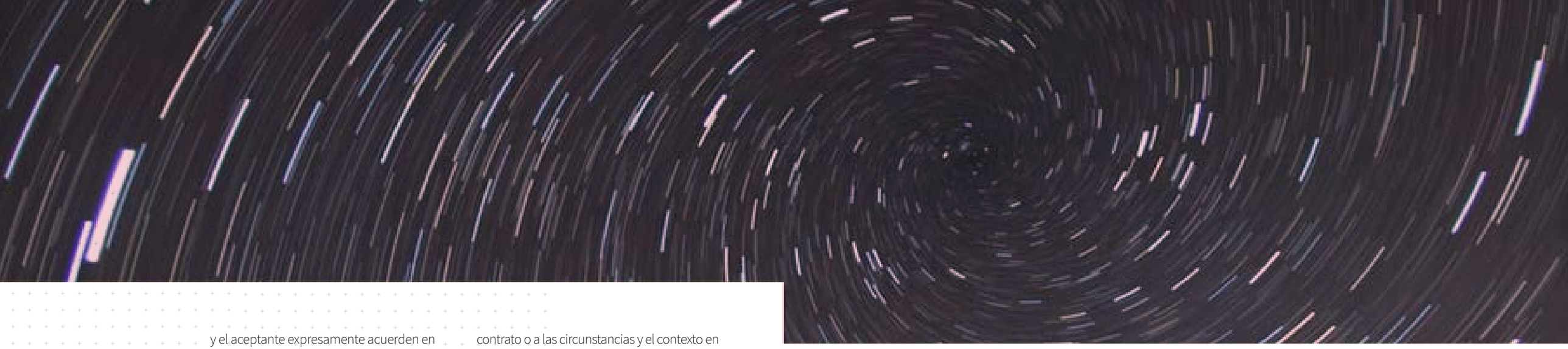
La velocidad de la trasmisión y el alcance casi universal han hecho que las comunicaciones electrónicas hayan dejado de ser una excepción para la contratación y más bien se hayan convertido en el medio más utilizado para expresar la intención y la voluntad. Así, con el paso del tiempo, internet y los mensajes de datos que circulan a través de la red global se convirtieron en nuevas formas utilizadas para la negociación, suscripción, celebración y ejecución de los contratos.

Ahora bien, las consecuencias de la ausencia física de los contratantes al contratar y la manera de expresar el consentimiento en el entorno digital han sido temas controversiales en la teoría del negocio jurídico por medios electrónicos. Al igual que la contratación en masa, el mercado digitalizado de productos y servicios contribuye al debilitamiento de la visión tradicional del contrato y, al mismo tiempo, a su rehabilitación social y económica con la función de organizar relaciones a distancia y con un ámbito internacional.

El artículo 2 del Código de Comercio establece que los comerciantes y los asuntos mercantiles se rigen por las disposiciones de la ley comercia [73]. En ese sentido, la Ley 527 de 1999, como ley que regula el comercio por medios electrónicos, se debe interpretar como parte de la ley comercial y como complemento del código, en un solo ordenamiento mercantil que se integra ante la necesidad de entender cabalmente el acto mercantil en el ecosistema digital.

La Ley 527 de 1999, en el capítulo III sobre comunicación de los mensajes de datos, incluye de manera expresa la posibilidad de que la oferta y la aceptación, como actos que permiten la formación del contrato, puedan ser expresadas por medio de mensaje de datos. En caso de que se lleve a cabo un cruce de oferta y aceptación por medios electrónicos, se entenderá celebrado un contrato salvo que el oferente

73. Artículo 2 del Código de Comercio reza: *"aplicación de la legislación civil: En las cuestiones comerciales que no pudieren regularse conforme a la regla anterior, se aplicarán las disposiciones de la legislación civil".*



y el aceptante expresamente acuerden en contrario. De manera aún más general para afirmar el carácter vinculante de los medios electrónicos en materia contractual, la Ley 527 de 1999 establece que no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Para el derecho privado tradicional, civil y comercial, la intención y la voluntad son pilares de los actos jurídicos ya que se partía de la visión utópica del equilibrio de fuerzas entre los sujetos de derecho en el tráfico económico y en el intercambio de bienes y servicios. El paradigma era el libre albedrío y la libertad de escogencia impoluta frente a relaciones entre iguales. Como corolario de lo anterior, en el Código Civil, al tenor del artículo 1502[74], las obligaciones entre sujetos de derecho, mediante un acto o declaración de voluntad, requieren como elemento estructural que las partes consientan o expresen su asentimiento a vincularse jurídicamente en dicho acto o declaración. Además, a la luz del artículo 1618 del mismo código, la regla fundamental para la interpretación de los contratos es la búsqueda de la intención común de los contratantes[75]. Este principio supera a cualquier otro en la actualidad por la práctica en el foro judicial y arbitral, siendo este referido al tenor literal del contrato o a las circunstancias y el contexto en que se llevó a cabo la relación contractual.

Con el Código de Comercio, los principios que gobiernan la formación de los actos y contratos y las obligaciones de derecho civil, sus efectos, interpretación, modo de extinguirse, anularse o rescindirse también eran aplicables a las obligaciones y negocios jurídicos mercantiles. Es decir, el consentimiento se podía expresar con libertad y sin mayor límite en cuanto a su modalidad y forma. Esto fue ratificado expresamente más adelante en el mismo código al considerar que los comerciantes podrán expresar su voluntad de contratar u obligarse verbalmente, por escrito o por cualquier modo inequívoco.

En el siglo XX, las actividades comerciales e industriales, con diversas formas de mecanización de sus procesos y la masificación de los medios de comunicación social, demostraron que el mercado no era una panacea, sino más bien el escenario de conflictos y confrontación de intereses entre grandes poderes empresariales y consumidores o usuarios; estos últimos más bien sometidos a una gran asimetría de poder económico. Con la Cuarta Revolución Industrial en ciernes, se anticipa que los datos y la información personal son la base de la utilización de algoritmos que permiten la publicidad y el mercadeo con perfiles que predicen, analizan e incluso manipulan la publicidad para influenciar los gustos y hábitos, en muchos casos con intrusión a la vida privada. Los algoritmos pueden servir para manipular la información, para privilegiar un contenido respecto de otro por razones comerciales o por el pago de publicidad que afecten la transparencia de las búsquedas de contenidos digitales.

Con el derecho de los mercados, materia con varias facetas y perspectivas, entre los cuales el derecho del consumo y el derecho de la competencia ocupan un lugar preponderante, el ordenamiento jurídico responde a la velocidad de la transacción, a la eficiencia en el intercambio de bienes y servicios, a la automatización en la decisión y a la era de la información o de la desinformación —por las noticias falsas, los *influencers* pagados para presentar información exagerada o falsa y las suplantación de identidad personal y corporativa, entre otros—. El nuevo arsenal jurídico permite fijar reglas de juego que permiten soñar de nuevo con la utopía de relaciones en equilibrios económicos renovados y de mayor control en la utilización de la información de los individuos y consumidores. Lo ideal es que de este modo se permita un libre ejercicio de la autonomía e iniciativa privada y que tales relaciones se enmarquen en principios de justicia social y contractual, así como de la buena fe como elemento integrador del negocio jurídico por medios electrónicos.

La expresión de la voluntad en el entorno digital se degrada aún más en su relevancia jurídica y social, por ejemplo, cuando se interpreta que la simple navegación en una página web o la utilización de una aplicación constituyen consentimiento válido, suficiente y eficaz. Los términos y condiciones de uso de los recursos informáticos son el contrato —o declaración unilateral— más usual con el fin de definir los derechos y deberes de los proveedores de bienes y servicios en el entorno digital, así como de los consumidores y usuarios. El contrato por medios electrónicos es ahora la forma usual de llevar a cabo la fase previa, la celebración y la ejecución de las relaciones jurídicas, económicas y sociales.

74. Artículo 1502 del Código Civil.

75. Artículo 1602 del Código Civil

2.2 La declaración de voluntad en el comercio electrónico

La forma —apariencia exterior, signos externos y ropaje exterior— es elemento del negocio jurídico no solo por el mandato legal que así lo especifique, sino además porque permite, a través del contrato, que sea perceptible por los sentidos. No se debe confundir la forma con el contenido esencial del negocio, que es el que enumera y describe la declaración de voluntad y de la intención de las partes como tales. Por un lado, el contenido del negocio jurídico, cuyo objeto define su alcance, se expresa por la forma utilizada por los contratantes. Por otro lado, en la forma se centra la actividad encaminada a cumplir las formalidades, si fuera el caso, o a probar la existencia del negocio jurídico con el fin de cumplir la carga probatoria establecida por el ordenamiento legal.

En el derecho moderno de las obligaciones y los contratos se evidencia la fuerza determinante del principio del "consensualismo", que corresponde al antiguo adagio ***solut*** consensus ***obligat***[76], según el cual dentro de las condiciones esenciales para la formación, validez y existencia de los contratos no se encuentran per se las exigencias de forma, sino que únicamente deben concurrir las capacidades de las partes para expresar el consentimiento sin vicio alguno, el objeto o propósito y la causa lícitos[77].

En las actividades mercantiles, *"los comerciantes podrán expresar su voluntad de contratar u obligarse verbalmente, por escrito o por cualquier modo inequívoco. Cuando una norma legal exija determinada solemnidad como requisito esencial del negocio jurídico, este no se formará mientras no se llene tal solemnidad"*[78]. Los medios electrónicos pueden equivaler a la forma escrita siempre y cuando sean accesibles para su posterior consulta y también pueden calificarse como un modo inequívoco y concluyente en el que se expresa la voluntad de los contratantes[79], por ejemplo, por la utilización reiterada en las comunicaciones relacionadas con una actividad mercantil o una negociación de un correo electrónico o de una página ***web*** o de la plataforma tecnológica para intercambios comerciales. También puede considerarse como una actividad de omisión, pasiva o de silencio que tiene valor negocial, como en el caso de que la falta de acuse de recibo de un mensaje de datos pueda tener alguna consecuencia desde la óptica contractual.

El principio de "la libertad de forma" es predominante en relación con el contrato y el negocio jurídico por el cual las partes pueden expresar su consentimiento respecto a un contrato que pretenden celebrar y, desde luego, respecto del contenido de este por cualquier medio idóneo. Así mismo, desde el punto de vista probatorio existe la libertad de medios probatorios para probar los contratos y las obligaciones. La libertad probatoria es plena respecto de los contratos consensuales. Por el contrario, *"el contrato solemne no tiene existencia jurídica sino desde que se cumple la formalidad externa que la Ley exige para su perfección; ni siquiera la voluntad de las partes contratantes para un caso particular tan fundamental principio"*[80].

El uso masivo de las tecnologías de la información y las comunicaciones TIC y del comercio electrónico ha transformado el ritmo de las actividades mercantiles, generando la aparición de nuevos agentes del mercado. Se han disminuido las barreras de entrada en la oferta de bienes y servicios a escala internacional, y a su vez los modelos de negocio del e-commerce menoscaban la protección tradicional de los consumidores y usuarios. Para esto, es necesario que el derecho de los mercados garantice la confianza y el equilibrio en el entorno digital que conlleva la oferta mercantil en tiendas, establecimientos de comercio y plataformas virtuales a distancia y sin la posibilidad de tener contacto con los productos. Así mismo, la automatización de conductas y actividades y la desmaterialización de los documentos mercantiles, incluyendo la celebración de los contratos electrónicos, la suscripción de títulos valores por medios electrónicos y la aceptación del contenido de estos, tienen como antesala la expresión del consentimiento libre, expreso y voluntario, como ha sido tradicional.

76. .Este adagio surge como resultado de un proceso de evolución en el que el juramento propio de los actos jurídicos en la Edad Media se debilita por influencia del derecho canónico y de la Iglesia católica para evitar que los fieles juraran en falso. Cfr. Peña Valenzuela (2015).

77. El artículo 1502 del Código Civil reza: *"Requisitos para obligarse: […] 2.*°) que consienta en dicho acto o declaración y su consentimiento no adolezca de vicio. 3.o) que recaiga sobre un objeto lícito. 4.°) que tenga una causa lícita".

78. Artículo 824 del Código de Comercio.

79. Artículos 1298 y 2150 del Código Civil y 854 del Código de Comercio

80. Corte Suprema de Justicia, Sala de Casación Civil, Sentencia de 5 de julio de 1983.

La utilización de medios electrónicos para expresar la voluntad de obligarse y el libre consentimiento respecto de un contrato es un ejemplo de la libertad que existe para escoger la forma más adecuada para exteriorizar la intención de celebrar un contrato. La Cámara de Comercio de Bogotá, con el apoyo de la línea de investigación de derecho comercial de la Universidad del Rosario, llevó a cabo un estudio de validez a las 78 costumbres mercantiles certificadas. Entre las que correspondían al sector informático se certificó que: *"en Bogotá, D. C., es costumbre mercantil que todo visitante de un sitio de internet o una página web, por el hecho de navegar en la misma, se obliga a respetar los términos y condiciones sobre su uso, contenidos y normas de propiedad intelectual"*[81].

De manera expresa, la Ley 527 de 1999, que complementa las disposiciones del Código de Comercio, reconoce que *"en la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos"*[82]. Esta norma actualiza las normas del Código de Comercio sobre contratación entre ausentes[83]. Así pues, los mensajes de datos son suficientes como medio para que una oferta y su aceptación se entrecrucen y formen un contrato válido y existente. El cumplimiento de formalidades puede ser necesario, de manera excepcional, si el ordenamiento jurídico así lo establece para el nacimiento o extinción de los derechos o para probar dicha oferta o aceptación. De hecho, un contrato solemne es el que requiere el cumplimiento de una formalidad determinada para su existencia ***(ad substantiam actus)***, validez ***(ad validitatem)*** y oponibilidad o prueba ***(ad probationem)***. La Ley de Comercio Electrónico, de manera general, se refiere a que ***"en las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos"***[84]. Este reconocimiento del valor de los mensajes de datos no se limita al ámbito contractual mercantil, sino que también incluye los contratos de consumo. Es decir, en cualquier relación jurídica —incluyendo las de naturaleza civil, de consumo y las mercantiles— se debe reconocer la fuerza y eficacia de los mensajes de datos.

81. Cámara de comercio de Bogotá. (2019). Recuperado de https://www.ccb.org.co/Transformar-Bogota/Costumbre-Mercantil/Listado-de-Costumbres-Mercantiles.

82. Artículo 14 de la Ley 527 de 1999.

83. Artículos 850 y 851 del Código de Comercio. El artículo 850 reza: *"propuesta verbal: La propuesta verbal de un negocio entre presentes deberá ser aceptada o rechazada en el acto de oírse. La propuesta hecha por teléfono se asimilará, para los efectos de su aceptación o rechazo, a la propuesta verbal entre presentes".* El artículo 851 reza: *"propuesta escrita: Cuando la propuesta se haga por escrito deberá ser aceptada o rechazada dentro de los seis días siguientes a la fecha que tenga la propuesta, si el destinatario reside en el mismo lugar del proponente; si reside en lugar distinto, a dicho término se sumará el de la distancia".*

84. Artículo 14 de la Ley 527 de 1999

No puede entenderse que, para efectos de los contratos celebrados o ejecutados por medios electrónicos, la inclusión de la firma electrónica o la firma digital sean formalidades ***ad substantiam*** o ***ad probationem*** que deben ser cumplidas so pena de alguna sanción jurídica de invalidez, inexistencia o inoponibilidad del negocio jurídico. Es lo contrario: cuando en el ordenamiento jurídico se exige como formalidad la inclusión de la firma de las partes, tal requisito se puede cumplir en el mundo digital por un medio equivalente, sea la firma electrónica o la firma digital. En el mismo sentido, la Ley 527 de 1999, al establecer el contrato por medios electrónicos, ratifica "la libertad de formas" como muestra de la predominancia del principio del consensualismo y reitera de manera expresa que los mensajes de datos son medios idóneos y aptos —complementarios a los tradicionales— para expresar la voluntad negocial. La Ley 527 de 1999 trae consigo la consagración expresa de la equivalencia del mensaje de datos a funciones jurídicas "formalistas" como el "escrito", "original" y "firma" y, por ende, reconoce la persistencia del formalismo dentro del derecho actual, pero busca atenuar posibles consecuencias adversas e inesperadas para las partes que utilizan el entorno digital.

El contrato electrónico se celebra por el mero acuerdo de voluntades expresado mediante medios electrónicos. Como excepción a esta regla, la Ley 527 establece la posibilidad que tienen las partes de acordar como condición para la formación del contrato la recepción del acuse de recibo. La aceptación constituye la consumación de un negocio jurídico con consecuencias jurídicas que pueden ser importantes, por lo que la voluntad de obligarse por parte del aceptante debe existir claramente. Deben concurrir tanto la voluntad de consentir en el negocio jurídico específico como la de exteriorizar el querer interno para el perfeccionamiento del negocio.

La contratación electrónica obedece a la regla medular del derecho mercantil según la cual las estipulaciones de los contratos válidamente celebrados preferirán a las normas legales supletivas y a las costumbres mercantiles[85]. En el caso de los mecanismos de autenticidad e integridad, también se privilegia al acuerdo de las partes ya que, salvo prueba en contrario, se presume que cualquiera de estos mecanismos, que decidan utilizar las partes mediante acuerdo, cumplen los requisitos de firma electrónica[86].

85. El artículo 4 del Código de Comercio reza: *"preferencia de las estipulaciones contractuales: Las estipulaciones de los contratos válidamente celebrados preferirán a las normas legales supletivas y a las costumbres mercantiles".*

86. El artículo 8 del Decreto 2364 de 2012 reza: *"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, entre otros, los siguientes factores: 1) El concepto técnico emitido por un perito o un órgano independiente. y especializado. 2) La existencia de una auditoría especializada, periódica e independiente sobre los procedimientos, métodos o dispositivos electrónicos que una parte suministra a sus clientes o terceros como mecanismo electrónico de identificación personal".*

2.3 La declaración de voluntad en la contratación inteligente (smart contracts)

La transición de los contratos electrónicos a los contratos inteligentes constituye una etapa en la evolución de la contratación electrónica, y no es una ruptura y mucho menos avizora la destrucción del concepto o el final de la noción de contrato. Por el contrario, un ***smart contract*** se debe apreciar teniendo en cuenta elementos tradicionales del negocio jurídico como, por ejemplo, la forma, el consentimiento y la prueba.

La contratación inteligente, como la contratación web, tiene como base la autonomía privada y el énfasis de esta última en la libertad de las partes para definir los términos y condiciones de la contratación electrónica. Esto marca entonces un renacimiento del contrato, más que su ocaso. Precisamente, frente a las discusiones respecto de la eficacia de la regulación de la economía digital en sus distintas facetas, es claro que el contrato —independientemente si es denominado contrato web o contrato inteligente— es el instrumento más utilizado y eficaz para las partes.

La inquietud surge respecto de la abstracción que introducen los contratos inteligentes. Es cierto que la influencia de los algoritmos en temas como las búsquedas de internet y la publicidad digital había generado ya esta discusión en otras áreas del derecho. En todo caso, no parece creíble que los contratos inteligentes traigan consigo una pérdida absoluta del monopolio jurídico en materia contractual para dar paso a un nuevo poder en cabeza de programadores y científicos de datos. Más bien se propugna por un diálogo entre abogados y programadores y arquitectos de los sistemas de información para lograr afinar ese punto de convergencia que es la contratación inteligente. En esa medida se aprecia un movimiento académico encaminado a introducir en los programas de formación de los abogados la programación de sistemas de información y el estudio de los lenguajes informáticos adecuados para tal fin. La inclusión de términos legales mediante códigos informáticos parece ser una síntesis afortunada de la evolución del contrato para satisfacer las necesidades de la economía digital. De igual forma es importante resaltar que la evolución del contrato obedece a los cambios tecnológicos y a los nuevos modelos de negocios.

Con ***blockchain*** se experimenta una transformación de la red de transferencia de paquetes de información digital a una red de transacciones y valor. Así, del internet se han apropiado en buena medida las empresas para actividades comerciales, lo cual no es sorprendente por el poder de generación de riqueza de la red y de la economía digital.

Otra perspectiva marca la evolución de los términos y condiciones como contrato más utilizado y usual en internet definiendo una etapa de la red para la distribución de contenidos y para su monetización y la novedad de las instrucciones codificadas y automatizadas en los contratos inteligentes. Estos últimos se debaten de manera pendular entre su posible interpretación como código que se autoejecuta o como instrucciones que se cumplen de manera automática. De manera

preliminar, parecería que ambas caracterizaciones de los ***smart contracts*** son válidas. El punto de quiebre que les da un puesto en el mundo de los contratos y que también se puede comparar en una evolución de ambos es la consolidación de la fuerza del internet con la masificación de las páginas ***web*** y —un poco más tarde— de las aplicaciones móviles. Así mismo, podría señalarse que la fuerza motora inicial de los contratos inteligentes es la aparición de múltiples y variados modelos de criptomonedas como aplicaciones de ***blockchain***. En ese sentido, no debe olvidarse que el efecto disruptivo de ***blockchain*** obedece a la posibilidad de flexibilizar su características, arquitectura y programación.

En definitiva, se observa que los contratos ***web*** aceleraron la aparición y consolidación de la contratación electrónica como nueva categoría de los contratos. El telón de fondo de ese desarrollo fue la masificación de la red global internet y, en particular, de la ***World Wide Web*** o www. Por su parte, la contratación inteligente tiene como base ***blockchain*** que, como tecnología convergente, cuenta con una base de datos universal con la combinación de los hash para la integridad, PKI (clave pública y privada) para encadenar los bloques y la descentralización de los registros a escala de los nodos ***(distributed ledger)***. La flexibilidad de esta tecnología en cuanto a diversidad y alternativas en diseño del sistema de información presenta unas características específicas. Por ejemplo, en el caso de las criptomonedas, las cadenas de bloques se adecuan a las condiciones de intercambio de valor en un círculo cerrado pero a la vez distribuido —sobre todo ***bitcoin***—.

En el caso de la ***forma del contrato***, es importante comparar ambas categorías. Los contratos ***web*** aparecen vinculados a las páginas ***web*** y luego a las aplicaciones y plataformas. La presentación o publicación electrónica de los términos y condiciones expresados en lenguaje alfanumérico constituyeron la principal novedad en cuanto a la forma. Comenzó la desmaterialización del contrato.

Por otra parte, la forma de los contratos inteligentes se determina por la manera como se define la arquitectura de los bloques y de

su encadenamiento. De este modo se continúa la desmaterialización de la forma del contrato y, además, su misma presentación, cambiando el lenguaje tradicional hacia lenguajes matemáticos y de programación.

El *consentimiento* en los contratos web genera el dilema —aún no resuelto en muchos países— entre los contratos que requieren una conducta específica o asentimiento expreso, definido como ***click-wrap agreement***, y el consentimiento basado en la mera navegación en la página o en la utilización de la herramienta, esto es, ***browse-wrap agreement*** (contratos por navegación). Esta división ha generado una jurisprudencia muy prolífica en los Estados Unidos que ha oscilado reconociendo validez y efectos a ambas formas de expresión del consentimiento.

En los contratos inteligentes la automatización tiende a disminuir aún más la función cardinal del consentimiento como expresión de la voluntad de los sujetos del negocio jurídico. Sin embargo, las partes deben ponerse de acuerdo en todo caso respecto de las condiciones, obligaciones o supuestos que van a ser codificados en el contrato inteligente, es decir, si existe consentimiento respecto de la base legal que va a convertirse en instrucciones en código informático. Es posible que este escenario cambie como consecuencia de la combinación del blockchain y el machine learning en el sentido de que las máquinas inyectadas con miles de millones de datos puedan tomar decisiones por sí solas. En ese caso el consentimiento y la expresión volitiva dejarán de ser una condición eminente del ser humano.

El ***blockchain*** y los ***contratos inteligentes*** convergen respecto de la integridad y la autenticidad inherentes a sistemas de información. La fuente de confiabilidad probatoria de blockchain está en la base de este sistema de información que parte de la criptografia, de los ***hash*** y de la firma digital y electrónica con el sistema dual de claves pública y privada. El encadenamiento de los bloques depende de la autenticación plena, así como de la integridad y el no repudio. La columna vertebral del ***blockchain*** está garantizada por el reconocimiento de los mensajes de datos en sus efectos probatorios y contractuales, así como en los equivalentes funcionales.

Otra tecnología disruptiva que puede hacer más eficaz la contratación es la inteligencia artificial con elementos como los algoritmos, las redes neuronales y los agentes inteligentes que pueden influenciar el consentimiento antes de su formación. Los ***botnets*** permiten un servicio al cliente personalizado con la interacción frente a sistemas de información alimentados por volúmenes gigantescos de datos que anticipan y predicen tendencias de consumo.

El aporte fundamental del derecho respecto de la tecnología es la confianza. Esta se debe recobrar con instrumentos jurídicos que apoyen la gestión de riesgos tecnológicos. Los contratos ***web*** no lograron ese fin de manera completa, pero los ***smart contracts*** pueden ser un avance significativo porque precisamente son una síntesis entre la tecnología y el derecho que permite una confianza absoluta respecto de su celebración y ejecución.

Conclusiones

1.

La categoría jurídica de los mensajes de datos es la base del modelo de reglas jurídicas del comercio electrónico de acuerdo con la CNUDMI, que se introdujo en el ordenamiento jurídico colombiano mediante la Ley 527 de 1999.

2.

Con la Ley 527 de 1999 se irradió de manera paulatina el valor jurídico del mensaje de datos, así como los requisitos de existencia, validez y oponibilidad de los documentos electrónicos.

3.

La equivalencia funcional es el principio cardinal para lograr el vínculo-puente entre los hechos, los documentos, los actos y los negocios jurídicos tradicionales del mundo analógico y los mensajes de datos, los documentos electrónicos y los registros en línea.

4.

La confiabilidad despunta como un requerimiento técnico reconocido por el derecho para valorar los mecanismos de autenticidad e integridad vinculados a un mensaje de datos.

5.

Las firmas electrónicas y digitales son mecanismos de autenticidad e integridad que aseguran la confiabilidad técnica de los documentos electrónicos atribuyendo la autoría y la trazabilidad de cambios en su contenido.

6.

La prueba de los hechos se respalda en la masificación de dispositivos electrónicos que permiten la creación, transmisión y almacenamiento de mensajes de datos y compartirlos.

7.

Los mensajes de datos se han convertido en el medio más utilizado para expresar y evidenciar los hechos que ocurren en el día a día de las personas y las entidades, así como el vehículo de la expresión de voluntad o de la intención.

8.

La formación de los contratos se lleva a cabo por medios electrónicos, sea por el intercambio de oferta y aceptación o por procesos de negociación a través de plataformas, redes sociales, aplicaciones o páginas ***web***.

9.

La contratación electrónica está originalmente vinculada a textos tradiconales, términos y condiciones presentados y publicados en páginas ***web***. De manera paulatina, la celebración y ejecución se automatiza mediante algoritmos.

10.

La autonomía privada permite la autorregulación de intereses en ***blockchain*** y contratos inteligentes en el marco del respecto del orden público y en cumplimiento del principio de buena fe.

11.

La contratación inteligente permite aplicar técnicas algorítmicas, de inteligencia artificial, con analítica de datos en todas las etapas del contrato, en la fase de consentimiento y declaración de voluntad, así como en la ejecución y cumplimiento de las ejecuciones incluidas en este.

12.

La aplicación del modelo legislativo de la CNUDMI a los registros descentralizados de ***blockchain*** demuestra la neutralidad tecnológica, es decir, la capacidad de la adaptación de un concepto general como es el mensaje de datos a nociones propias de tecnologías disruptivas.

Bibliografía

Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005).

Peña Valenzuela, Daniel (2015). ***De la firma manuscrita a las firmas electrónica y digital***. Universidad Externado de Colombia.

Jurisprudencia

Congreso de Colombia. (27 de marzo de 1971). ***Código de Comercio (Decreto 410 de 1971)***. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/codigo_comercio.html.

Congreso de Colombia. (21 de agosto de 1999). ***Ley de Comercio Electrónico (Ley 527 de 1999)***. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html#10.

Código de Procedimiento Penal. (2004). Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html.

Corte Suprema de Justicia, Sala de Casación Civil. (16 de diciembre de 2010). ***Sentencia 2004-01074***. Magistrado Ponente: Pedro Octavio Munar.

Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (2011). Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html#PARTE%20PRIMERA.

Presidencia de la República de Colombia – Departamento Administrativo de la Función Pública. (10 de enero de 2012). ***Decreto 019 de 2012, "por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública"***. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/decreto_0019_2012.html.

Código General del Proceso. (2012). Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html.

Presidencia de la República de Colombia – Ministerio de Comercio, Industria y Turismo. (22 de noviembre de 2012). ***Decreto 2364 de 2012, "por el cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones"***. Recuperado de: http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/NOVIEMBRE/22/DECRETO%202364%20DEL%2022%20DE%20NOVIEMBRE%20DE%202012.pdf.

Leyes modelo

Ley Modelo de la CNUDMI sobre documentos transmisibles electrónicos (2017).

Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001).

Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996).

Guías legislativas y recomendaciones

CNUMDI (1985). ***Recomendaciones dirigidas a los Gobiernos y a las organizaciones internacionales acerca del valor jurídico de los registros de computadora*** (1985).

Textos explicativos

CNUMDI (2007). ***Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas*** (2007).

VARIACIONES SOBRE LAS FIRMAS ELECTRÓNICAS, FIRMAS DIGITALES Y TEMAS AFINES

VARIATIONS ABOUT ELECTRONIC SIGNATURES, DIGITAL SIGNATURES AND RELATED THEMES.

Rodrigo Puyo Vasco

Resumen:

Este artículo reseña la permanencia de viejos y nuevos problemas en las normas sobre firmas digitales y, en general, firmas electrónicas. Así mismo, señala los principales pronunciamientos judiciales sobre las leyes que regulan la materia. Igualmente, estudia las más relevantes reglas legales sobre las firmas, así como los aspectos de validez transfronteriza de las normas y, finalmente, contiene unas críticas sobre la materia.

Palabras clave: firma electrónica; firma digital; equivalencia funcional; documento electrónico; entidades de certificación; acreditación; Ley 527 de 1999; validez transfronteriza.

Abstract:

This article reviews the permanence of old and new problems within the rules regarding Digital Signatures, and, in general, Electronic Signatures. Likewise, it points out the main judicial rulings about the laws regulating the matter. It also studies the most relevant rules on signatures, cross border validity of those laws, and finally, it contains, some critics on the subject.

Introducción:

La celebración de los veinte años de la Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico, de las firmas digitales y de las entidades de certificación, nos revela la presencia de antiguos y nuevos problemas jurídicos de estas instituciones. Algunos de ellos han sido resueltos en forma parcial, y en otros subsisten controversias sin resolver, fruto en buena parte de la novedad de esta legislación, de la aparición del mundo de las tecnologías, de su naturaleza transversal e instrumental en el mundo jurídico y de su innegable vocación global, que impide soluciones locales aisladas del contexto internacional.

Dentro de las variopintas dificultades de orden normativo en la materia se encuentran: la falta de unidad en el concepto de firma electrónica, ya sea simple, certificada, avanzada o *digital*; la referencia a una predicada neutralidad tecnológica, que muchas veces no se cumple y en otras aparece inconveniente en lo jurídico y alejada de la realidad; las imprecisiones entre las nociones de autoridad de registro y de certificación; la reciente noción de acreditación de los terceros de confianza independientes que sirven de fedatarios de las firmas, es decir, las entidades de certificación, y la ausencia de marcos jurídicos generales internacionales que en un mundo de comercio global sirvan para otorgar un mínimo de seguridad legal en las transacciones, dentro de un dinámico marco de derecho internacional privado[87], entre otras.

Como adelante se analizará, en unas reflexiones sobre las firmas electrónica y digital, las normativas nacionales no están exentas de estas dificultades, a la par que es evidente la ausencia de una mayor y necesaria reglamentación legal nacional que complemente la expedida en 1999 y el Decreto 019 de 2012, así como las normas concordantes de los códigos generales del proceso y del contencioso administrativo en relación con los documentos electrónicos y su función como medios probatorios legales y el marco vigente que autoriza adelantar procesos judiciales por la vía informática con plena validez.

De la Ley 527 de 1999

En un esfuerzo por estar al día con los progresos legales generados por la revolución tecnológica de las comunicaciones, con acierto el Estado colombiano acogió el texto de la ley modelo elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). El texto de esta normativa quedó incluido en la Ley 527 de 1999.

Esta ley está dividida en cuatro grandes capítulos en referencia a los temas de este análisis.

I. El primero relativo a los menajes electrónicos de datos y al comercio electrónico.
II. El segundo sobre las firmas digitales.
III. El tercero trata los aspectos referidos a las entidades de certificación.

87. Un ejemplo de estas normas es el eIDAS (***Electronic Identification and Signature***), Reglamento Europeo 910/2014, cuya vigencia inició en julio de 2016 y que reguló la identificación electrónica para los servicios de confianza relativo a las transacciones electrónicas en la Unión Europea. Este reglamento se convierte en el modelo que se debe seguir para lograr un estándar internacional, bajo un modelo de interoperabilidad con una misma base técnica, los certificados de firma electrónica avanzada o digital, y una misma base normativa, Ley Marco de Firma Electrónica de la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional, adoptada por más de 140 países. Después de más de dos décadas de existencia de la Ley Marco de Firma Electrónica se hace necesario, en un contexto comercial global, interoperar digitalmente con cualquier país, objetivo común para el cual solo existe un condicionamiento en la actualidad: contar con una misma base normativa de ***e-commerce,*** esto es, haber adoptado la Ley Marco de Firma Electrónica. país, objetivo común para el cual solo existe un condicionamiento en la actualidad: contar con una misma base normativa de ***e-commerce,*** esto es, haber adoptado la Ley Marco de Firma Electrónica.

I. El último estudia la admisibilidad y fuerza probatoria de los mensajes de datos.

En relación con los mensajes de datos, estos fueron definidos en el artículo 2, literal b, de la ley como: "La información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pueden ser, entre otros, el intercambio electrónico de datos EDI, el correo electrónico, el telegrama, el télex o el telefax […]". Esta es la base de la construcción del entramado legal de que trata la ley, pues finalmente es el documento de naturaleza electrónica de contenido jurídico lo que da origen a toda la reflexión reglamentaria que surge de la aparición de un nuevo medio de transmisión o, mejor, de la inclusión de contenidos con consecuencias legales, diferentes a la palabra o al tradicional medio físico o papel, y que se convierten en la principal herramienta que tiene como base el mundo informático.

Por su parte, las entidades de certificación serán personas jurídicas públicas o privadas que emitan certificados, en relación con las firmas electrónicas o digitales, sobre la integridad de los mensajes[88]. Para ese fin, estas entidades deben cumplir requerimientos y encontrarse acreditadas por el Organismo Nacional de Acreditación (ONAC), antes la Superintendencia de Industria y Comercio, erróneamente trasladada esa función al órgano mencionado. De igual forma, estos organismos deben contar con capacidad económica y técnica para la emisión y conservación de certificados sobre la autenticidad de las firmas digitales.

Por último, la Ley 527 de 1999 les otorga validez probatoria a los mensajes de datos en forma similar o equivalente a los documentos físicos, y se entenderán firmados los mensajes, cuando se exija esta formalidad, si se ha utilizado un método que: (i) permita identificar el iniciador del mensaje y su conformidad con el contenido, y (ii) sea confiable para el propósito deseado. Si se exige que sea original, debe haber garantía de su integridad, si puede ser mostrado a la persona a la que se debe presentar. Su fuerza probatoria está en concordancia con lo prescrito en el Código General del Proceso, artículos 244 y concordantes.

88. Artículo 160 del Decreto 019 de 2012, que modifica el artículo 26 de la Ley 527 de 1999: *"ARTÍCULO 160. CARACTERÍSTICAS Y REQUERIMIENTOS DE LAS ENTIDADES DE CERTIFICACIÓN. El artículo 29 de la Ley 527 de 1999, quedará así: "Artículo 29. Características y requerimientos de las entidades de certificación. Podrán ser entidades de certificación. las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que cumplan con los requerimientos y sean acreditados por el Organismo Nacional de Acreditación conforme a la reglamentación expedida por el Gobierno Nacional. El Organismo Nacional de Acreditación de Colombia suspenderá o retirará la acreditación en cualquier tiempo, cuando se establezca que la entidad de certificación respectiva no está cumpliendo con la reglamentación emitida por el Gobierno Nacional. con base en las siguientes condiciones:*

1.1. Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;

1.2. Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley;

1.3. Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo periodo que la ley penal o administrativa señale para el efecto".

01

Discusiones sobre la validez constitucional de los mensajes de datos y la firma digital y su régimen

En este sentido han sido varios los pronunciamientos de la Corte Constitucional y del Consejo de Estado. Entre los más destacados se encuentra la ***Sentencia de la Corte Constitucional C622 de 2000.*** Esta sentencia es de gran transcendencia pues analizó la demanda que se oponía a la Ley 527 de 1999 toda vez que los interesados consideraban en su declarativa de inexequibilidad que se invadía el campo de los notarios como únicos depositarios de la fe pública. Además, se argumentaban tecnicismos propios en el trámite congresional al darle categoría de ley estatutaria y por tanto exigir un trámite especial.

La Corte Constitucional negó las pretensiones al no aceptar la exclusividad notarial en el monopolio de la fe pública y tampoco considerar vulnerados los reglamentos del trámite de la iniciativa legal. Así, después de realizar un prolijo examen sobre la novedosa legislación, se pronunció sobre dos temas fundamentales:

a. Ratificar la ***equivalencia funcional del documento electrónico***, previo el cumplimiento de los requisitos consagrados en la ley, al documento sobre papel, lo cual se ha convertido en el más importante respaldo jurídico al mundo jurídico que utiliza los medios electrónicos.
En este sentido dijo la Corte:

*En conclusión los **documentos electrónicos** están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez especialmente con respecto a la identificación del origen y conten ido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la Ley.*

b. Aceptar la ***firma digital***, es decir, aquel valor alfanumérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido o vinculado a la clave criptográfica del iniciador, permite determinar que se ha obtenido exclusivamente con la clave criptográfica del iniciador y que el mensaje no ha sido modificado después de efectuada la transformación (artículo 2, literal C).
Al respecto la Corte expresó:

A través de la firma digital se pretende garantizar que un mensaje de datos deter-

minado proceda de una persona determinada, que ese mensaje no hubiera sido modificado desde su creación y trasmisión y que el receptor no pudiera modificar el mensaje recibido […] Concluyendo, es evidente que la trasposición mecánica realizada sobre papel y replicada por el ordenador a un documento informático no es suficiente para garantizar los resultados tradicionalmente asegurados por la firma autógrafa, por lo que se crea la necesidad de que ***existan establecimientos*** *que certifiquen la validez de esa firma. Por tanto, se crea la necesidad de que existan establecimientos que certifican la validez de las firmas.*

Esta opinión judicial del más alto tribunal constitucional otorgó certeza y fundamentación a la ***firma digital*** entre nosotros.

Una segunda sentencia de la Corte Constitucional, la C831 del año 2001, de menor trascendencia y complementaria de la anterior, se refirió a una demanda que argumentaba la inconstitucionalidad de la ley al referirse su artículo 6 a todo tipo de información en los mensajes de datos, debiendo estar circunscrita, según la demanda, a los temas mercantiles, pues en caso contrario estaría en contradicción con el artículo 28 superior. Esta demanda tampoco tuvo una decisión favorable.

Posteriormente fueron demandadas las normas del Decreto 019 de 2012, llamado antitrámites, en sus artículos 161, 162 y 163, sobre entidades de certificación, lo cual fue resuelto mediante la Sentencia 219 de 22 de abril de 2015, de la Corte Constitucional. Este tribunal desechó la petición de declarar contraria a la carta estas normas que en esencia trasladaron la vigilancia, llamada en este caso "acreditación", de las entidades de certificación a un organismo privado conocido como ONAC (Organismo Nacional de Acreditación).

Ahora bien, cabría discutir tanto este pronunciamiento judicial como las normas que sufrieron ese examen de constitucionalidad. No obstante la sentencia revisó los presupuestos constitucionales relativos al otorgamiento de las facultades extraordinarias legislativas al ejecutivo, así como la posibilidad de delegar funciones públicas en corporaciones de naturaleza privada sin ánimo de lucro de carácter certificador y tecnológico, como lo es el ONAC, y haber encontrado que se ajustaban a los mandatos constitucionales, en lo cual puede asistirle razón, lo cierto y la verdad jurídica y factual es que el ONAC no tiene como finalidad acreditar ni revisar el funcionamiento de las entidades de certificación digital; su función está relacionada con las entidades que *adelantan la evaluación de la conformidad* y que realizan la certificación de productos y sistemas de gestión, reduciendo obstáculos al comercio mediante la emisión de certificados emitidos por entidades acreditadas. Esta importante función que desarrolla ese organismo no concuerda con la función que el decreto ley le asigna respecto de las entidades de ***certificación digital***, las cuales no son entidades que acrediten productos o servicios.

En el ámbito internacional estas entidades tienen otros fines. Por ejemplo, las entidades agremiadas en la Asociación Europea de Acreditación (EA), y en particular la española, conocida como ENAC, referidas a laboratorios de ensayo o de calibración, clínicas de gestión medioambiental, emisión de gases, producción de gases de materiales de referencia o de personas, en ningún caso acreditan a entidades certificadoras de ***firma digital***, pues su naturaleza y funciones son diferentes. Aunado a lo anterior se tiene el hecho de que los criterios de acreditación establecidos por el ONAC, CEA.4-1.10, están exclusivamente referidos al mecanismo de firma digital, esto es, al cumplimiento de requisitos enfocados en la infraestructura de clave pública (PKI) y, a pesar de ello, en la actualidad se han acreditado servicios que no integran certificados de firma digital.

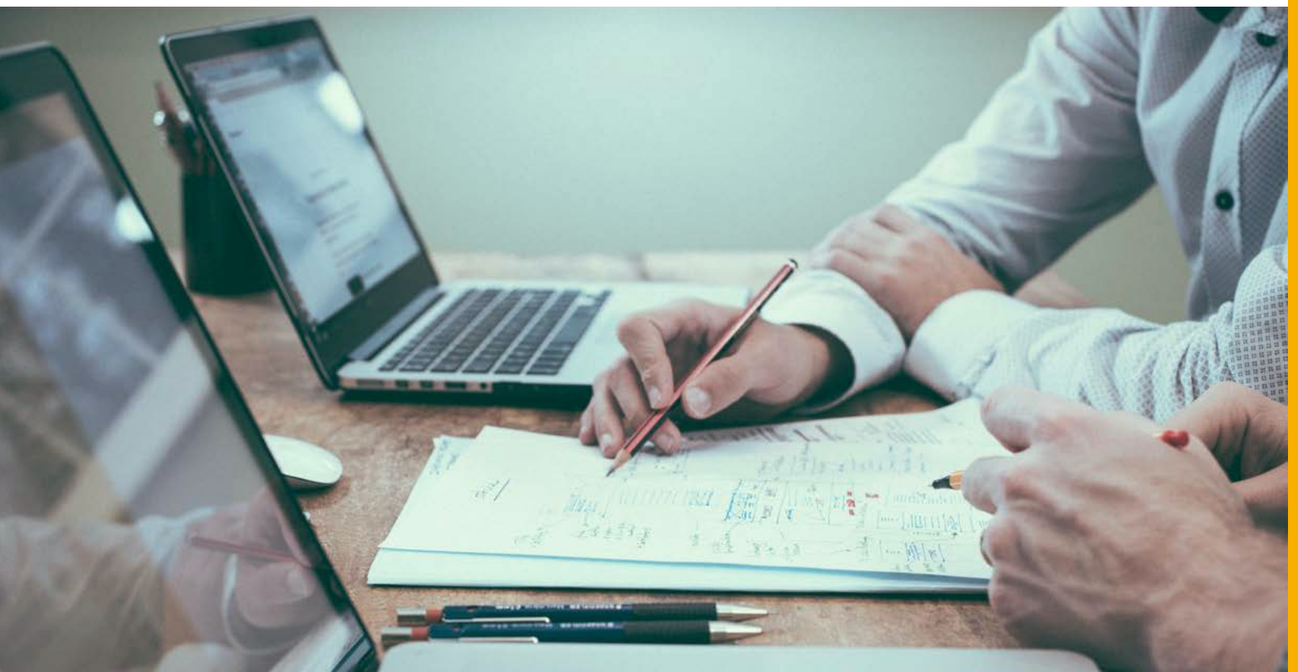
En conclusión, las entidades de certificación deberían seguir vigiladas y controladas por la Superintendencia de Industria y Comercio (SIC), y autorizadas en su funcionamiento por otro organismo, preferiblemente estatal, dadas sus funciones cercanas a la de ser fedatarias de la firma en los documentos electrónicos. Claro está, para ello se deben cumplir exigencias técnicas, pero sin asimilarlas, como en efecto se hace, a organismos técnicos alejados de su naturaleza y variándoles su régimen de acreditación, el cual finalmente ha sido duplicado, en este caso desconociendo la finalidad antitrámite que orientaba a la Ley 1474 de 2011 y a sus desarrollos consagrados en el Decreto Ley 019 de 2012.

Sin embargo, al estar definido de fondo este tema constitucional, solo quedaría esperar una modificación legal que acercara el esquema legal colombiano de vigilancia a la naturaleza de las entidades de certificación, de conformidad con la legislación internacional uniforme.

Por su parte, el Consejo de Estado, en pronunciamiento de 8 de febrero de 2018, negó las pretensiones de un demandante que pretendía la anulación de los artículos 4 y 15, numeral 1, del Decreto 1747 de 2000, reglamentario de la Ley 527 de 1999, que diferenciaba el valor probatorio o legal de los certificados emitidos por una entidad de certificación legal abierta de los de una naturaleza cerrada.

Recordemos que en Colombia se introdujo esta diferenciación entre entidades de certificación abiertas y cerradas (Decreto 1747 de 2000 artículo1, derogado por el Decreto 333 de 2014), que consiste en que los servicios que prestan estas últimas son gratuitos y únicamente comprenden el intercambio de mensajes entre estas y el suscriptor, en tanto que las abiertas prestan los servicios a título oneroso y su campo de acción es ***erga omnes***. En ese sentido, el Alto Tribunal desestimó acertadamente las pretensiones del demandante, considerando que no existe discusión frente a la validez y la fuerza jurídica y probatoria de los certificados de firma emitidos por entidades de certificación cerradas y que no era acertada la afirmación del demandante en el sentido de que el decreto les otorgaba un mayor valor a los certificados expedidos por las entidades de certificación ***abierta***. Este punto es de especial importancia pues no es plausible equiparar las entidades de certificación digital abierta con la de certificación cerrada en tanto cumplen funciones distintas, sin que las exigencias de los artículos en mención comporten en grado alguno el desconocimiento jurídico de los certificados de firma emitidos por estas últimas.

Estos antecedentes jurisprudenciales sobre los textos legales son de importancia a la luz del análisis legal del que ha sido objeto nuestra escasa legislación en la materia, otorgándole validez total a los principios de ***equivalencia funcional de los documentos electrónicos***, base de la legislación. También se observa la categoría superior de la llamada ***firma digital*** sobre las demás firmas electrónicas y cómo se ha autorizado al ONAC como entidad de acreditación sobre las ***entidades de certificación***, lo cual, pese a nuestras glosas sobre la naturaleza de dichas entidades y sus funciones, les imprime una certeza de seguridad jurídica a las entidades de certificación digital y a sus actuaciones por la calidad técnica que tiene el ONAC.



02

Firmas y firmas

Las firmas tienen una vieja historia en la civilización. Se confunden en la antigüedad con los sellos y mandatos reales, con el trabajo de los escribas eclesiásticos o seculares y con los copistas mercantiles. En el arte pictórico o escultórico, la exigencia de firma ha confirmado la autenticidad de las obras. A medida que avanzó el proceso de alfabetización de las sociedades se incrementaron las exigencias de la firma como medio jurídico que afirmara el origen documental, máxime en la cultura del papel, que en la actualidad está en trance de superarse.

En las codificaciones mercantiles, incluidas las nuestras, la firma posee una categoría jurídica especial esencial para ciertos documentos, al igual que en el derecho notarial y en los códigos procesales. Debe recordarse cómo en nuestra ley comercial el artículo 826 del Estatuto Mercantil define la firma como: *"[…] la expresión del nombre del suscriptor o de algunos de los elementos que la integren o de un signo o símbolo empleado como medio de identificación personal […]"*, y el siguiente artículo, el 827, expresa que *"la firma que procede de **algún medio mecánico no se considerará suficiente sino en los negocios** en que la ley o la costumbre lo admitan"*. Por tanto, nuestra ya casi cincuentenaria legislación comercial preveía firmas diferentes de las autógrafas, obviamente autorizadas por la ley.

Como atrás se dijo, la Ley 527 de 1999 consagró el principio de la ***equivalencia funcional de los documentos*** y de las firmas telemáticas o electrónicas a las tradicionales suscritas en medios físicos. Dentro de su capítulo sobre las definiciones normativas, artículo 2, dicha ley definió la ***firma digital*** como aquella que se adhiere a un mensaje de datos y que, utilizando ***un procedimiento matemático conocido***, vinculado a la clave del iniciador (clave pública y clave privada) y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje no ha sido modificado después de efectuada la transmisión del mensaje de datos.

Posteriormente, el artículo 7 de la misma ley prescribe la equivalencia funcional de la ***firma electrónica*** en los ***mensajes de datos electrónicos*** destinados a cumplir una obligación o como generador de consecuencias jurídicas cuando: a) se ha utilizado un método que permita identificar al iniciador de un ***mensaje de datos*** y para indicar que el contenido cuenta con su aprobación; b) el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o convenido. Este mecanismo de firma fue objeto de reglamentación a través del Decreto 2364 de 2012, como se explicará adelante, donde se precisó el alcance de las firmas electrónicas, pero no se explicó la diferenciación con las firmas digitales.

Más adelante la ley, en su artículo 28, distingue a la ***firma digital*** con atributos especiales, al precisar que su suscriptor tiene la intención de acreditar ese mensaje de datos y de ser vinculado con su contenido, siempre que sea la única persona que la usa, sea posible de ser verificada, esté bajo el control de quien la usa y sea posible su verificación. En el mismo apartado de las definiciones del capítulo inicial de la ley, esta define las entidades de certificación como aquellas personas facultadas para emitir certificados en relación con las firmas digitales y, posteriormente también, con las firmas electrónicas.

El artículo 7 de la misma Ley 527 de 1999 fue reglamentado por el Decreto 2364 de 2012, apelando al documento CONPES 3670 de 2009[89], en relación con la firma electrónica definiéndola así: "Métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas, que permita identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado para los fines para los que se utiliza la firma". Por su parte, el artículo 4 acepta que el manejo es confiable cuando los datos de creación correspondan exclusivamente al firmante y sea posible detectar alteraciones en su texto. Finalmente, la ley le otorga validez y efectos jurídicos a la firma electrónica si esta cumple con los requisitos del decreto y se somete a una auditoría especializada y periódica sobre los procedimientos que una parte suministra y al concepto técnico de un tercero independiente.

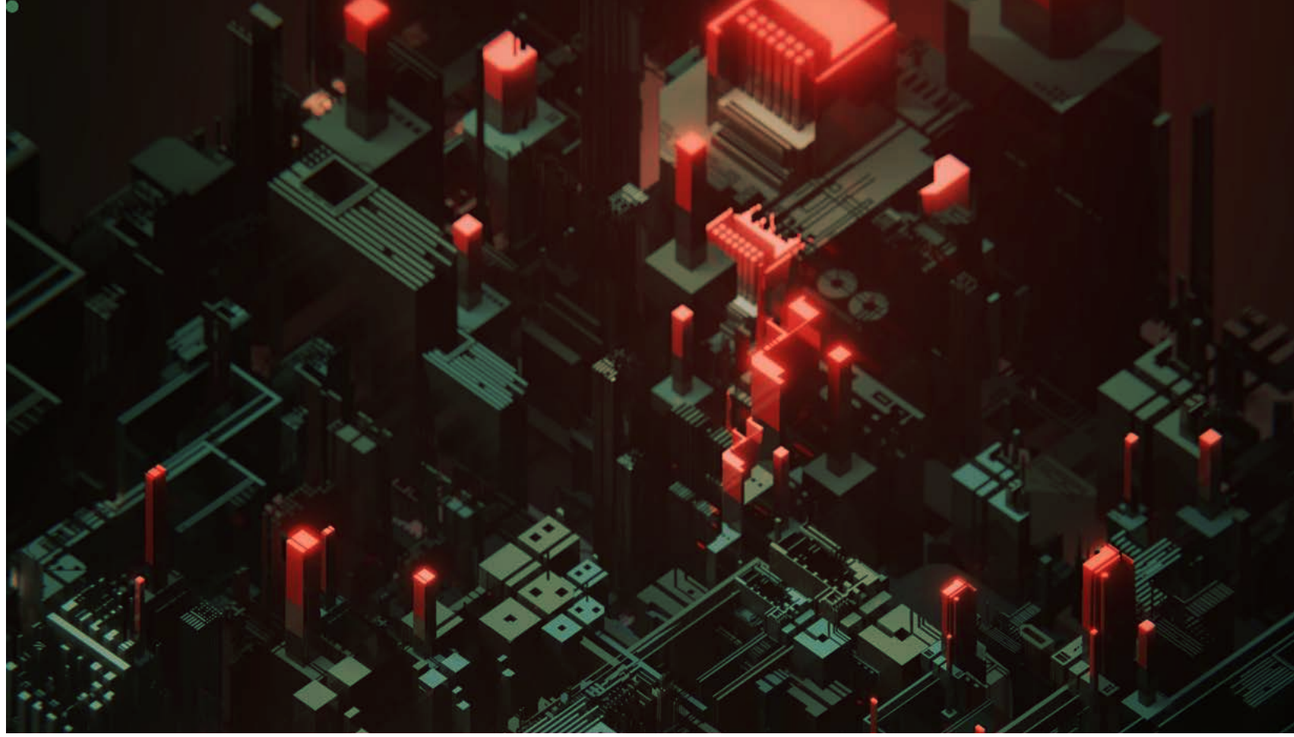
Este decreto, con claras imprecisiones de lenguaje en su redacción, generó una innecesaria confusión al no ser necesario, por vía reglamentaria, crear la categoría de "firma electrónica". Sin esa denominación y sin el decreto en mención, esta categoría ya existía en la ley. Además, se incurrió en un grave error al no mencionar expresamente la firma digital como una especie superior dentro del género de las "firmas electrónicas", facilitando de esta manera argumentos a quienes sin fundamento jurídico pretenden rebajar la categoría de la firma digital y asimilarla a las comunes firmas electrónicas.

Puede explicarse el origen de este decreto, más allá de los interesados nacionales contrarios a las firmas digitales, en el hecho de que el Estado consideró pertinente precisar que la Ley 527 de 1999 no era obstáculo para el ejercicio del tratado de libre comercio suscrito con los Estados Unidos y aprobado por la Ley 1143 de 2007. Sin embargo, debe recordarse lo dispuesto por el artículo 43 de la Ley 527 de 1999 sobre reciprocidad de certificados de firmas digitales, el cual les otorga validez a los emitidos por entidades extranjeras, lo cual es aplicable a este tratado.

La distinción y confusión existente en Colombia respecto de las firmas no es ajena a la discusión en otras latitudes donde se establecen categorías de firmas simples, firmas avanzadas, firmas avanzadas certificadas, e signature, digital signature, entre otras. En la Unión Europea se ha reconocido la existencia de esta confusión y cómo las reglamentaciones nacionales, en muchas ocasiones, han generado imperfecciones en la armonización de las leyes de los Estados que la componen.

Buscando un remedio a esta dificultad, la Unión Europea procedió a aprobar el

89. Hoy se encuentra recopilado el Decreto 2364 de 2012 en el Decreto Único Reglamentario 1074 de 2015 de Mincomercio, que contiene las normas del sector.



Reglamento Comunitario 910 /2014, de 23 de julio de 2014, sobre identificación electrónica y los servicios de confianza para las transacciones electrónicas del mercado, intentando superar el fracaso normativo de la Directiva 1999/93/ CE y obligando a los Estados a "garantizar la aceptación trasfronteriza de las firmas calificadas (entiéndase digitales), con los mismos efectos que a las firmas manuscritas"[90]. De esta forma la Unión Europea busca superar esta crisis conceptual asignándole a la firma calificada o digital una supremacía normativa.

Con miras a tener nacionalmente un marco jurídico cierto, evitarles confusiones a los operadores de los negocios mercantiles, que no tienen por qué introducirse o participar en discusiones académicas propias de los letrados en ciencias jurídicas y de los especialistas en criptografía, y a fin de incrementar el e-commerce o comercio electrónico, debería procederse a clarificar, sin ambigüedades, el ya tópico tema de las firmas virtuales acogiendo las tendencias marcadas por la Unión Europea, la cual en un mercado muy amplio y dinámico ha procedido a resolver mediante la simplificación conceptual esta selva de contradicciones, ajena a la dinámica del mundo empresarial. Sin embargo, más allá de la precisión y alcance de los mecanismos de firma, la directiva en mención plantea un estándar de identificación digital aplicable a todos los países miembros de la Unión Europea, cuya base tecnológica no es otra que la infraestructura de clave pública (PKI) prestada por terceros de confianza cuyos certificados tienen plena validez en cualquier país miembro.

En el ámbito nacional, una buena precisión sobre las diferencias entre firma electrónica y firma digital se encuentra en el Concepto

90. Ver Merchán Murillo (2016, p. 176, 177, 178). Este autor advierte además que estas nuevas reglas comunitarias tratan de lograr la interoperabilidad, a pesar de que no siempre sean necesarias en la práctica, pues evitan el riesgo debido a la tecnología utilizada y que están estandarizadas.

17-69600 de la Superintendencia de Industria y Comercio[91]. En igual sentido se ha pronunciado el tratadista Erick Rincón C. (2017), quien añade la categoría de firma digital certificada, "entendiendo por ella la firma en la cual interviene una entidad de certificación que identifica, tanto la entidad de certificación el certificado, como al suscriptor y contiene la clave

Se puede afirmar, en este orden de ideas, que siempre será necesaria la intervención de un tercero independiente, es decir, de una "entidad de certificación", cuando nos referimos a claves públicas o privadas y, por tanto, a la firma con valor jurídico especial, ya sea electrónica o digital.

La Ley 527 de 1999, en su artículo 2, literal d, definió las entidades de certificación como "aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la trasmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basados en las firmas digitales".

Estas entidades, de conformidad con el Decreto 019 de 2012, que modificó la Ley 527 de 1999, deben ser una persona jurídica y pueden certificar tanto las firmas digitales, o sea, las que cumplan los requisitos de la Ley 527 de 1999, como las firmas electrónicas de que trata el Decreto 2364 de 2012, a la luz las autorizaciones que le otorgara el artículo 161 del Decreto 019 de 2012.

Finalmente, ***el artículo 4 de la Ley 527 de 1999***, siguiendo a la ley modelo de Uncitral-CNUDMI, introdujo una novedad normativa del mayor interés: los acuerdos privados, en virtud de los cuales las partes, en ejercicio de la autonomía de la voluntad, pueden modificar mediante acuerdo las disposiciones contenidas en el capítulo III de la ley, es decir, el relativo a los mensajes de datos. Esta norma, acorde con el espíritu de una libre autonomía de la voluntad que la orienta, está en mora de pronunciamientos doctrinales, pues puede convertirse en una herramienta que facilite la ágil comunicación de los mensajes de datos mediante protocolos convenidos por las partes[92], sin que ello implique que dichos protocolos puedan llegar a tener el mismo alcance y efectos jurídicos de una firma digital.

91. *"De conformidad con lo previsto en el artículo 28 de la Ley 1755 de 2015, que sustituyó el Título II del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, fundamento jurídico sobre el cual se funda la consulta objeto de la solicitud, procede la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO a emitir un pronunciamiento, en los términos que a continuación se pasan a exponer, así: Nos permitimos realizar las siguientes precisiones: 1. OBJETO DE LA CONSULTA. Atendiendo a la consulta por usted radicada en esta entidad a través de su comunicación de la referencia en la cual señala: 'De acuerdo con la normatividad aplicable a la materia, ¿en las relaciones comerciales en donde se adquieran bienes o servicios mediante sistemas de financiación o por medio de operaciones de crédito, es posible que los mensajes de datos y documentación electrónica sea válida, eficaz y exigible, contractualmente para os consumidores donde con formas electrónicas se evidencie la voluntad de ambas partes para contraer obligaciones que estén soportadas por títulos valores o contratos?, ¿Se cumplirían las obligaciones como parte, si una vez celebrado el contrato de forma electrónica se envían dichos documentos (contratos, autorizaciones, y pagaré) vía electrónica?(…) (…)* ***Expídase concepto sobre la validez de las firmas electrónicas,*** *al momento de adquirir obligaciones y crear relaciones comerciales mediante sistemas de financiación o ventas financiadas y demás disposiciones referentes frente a este tema.[…]*

Por lo demás, será necesario que hubiese sido refrendada por una entidad acreditada, toda vez, que conforme lo asentó la Corte Constitucional, éstas "certifican técnicamente que un mensaje de datos cumple con los elementos esenciales para considerarlo como tal, ***a saber la confidencialidad, la autenticidad, la integridad y la no repudiación de la información, lo que, en últimas permite inequívocamente tenerlo como auténtico" (C-662 de 2000), pues, a decir verdad, ellas cumplen una función similar a la fedante.*** *4.2 Por otra parte, debe dejarse en claro qué ocurre con los documentos electrónicos carentes de firma, punto en el cual cabe asentar que aunque ella es útil para establecer la autenticidad del documento electrónico no es imprescindible, habida cuenta que cuando el mensaje carece de ella, el juez puede adquirir certeza sobre su autoría mediante otros mecanismos, particularmente, mediante el reconocimiento que del mismo haga la persona a quien se le atribuye o el que hagan sus causahabientes, todo esto sin olvidar que podrá la parte que lo aportó tramitar el incidente de autenticidad, en el que le incumbirá la carga de probarla. En ese orden de ideas, el reconocimiento regulado por el artículo 269 del Código de Procedimiento Civil se impondrá como insoslayable respecto del mensaje de datos desprovisto de una firma digital, habida cuenta que se trata de un documento que no ha sido suscrito ni manuscrito por su autor y carece de un signo de individualidad que permita imputar autoría y, por ende, ejercer el derecho de contradicción a la persona que la parte que lo aporta señala como su creador".* ***Además, la doctrina a identificado que "la firma digital es una especie de firma electrónica que para el caso se presentaría como el género. Igualmente es importante precisar que la enumeración de algunos métodos que la norma trae para la generación de una firma electrónica, no es una enumeración exhaustiva, de tal forma que se podrá aceptar cuantos métodos se utilicen siempre y cuando estos sean confiables y apropiados para el fin de la firma, así como el cumplimiento de cualquier acuerdo entre las partes"*** *(Flórez,* 2014) (apartes del Concepto 1769600 SIC-22 de marzo de 2017).

92. *"Artículo 4. Modificación mediante acuerdo. Salvo que se disponga otra cosa, en las relaciones entre las partes que generan, enviar, recibir, aclarar o procesar de alguna otra forma mensaje de datos las disposiciones del capítulo III, parte I, podrán ser modificados mediante acuerdo".*

03

Validez trasfronteriza de las firmas

Dentro de la incipiente utilización de los documentos electrónicos y las firmas asociadas a ellos faltan criterios uniformes de las entidades públicas para su utilización en demérito de la seguridad jurídica y de la facilidad y simpleza que exige el muy dinámico mundo negocial. La dificultad que surge de esta falta de uniformidad normativa en la materia se traslada en forma crítica a la utilización de los documentos electrónicos en las transacciones internacionales de comercio, dificultad que ha advertido la Comisión de las Naciones Unidas para el Derecho Mercantil. Esta propuso en su ley modelo, a partir de la cual se originó nuestra Ley 527 de 1999, el principio de la reciprocidad del reconocimiento de los certificados de firmas digitales emitidos por autoridades extranjeras, reconocido en el artículo 43 de nuestro estatuto.

En la teoría del derecho internacional se conocen tres formas destinadas a otorgar eficacia trasfronteriza a los certificados de firma electrónica avanzada o digital: el primer escenario es cuando se pretende utilizar los certificados de firma digital en un marco jurídico integrado, es decir, un mercado común; el segundo contempla la existencia de convenios o tratados internacionales entre los países en los cuales se desarrollan los negocios, y el tercero se presenta en torno a reconocimientos recíprocos de la validez de los documentos y firmas emitidas por entidades extranjeras.

Debe anotarse cómo ni en los acuerdos de libre comercio del área andina, ni en el Asia Pacífico, ni en el tratado de libre comercio con la Unión Europea, suscritos por el Estado colombiano, se han formalizado convenios para la utilización de firmas electrónicas, cualquiera que sea su modalidad, pues tan solo, y como atrás se anotó, el Decreto 2364 de 2012 hace relación al tratado de libre comercio con los Estados Unidos. Esta ausencia de convenios o tratados genera una falta de certeza o de seguridad jurídica en esta materia, sin que existan iniciativas estatales tendientes a remediar esta situación.

Además, la misma Comisión de las Naciones Unidas para el Derecho Mercantil, en el año 2005 y teniendo en cuenta la multiplicidad de legislaciones estatales sobre la materia que terminan obstaculizando la validez o reconocimiento de los certificados y de las firmas digitales, promovió un ***tratado o convenio internacional sobre la utilización de las comunicaciones electrónicas en los contratos internacionales***. Este convenio fue suscrito por Colombia en el año 2007 y hasta el presente no ha sido ratificado por el Congreso. El tratado está dirigido en uno de sus capítulos a ***"Promover la seguridad, mediante la adopción de criterios para establecer la equivalencia funcional entre las comunicaciones electrónicas o documentos de papel para el cumplimiento de los requisitos formales de escrito, original y firma".***

El país ha sido negligente en la suscripción de acuerdos o convenios internacionales en esta materia. Por ejemplo, luego de doce años, el acuerdo promovido por la Comisión de Naciones Unidas no ha sido llevado a estudio del Congreso, ni tampoco se ha impulsado un acuerdo con la Unión Europea, la cual, con su actual personería jurídica, está facultada para suscribirlo. Así mismo, no existen reglas con los países andinos ni con los del Pacífico. Tan solo la tercera opción del derecho internacional, descrita anteriormente, tendría validez por lo dispuesto en el artículo 43 de la Ley 527 de 1999[93]. Sin embargo, esta es la que menos seguridad jurídica ofrece. Un ejemplo por seguir es, como se mencionó, el eIDAS, Reglamento Europeo 910 /2014 cuya vigencia inició en el año 2016. Lo anterior lleva a plantear una dura crítica a nuestras políticas en esta materia, pues si la misma Ley 527 en su artículo 3, al referirse a la interpretación de sus textos, ordenó que "Habrá de tenerse en cuenta su origen internacional, la necesidad de promover su aplicación y la observancia de la buena fe", no tiene justificación la falta de diligencia para llegar a acuerdos bilaterales o multilaterales que otorguen márgenes de seguridad y certeza a las transacciones internacionales.

93. Antonio Merchán Murillo (2016, p. 176, 177, 178) y Juan Francisco Rodríguez (2018, p. 290-307) tratan ***in extenso*** el tema en mención. El primero expresa: ***"Además, ante las dificultades planteadas en el marco de la firma electrónica, el reglamento*** [se refiere al 910/2014 de 23 de julio, de la Unión Europea sobre firma electrónica] ***regula en el artículo 25 y siguientes las normas relativas a la firma electrónica ampliando, el artículo 5° del a Directiva, estableciendo una obligación explícita de otorgar a las firmas electrónicas calificadas los mismos efectos que a las firmas manuscritas. Además, los estados miembros deben garantizar la aceptación trasfronteriza de las firmas electrónicas cualificadas, en el contexto de la prestación de servicios y no deben introducir requisitos adicionales, que puedan crear obstáculos a la utilización de tales firmas"*** (p. 177).

Conclusiones

El país ha iniciado el tránsito legal en esta materia siguiendo los estándares internacionales, lo cual es apropiado pues la vocación global de estos y su vinculación con la tecnología mundial lo exigen.

No obstante, deben superarse los claroscuros existentes respecto de las firmas electrónicas, firmas electrónicas certificadas y firmas digitales, pues si bien las tres pueden coexistir, es clara la tendencia mundial al otorgarle un valor mayor y una equivalencia funcional con el papel y autenticidad a la firma digital, es decir, aquella que utiliza un *"Procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje"*. Esto no impide la utilización de las firmas electrónicas cuando cumplan los requisitos establecidos en las normas (Decreto 2364 de 2012), pero sin los atributos inherentes a la firma digital.

La utilización de acuerdos privados o convenios de que trata el artículo 4 de la ley deberían ser promovidos, pues facilitarían el comercio y la seguridad negocial. A su vez, no sobraría reconsiderar las funciones del ONAC respecto de las entidades de certificación, ajustándose a los modelos internacionales, y actualizar los criterios específicos de acreditación ampliando su marco de acción.

Es imprescindible crear una unificada política pública en materia de documentos y firma electrónica en general, pues se advierten variados y contradictorios conceptos. Un paso en ese sentido es la aplicabilidad del modelo de servicios ciudadanos digitales (Decreto 1413 de 2017).

Por último, está pendiente la asignatura de los convenios y tratados internacionales que otorguen certeza y seguridad jurídica al comercio trasnacional. En ese sentido se debería generalizar la reglamentación del eIDAS a nivel mundial, aplicable a aquellos países que han adoptado la Ley Marco de Firma Electrónica.

Bibliografía

Flórez, Germán (2014). La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial. ***Verba Iuris, 31***, 43-71. Bogotá D. C., Colombia.

Gutiérrez Gómez, María Clara (2002). ***Internet, comercio electrónico & telecomunicaciones***. Legis S. A.

Illescas Ortiz, R. y Ramos Herranz, I. (2010). ***Derecho de comercio electrónico***. Buenos Aires.

Madrid Parra, Agustín (2001). ***Aspectos jurídicos de la identificación en el correo electrónico. Derecho de comercio electrónico***. Valencia.

Merchán Murillo, Antonio (2016). ***Firma electrónica: funciones y problemática***. Madrid.

Rincón Cárdenas, Erick (2017). ***Derecho del comercio electrónico y de internet***. Tercera Edición. Bogotá D. C.: Legis S. A.

Rodríguez A., Juan Francisco (2018). ***Ámbito contractual de la firma electrónica***. Barcelona: Bosch Editores.

Jurisprudencia

Ley Modelo Uncitral.

Corte Constitucional, Sentencias: C622 de 2000, C831 de 2001 y C219 de 2015.

Consejo de Estado, febrero 8 de 2018.

Concepto SIC 17-69600 de 22 de marzo de 2017.

Código de Comercio.

Unión Europea.

Reglamento Comunitario 910/2014.

Directiva 1999/92.

AUTENTICACIÓN ELECTRÓNICA, FIRMA ELECTRÓNICA Y FIRMA DIGITAL.EL EMPODERAMIENTO DE LA IDENTIDAD DIGITAL

Mario Fernando Ávila Cristancho[94]

Resumen

La autenticación electrónica ya no se trata de una fuente técnica para validar la identidad de las personas ante un sistema, identificarla o individualizarla y que les permite incorporar mecanismos de firma digital para comprobar los compromisos adquiridos en el mundo digital, sino que está evolucionando para insertarse en la sociedad como una herramienta que permite lograr su identidad digital.

Se está exigiendo el fortalecimiento de una identidad única que permita validar las transacciones comerciales e interacciones sociales tanto en lo presencial como en lo digital, pues las relaciones humanas están perdiendo sus fronteras entre uno y otro canal. Lograr la identidad única segura, única e inmutable que funcione tanto en lo físico como en lo electrónico es el gran reto que debe seguir recibiendo el continuo apoyo de los sectores público y privado. Asimismo, incrementar la inversión en los planes, políticas y proyectos relacionados a la identidad digital de las personas será fundamental para el crecimiento de la economía digital e inclusive para la implementación de nuevas tendencias alrededor de la política y el ejercicio de los derechos civiles, pues será el eje central de las relaciones humanas sin la limitación propia que puede generar el medio en el que interactúan: físico o digital.

Palabras clave: autenticación electrónica; firma electrónica; firma digital; identidad personal.

94. Abogado de la Universidad del Rosario, especialista en Derecho de Negocios Internacionales, magíster en Derecho Privado de la Universidad de los Andes y magíster en Dirección de Empresas (MBA) de la Universidad Francisco Vitoria de Madrid, España. Especializado en dirección estratégica, administración de negocios, habilidades directivas, administración del talento humano y negocios digitales de la George Washington Bussines School. Ha sido profesor de la clase de Comercio Electrónico en la Universidad del Rosario; asesor administrativo y financiero; coordinador del Registro Mercantil y director encargado de los registros mercantiles y de las entidades sin ánimo de lucro de la Vicepresidencia de Servicios Registrales de la Cámara de Comercio de Bogotá, entidad para la cual se desempeña en la actualidad como asesor jurídico. Cuenta con amplia trayectoria y experiencia en la gerencia de proyectos tecnológicos enfocados a la virtualización de los servicios registrales que presta la Cámara de Comercio de Bogotá, la autenticación y firma de los documentos electrónicos presentados para el registro público, la mejora de los sistemas tecnológicos de administración de los registros públicos y los expedientes electrónicos y se ha desempeñado como asesor experto en proyectos de innovación digital, de servicios y procesos.

Abstract

Electronic authentication is no longer a technical source to validate the identity of people before a system, identify or individualize them, that also allows incorporate digital signature mechanisms to verify the commitments acquired in the digital world, on the contrary, it is evolving to incorporate as a tool that allows achieve their digital identity.

It is demanding the strengthening of a unique identity that allows validating business transactions and social interactions both in physically and in digital, because human relations are losing their borders between them,

Achieving the unique, secure, unique and immutable identity that works both physically and electronically is the great challenge that must continue to receive the continued support of public and private sectors, increase investment in plans, policies and projects related to The digital identity of people will be fundamental for the growth of the digital economy and even for the implementation of new trends around politics and the exercise of civil rights, as it will be the central axis of human relations without the own limitation that can generate the medium in which they interact: physical or digital.

Introducción

El 2019 es el año en el que celebramos importantes acontecimientos de nuestra vida digital. Entre ellos, el quincuagésimo aniversario de la irrupción del internet en nuestras vidas es, sin lugar a duda el más relevante, pues se conmemora el último hecho trascendental de la historia de la humanidad, que se ubica al mismo nivel del descubrimiento del fuego, la invención de la rueda, el Renacimiento o la llegada del hombre a la Luna.

Aquella simple pero exitosa conexión lograda en el marco del proyecto Arpanet entre las computadoras de las universidades de California y Stanford finalizando la década de los sesenta, que devino en una incipiente internet a inicios de los ochenta y que la humanidad empezó a sentir materializada para su entendimiento y experimentación en los noventa, nos subió sobre los hombros de un gigante. Al incansable ritmo de sus pasos, se redefinió en un parpadeo no solo la historia de la humanidad, sino sus más profundos conceptos mundanos y filosóficos relacionados a la existencia misma, pues, entre otros, nos llevó a la evolución de las relaciones terrenales y físicas a la interacción y convivencia en un mundo paralelo, completamente digital.

Como se ha esbozado, el internet que conocemos hoy en día —explotado como foro virtual de relacionamiento, interacción, transacción y medio de comunicación[95] y como plataforma tecnológica en la que se desarrollan nuevas tecnologías como el internet de las cosas y el ***blockchain***— tuvo sus inicios en la sociedad en los primeros años de la década de los noventa. Luego crecieron exponencialmente su disponibilidad, uso, capacidad y funcionalidad[96], al mismo ritmo que las tecnologías adyacentes (tales como la conectividad y la movilidad) evolucionaron.

Al principio, ese internet era un espacio "anónimo" donde las personas ocultaban en gran medida sus identidades reales. Constituía, pues, un foro virtual donde se interactuaba a través de ***alter ego*** cuya identificación en la comunidad ***web*** se expresaba a través de seudónimos, los cuales en la mayoría de las ocasiones variaban según el sitio en el que se estuviera navegando. Esto dificultaba generar ambientes apropiados y confiables para la interacción de las personas en escenarios diferentes al ocio, como lo pueden ser el consumo de servicios, la adquisición de bienes o la gestión de los deberes ante el Estado.

Sin embargo, el mundo actual, globalizado y unificado en un ambiente digital, ha llevado a la migración total hacia la red de los productos y servicios antes ofrecidos presencialmente —incluyendo los prestados por el Estado—, no obstante contar con un ambiente no presencial, propicio para mantener el anonimato. La necesidad de aprovechar esta situación en pro de simplificar los negocios, el cumplimiento de las obligaciones y en general la vida misma les exige cada vez más a las personas "revelar" su identidad del mundo físico, en algunos casos para vincularla en cada uno de sus seudónimos digitales y en otros para reemplazar estos por su nombre real.

Por otro lado, la masificación de usos y servicios digitales, dispuestos en millones de portales ***web***, miles de herramientas y dispositivos siempre conectados a la red, así como cientos de programas, aplicaciones y nuevas tecnologías disruptivas, hace imposible contar con igual cantidad de seudónimos digitales. Esto restringe cada vez más a las personas a contar con un número limitado de identidades para su recordación, cifra que tenderá a su reducción hasta contar con una sola, en la medida en que las vidas personal, laboral y social continúen su virtualización.

Fusionar en el mundo digital las anteriores necesidades —identidad real del usuario y un único método de reconocimiento y acreditación para todos los portales, dispositivos y servicios electrónicos— le permitirá a la persona no solo desenvolverse con facilidad, confiabilidad y seguridad, sino que, si se le añaden unos pocos componentes y voluntades adicionales, podrá lograr su plena identificación e individualización, lo que lo convertirá en un internauta único y diferente a los demás usuarios de la red. De este modo el usuario pasará de contar con un mero método de autenticación para acceso o firma robusto, certificado o simple a tener una verdadera ***identidad digital***.

Jurídica y técnicamente, se han hecho importantes esfuerzos en definir cuáles son los métodos confiables y apropiados que permitan obtener la idónea autenticación electrónica de las personas. Los resultados de estas iniciativas nos permiten día a día acercarnos cada vez más a aquel nirvana que hemos denominado identidad digital. Entre ellos celebramos, también en este año 2019, uno que marcó un hito en la historia legislativa de nuestro país pues integró a nuestro ordenamiento una norma que de forma general reguló lo relacionado al tratamiento de los mensajes de datos, entendidos estos últimos como toda ***"información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares"***[97], exceptuando expresamente su aplicación a las obligaciones pactadas en tratados internacionales y las advertencias escritas que por disposición legal deben estar impresas en cierto tipo de productos, que por su naturaleza se presentan en formato físico.

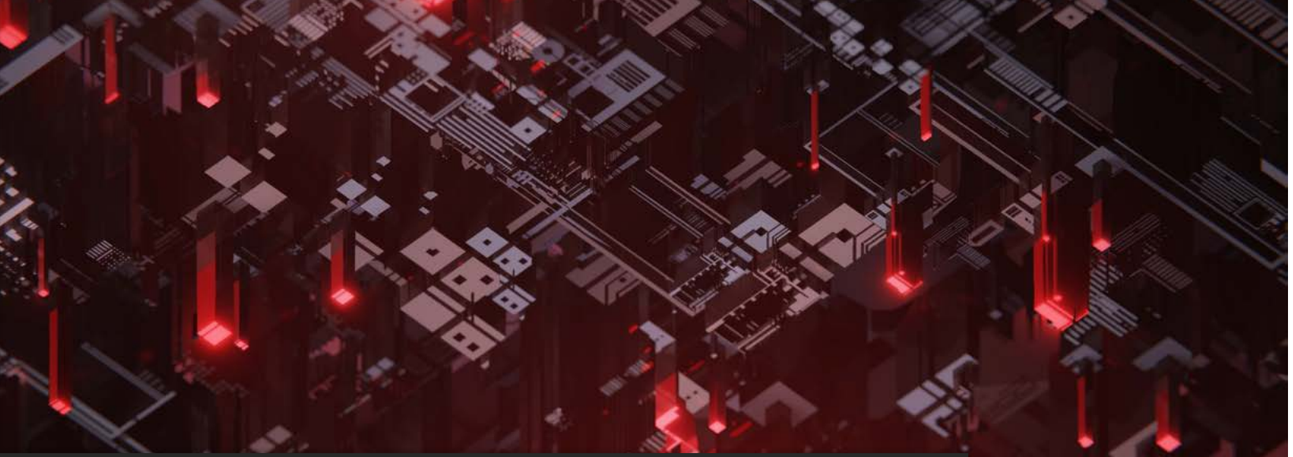
La Ley 527 de 1999, que en agosto 18 de 2019 cumplirá 20 años de promulgación, sentó importantes y fundamentales bases —aún vigentes— para el crecimiento, empoderamiento y desarrollo del entorno digital en Colombia. Al respecto el profesor Erick Rincón Cárdenas anota:

> *Uno de los principales obstáculos para el desarrollo de los negocios electrónicos lo constituye la inseguridad que genera el uso de las nuevas tecnologías frente al marco jurídico*

95. A través de herramientas cotidianas de uso masivo tales como las redes sociales, telefonía IP o aplicaciones móviles.

96. Según el informe conjunto de We Are Social (www.wearesocial.com) y Hootsuite (www.hootsuite.com), a abril de 2019 se contaba con aproximadamente 4.437 billones de internautas que hacían uso de la red en sus diferentes vertientes (https://wearesocial.com/blog/2019/04/the-state-of-digital-in-april-2019-all-the-numbers-you-need-to-know).

97. Ley 527 de 1999, artículo 2, literal a.



existente. Los partícipes en una operación de comercio electrónico deben tener la confianza suficiente de que todas las operaciones que van a realizar tienen valor jurídico.

Buscando otorgar al sector empresarial del país esa seguridad, las cámaras de comercio impulsaron la expedición de la Ley 527 de 1999 llamada Ley de Comercio Electrónico.

El objetivo central de esta ley es otorgar pleno valor probatorio a los mensajes de datos, como denomina la ley a la información digital. Hoy en día no se le pueden negar efectos jurídicos, validez o fuerza obligatoria a información alguna por el solo hecho de estar en forma de mensaje de datos. La información que se encuentra almacenada en un formato digital tiene el mismo valor jurídico que la información que se consigna en hojas de papel o en cualquier otro soporte físico (Cárdenas, 2015).

Esta ley fijó los parámetros jurídicos básicos que se deben tener en cuenta para la efectiva consecución de los negocios. Ello ha permitido a lo largo de estos años implementar un sinnúmero de técnicas y herramientas que aportan a la autenticación electrónica de los ciudadanos, pues este se estableció legalmente como uno de los componentes clave para la firma electrónica de los documentos digitales por ellos emitidos. Sin embargo, ¿estas técnicas son confiables, apropiadas e idóneas para el desarrollo del comercio electrónico en Colombia y, en sí, para la interacción de los ciudadanos en entornos digitales? ¿aportan efectivamente a la identidad digital de la persona o solo sirven como mecanismos de autenticación que requieren mayor desarrollo para su evolución?

En el marco de la conmemoración de los 20 años de la Ley 527 de 1999, nos aproximaremos con mayor detalle al concepto aquí planteado de ***identidad digital*** para entender su importancia como herramienta fundamental de cara al desarrollo del comercio electrónico, la economía digital y la evolución de la sociedad. Revisaremos los antecedentes de la autenticación electrónica, el firmado electrónico y el firmado digital en Colombia y, con todo ello, no solo resolveremos los cuestionamientos aquí planteados, sino que fijaremos las conclusiones que se deberán tener en cuenta para los siguientes 20 años.

01

Firmado electrónico: equivalente funcional para asumir y demostrar, con seguridad jurídica, compromisos adquiridos a través de medios electrónicos

Tal vez el principio jurídico más importante para el apropiado desarrollo de las relaciones digitales de las personas es el relacionado a la equivalencia funcional, entendido como aquel que permite ejecutar en el mundo electrónico las mismas actuaciones efectuadas en el mundo físico, siempre y cuando se asegure técnicamente el cumplimiento de los mínimos requisitos que determinan la existencia, validez y eficacia de la actuación realizada, según como se le exijan.

En un entendimiento simple pero efectivo de la Ley 527 de 1999 sobre los equivalentes funcionales mínimos requeridos para perfeccionar las relaciones comerciales electrónicas y prestar merito probatorio de los negocios realizados, la citada norma estableció que todos los componentes asociados al negocio deben quedar integrados en un medio o herramienta digital que asegure:

- Tener conocimiento del negocio realizado, es decir, que se pueda ver, leer, oír o entender de alguna manera el mensaje de conformidad con las capacidades de la naturaleza humana (***escrito***).
- Que la voluntad de los comerciantes en ningún momento sea afectada, eliminada o distorsionada por terceros ajenos a la relación y se mantenga tal cual como fue pactada (***original***).
- Que se tenga la capacidad de saber en cualquier momento lo acontecido en el negocio (***disponible***).
- Que las partes puedan manifestar, verificar y en especial demostrar su voluntad de realizar la actuación o asumir algún compromiso (***firmado***).

Este último equivalente funcional es entendido generalmente como la necesidad de homologar en ambiente digital la firma o rúbrica que una persona realiza sobre un documento (firma manuscrita), la cual en teoría es única e irrepetible pues proviene siempre de su puño y letra (lo que asegura su origen) y con la que se le acredita la emisión del mensaje contenido en el documento físico[98].

98. La Real Academia de la Lengua Española (www.rae.es) define la ***firma*** como:

"1. f. Nombre y apellidos escritos por una persona de su propia mano en un documento, con o sin rúbrica, para darle autenticidad o mostrar la aprobación de su contenido".

2. f. Rasgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento".

De igual forma, define a la ***rúbrica*** como:

"1. f. Rasgo o conjunto de rasgos, realizados siempre de la misma manera, que suele ponerse en la firma después del nombre y que a veces la sustituye".

Al respecto, la Ley 527 de 1999 estableció:

Artículo 7°. *Cuando cualquier norma exija la* presencia de una firma *o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:*

a) Se ha utilizado un método que permita ***identificar al iniciador*** *de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;*
b) Que el método sea tanto ***confiable como apropiado*** *para el propósito por el cual el mensaje fue generado o comunicado* [negrilla fuera de texto].

En los términos de la norma expuesta no quedaba duda sobre el primer requisito, pues se asoció a saber quién es el emisor de la información. No obstante, se requería adicionalmente que las partes tuvieran la tranquilidad de que el método de firmado por elegir era tanto confiable como apropiado para el negocio que se pretendiera realizar, lo que impidió la masificación del firmado electrónico en el país, pues llegar al consejo entre partes de lo que es confiable y apropiado depende de factores tales como quien asume los mayores riesgos o tiene la posición dominante y, lo más importante, si las partes se conocen previamente o no para tener la confianza entre ellas al efectuar la relación electrónica.

Dado este problema de masificación de la herramienta, y con el firme objetivo de impulsar el comercio electrónico en Colombia, se expidió el Decreto 2364 de 2012, que estableció como requisito adicional :

Artículo 4. *La firma electrónica se considerará confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si:*

1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.
2. ***Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma.***
Parágrafo. Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona:
1. Demuestre de otra manera que la firma electrónica es confiable; o
2. Aduzca pruebas de que una firma electrónica no es confiable [negrilla fuera de texto].

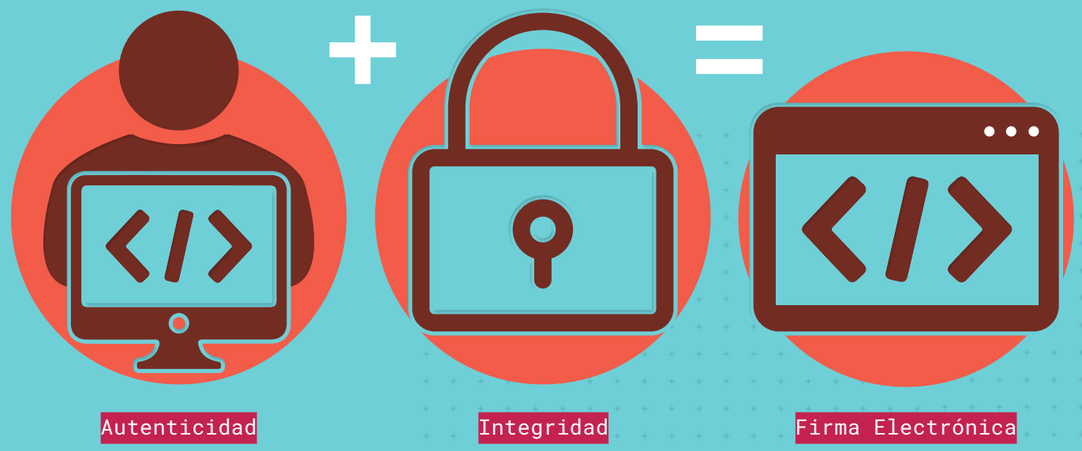
Lo anterior lleva a concluir que el equivalente aquí revisado es de vital importancia para la existencia y seguridad de los negocios electrónicos, pues indica no solo a quién se le exige el cumplimiento de lo pactado, sino que valida si los compromisos asumidos son aquellos sobre los cuales en efecto se tuvo la voluntad de celebrar y no tuvieron alteración alguna.

La ecuación que permitirá firmar electrónicamente, y con ello demostrar la voluntad para realizar alguna actuación digital o asumir algún compromiso a través de medios electrónicos, será el resultado de la suma entre haber identificado a la persona y que la actuación o compromiso se mantenga íntegro a como fue realizado por dicho individuo.

Así pues, se entiende que, por un lado, la autenticidad es el equivalente funcional electrónico de haber impuesto la firma de su puño y letra (origen). La integridad, por otro lado, es el equivalente funcional electrónico a que el documento físico no hubiera sido sujeto a adiciones, tachones o enmendaduras que hubieren alterado su contenido después de firmado y, por lo tanto, pueda ser sujeto a la tacha de no ser auténtico pues no se puede acreditar con fiabilidad que corresponde a la voluntad del signatario.

Es importante tener en cuenta que sobre el equivalente funcional electrónico (firma electrónica) de la firma (manuscrita) en el entorno se pueden encontrar las clasificaciones descritas a continuación.

Figura 1



Fuente: elaboración propia.

1.1 Firma electrónica simple

Como su nombre lo indica, es la forma pura y simple en la cual el mensaje de datos o archivo electrónico lleva inmerso algún componente que establece la identificación de su emisor (origen) y si aquel no ha sufrido alteraciones desde su expedición.

En este componente serán las partes dentro del proceso las que acuerden los métodos, técnicas o herramientas que se tendrán como válidas en su relación para determinar la autenticidad e integridad del mensaje. En este sentido, y dado que la apropiación de las herramientas fue asumida por las partes, serán estas las que soportarán ante terceros la confiabilidad de tales herramientas para que se acepte su negocio en caso de que este les deba ser escalado y generalmente si se llegase a presentar un eventual rechazo.

Finalmente, el mensaje de datos o archivo electrónico puede ser sujeto al repudio, entendiéndose este como la no aceptación o rechazo por parte del supuesto emisor, aduciendo que no realizó emisión alguna o que, habiéndolo hecho, se ha presentado alteración en el archivo o mensaje de datos "originalmente" expedido. Esto se valorará de conformidad con las metodologías o herramientas utilizadas, sopesando según el nivel de avance, robustez y/o posibilidad de vulneración de estas.

1.2 Firma electrónica certificada

En este componente, las partes integrarán a su relación jurídica métodos, técnicas o herramientas respaldadas por entidades acreditadas y de confianza, quienes por su naturaleza garantizan la idoneidad y calidad de tales mecanismos para asegurar en un nivel muy alto la autenticidad e integridad de los mensajes de datos o archivos firmados electrónicamente. En este entendido, y como su nombre lo indica, las entidades de confianza ***certifican*** o ***avalan*** que la metodología y/o las herramientas integradas en el firmado electrónico que fue utilizado en el negocio son lo suficientemente confiables y apropiadas para ser aceptadas.

Esta certificación no impide legalmente que el mensaje de datos o archivo electrónico pueda ser repudiado por el emisor, pero mitiga en un alto nivel el riesgo de esta situación pues, dada la naturaleza de las entidades de certificación (reconocidas desde la Ley 527 de 1999), inicialmente autorizadas por la Superintendencia de Industria y Comercio[99] y hoy en día acreditadas por el Organismo Nacional de Acreditación de Colombia[100] (ONAC), ellas están obligadas a utilizar métodos y/o herramientas apropiadas y avanzadas según el estado en que se encuentren la técnica y la ciencia[101].

1.3 Firma digital

La Ley 527 de 1999 establece en su artículo 2 que la firma digital es

> *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* [negrilla fuera de texto].

Es decir, es una tecnología criptográfica que asegura el mensaje emitido mediante la asignación y adhesión a este de un código numérico único (denominado ***hash***), que representa su contenido y es generado con la clave del emisor, de la cual solo este tiene conocimiento (clave privada). Así, el receptor descifrará el mensaje con su respectiva clave, verificando la información del titular de la clave que originó la información, y creará a su vez su propio ***hash*** del mensaje de datos recibido, el cual deberá ser exactamente igual al que fue inicialmente adherido; de lo contrario se entenderá que aquel ha sido modificado.

De manera que al adherirse un código numérico a un mensaje de datos se puede validar que este fue generado exclusivamente por parte de una clave determinada (origen) y se asegura técnicamente que cualquier modificación (sin importar su tamaño) inhabilita automática e inmediatamente la firma (integridad), sumándole una tecnología de doble clave (emisor y receptor, que entre sí se encuentran vinculadas). De este modo se incrementa exponencialmente el nivel de seguridad y la certeza de este mecanismo en el momento de asumir obligaciones y determinar a quién hacer exigible un derecho cuando estas han surgido en medios digitales.

Adicionalmente, el Legislador encargó a las entidades de certificación la labor de emitir las firmas digitales. Así se cuenta con un

99. Artículo 29 de la Ley 527 de 1999: *"Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional […]"*.

100. Artículo 29 de la Ley 527 de 1999 (modificado por artículo 160 del Decreto 019 de 2012): *"Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que cumplan con los requerimientos y sean acreditados por el Organismo Nacional de Acreditación conforme a la reglamentación expedida por el Gobierno Nacional […]"*, debidamente reglamentado en el Decreto 333 de 2014.

101. Artículo 4 del Decreto 333 de 2014: *"Los sistemas utilizados para el ejercicio de las actividades de las entidades de certificación se considerarán confiables si satisfacen los estándares técnicos nacionales e internacionales vigentes que cumplan con los criterios específicos de acreditación que para el efecto establezca el ONAC"*.

componente adicional que brinda seguridad técnica y jurídica a la herramienta, pues por disposición legal[102], desarrollada en el Decreto 333 de 2014, solo podrán ser acreditadas como certificadoras las personas jurídicas que cumplan una serie de requisitos administrativos, normativos, técnicos y patrimoniales que respaldarán sus funciones de certificación y respaldo.

Por lo expuesto, este mecanismo lleva inmerso el atributo jurídico del ***no repudio***, pues el Legislador estableció como presunción legal que el propietario de la clave privada (emisor) no podría desconocer ningún compromiso, obligación o actuación electrónica realizada a partir de esta:

> Ley 527 de 1999. Artículo 28. ***Cuando una firma digital haya sido fijada en un mensaje de datos*** se presume ***que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo […]*** [negrilla fuera de texto].

1.3.1 Firma digital abierta

Utiliza como componente especial una ***clave pública***[103] que se adjunta al mensaje de datos firmado digitalmente, con la cual cualquier persona que acceda a este, sin importar su naturaleza o relación con el emisor, podrá validar su integridad. De igual modo se asegura que la firma digital con la que el mensaje fue encriptado se generó con la clave privada del iniciador, sobre quien arroja la información relacionada a su identidad.

Este sistema de ***criptografía asimétrica*** donde se utilizan dos claves diferentes pero asociadas entre sí, una privada asignada al emisor y otra pública entregada sin restricción al receptor, mitigan fuertemente el riesgo de suplantación de identidad, pues eliminan la necesidad de entregar o dar a conocer la clave privada para el descifrado del mensaje de datos emitido.

Estas herramientas son respaldadas por las ***entidades de certificación abiertas***, que de conformidad con el Decreto 333 de 2014 son las que las que ofrecen al público en general servicios propios de las entidades de certificación de manera que (i) su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, y (ii) reciben remuneración por dicha actividad[104].

102. Artículo 29 (modificado por artículo 160 del Decreto 019 de 2012) y siguientes de la Ley 527 de 1999.

103. Artículo 3 del Decreto 333 de 2014: "*[…]* 6. Clave pública: ***valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador […]***".

104. Artículo 3, numeral 9, del Decreto 333 de 2014.

1.3.2 Firma digital cerrada

Como su nombre lo indica, no utiliza una clave pública o abierta para la verificación de cualquier persona. Por este motivo, solo podrá ser utilizada en las relaciones electrónicas surtidas entre el emisor de la firma y su respectivo suscriptor, quienes para ello utilizarán una única clave privada.

Estas herramientas son respaldadas por las denominadas ***entidades de certificación cerradas***, que son personas jurídicas 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[105].

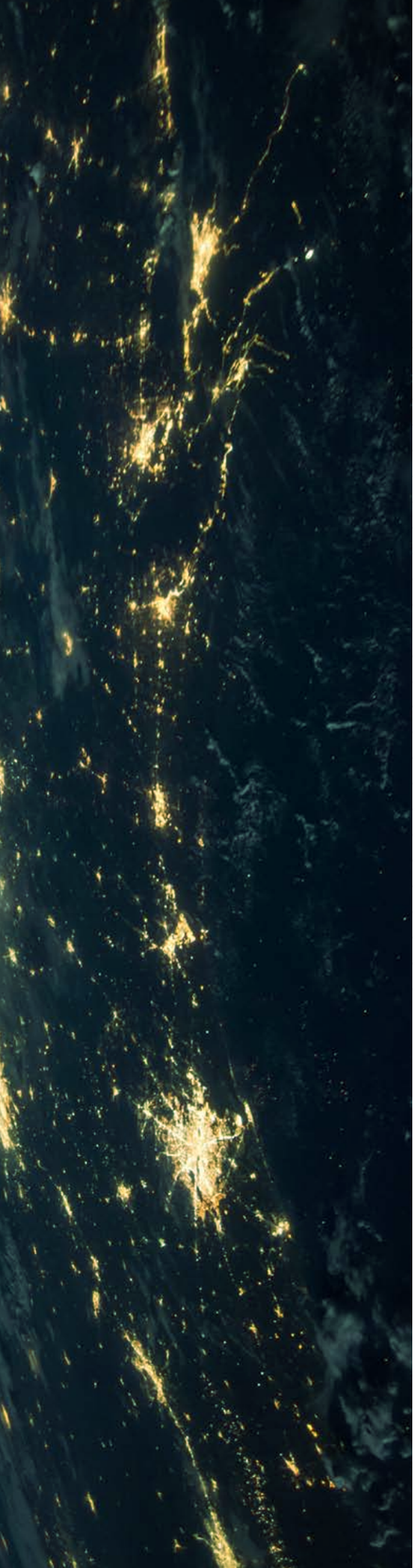
1.3.3 Firma digital certificada

Siguiendo el concepto aquí expuesto sobre las firmas digitales, el artículo 3 del Decreto 333 de 2014 establece adicionalmente que el ***certificado en relación con las firmas*** es el "***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***".

1.4 Apropiación de la firma electrónica

En Colombia se han realizado importantes esfuerzos para la apropiación de la firma electrónica (entendiendo la firma digital como una de las vertientes de esta) en las relaciones electrónicas suscitadas en el entorno. No obstante, acceder a unas u otras implicará diferentes niveles de esfuerzos por parte de los interesados, pues no será lo mismo invertir en la implementación de un sistema simple de firmado electrónico no certificado que en firmar digitalmente las transacciones, más aún si se tienen en cuenta factores adicionales tales como el número de interacciones, mensajes o relaciones efectuadas en un periodo de tiempo (costo de la herramienta implementada por cada mensaje firmado) o el patrimonio que se compromete en la relación jurídica.

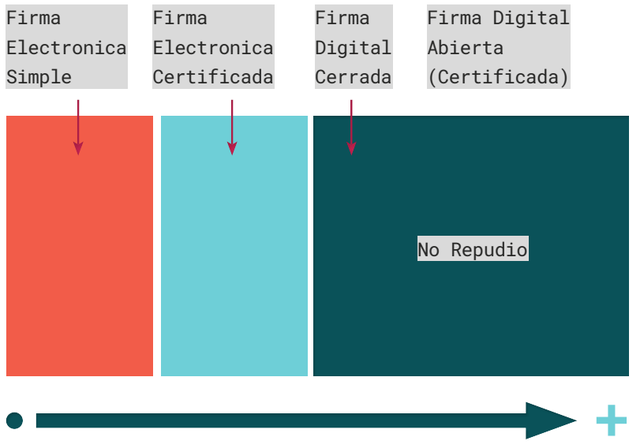
105. Artículos 3, numeral 8, y 5 y 6 del Decreto 333 de 2014.



La adopción de uno u otro mecanismo y el nivel de inversión y esfuerzo por realizar dependerán del análisis jurídico, operativo y de riesgos que se realice en la compañía o entidad estatal para su implementación. Descontando que el mundo actual demanda la virtualización de las operaciones presenciales y que los costos operativos de los servicios prestados digitalmente generalmente son menores a los prestados físicamente, este proceso exige resolver algunas preguntas, empezando por la más simple pero a su vez más importante: ¿realmente se requiere generar y almacenar evidencia electrónica de la relación efectuada o incluso sobre el bien o servicio prestado y por cuánto tiempo?

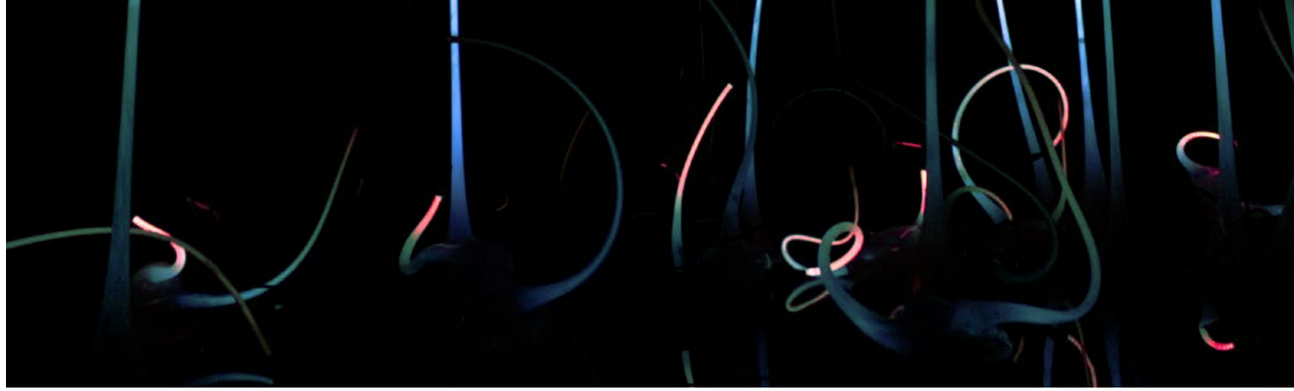
De igual forma se requiere otro conjunto de análisis tales como el nivel de probabilidad de que se presente un repudio de los mensajes generados o, si este llegare a presentarse y su resultado fuera adverso, ¿qué impacto reputacional, económico, jurídico o similar representaría para la organización o el negocio realizado?, ¿se puede corregir el inconveniente generado por un eventual no repudio y cuál sería el costo de dicha solución?, entre otros factores relacionados a la entidad estatal, compañía, negocio o sector en el que se desarrolle la relación electrónica.

Figura 2



Mayor certeza del origen
Menor probabilidad de ser repudiado
Mayor Seguridad y respaldo técnico y jurídico al negocio realizado

Fuente: elaboración propia.



Como se ha señalado, es claro que, sin importar el tipo de firma electrónica, como equivalente funcional de la rúbrica manuscrita, esta requiere de dos componentes esenciales para generar efectos jurídicos: la autenticidad (conocimiento de la identidad del emisor) y la integridad (seguridad de que el mensaje de datos no fue alterado después de firmado). En este sentido, la certeza del origen y/o la probabilidad de tener un resultado adverso ante el repudio dependerán en gran medida de las herramientas tecnológicas integradas para generar el mecanismo de firmado, aun si no se contase con una entidad certificadora de por medio.

Tanto la autenticidad como la integridad tienen a su vez un mayor o menor aporte de seguridad al proceso de firmado electrónico, dependiendo de la metodología utilizada, la tecnología disponible en el mercado o el estado de avance de la ciencia. Para la integridad, por ejemplo, el mercado cuenta con innumerables programas de auditoría informática que establecen con certeza el historial del *log* o cambios que se presenten en el registro de una base de datos. La Ley 527 de 1999 (artículo 30, modificado por el artículo 161 del Decreto 019 de 2012), por su parte, encarga a las entidades de certificación ofrecer servicios de estampado cronológico de mensajes de datos[106]. Sin embargo, en ninguno de estos casos se cuenta con la seguridad que ofrece la tecnología *blockchain*, que a partir de su sistema distribuido de registro y la codificación a través de un *hash* asociado a cada bloque generado en la cadena hace matemáticamente imposible la alteración de la información registrada en dicha herramienta.

En esencia, preservar la integridad de la información o al menos saber con certeza su eventual alteración es un asunto técnico para el cual hay muchas soluciones en el mercado y en eventual desarrollo, que brindan seguridad técnica y jurídica a los negocios digitales según el nivel de inversión que se destine a cada una.

106. **Artículo 3 del Decreto 333 de 2014:** *"[…]*7. Estampado cronológico: *mensaje de datos que vincula a otro mensaje de datos con un momento o periodo de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento o periodo de tiempo y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado".*

02

Autenticación electrónica: factor clave para el empoderamiento del internet, el desarrollo del comercio electrónico y la futura identidad digital

2.1 Autenticación no es lo mismo que firma electrónica

Es recurrente entender que estos dos conceptos son sinónimos, pues su usabilidad y funcionalidad ante un sistema operativo parte desde el mismo principio: realizar una actividad (como por ejemplo ingresar una contraseña secreta) que valide quién está ingresando a una máquina o programa o quien está dispuesto a enviar un mensaje de datos. Sin embargo, es importante recordar que toda firma electrónica lleva inmersa una autenticación previa del usuario, pero no toda autenticación conlleva a firmar electrónicamente un archivo o mensaje de datos.

Si una persona ingresa a una sucursal física bancaria para retirar dinero, el cajero que atiende la operación le demandará autenticarse para efectos de saber si quien está en su ventanilla es quien dice ser: el titular de la cuenta. Para ello lo más probable es que le solicite mostrar su documento de identificación para realizar el cotejo visual de la foto impresa en este y la persona que se lo entregó, validando adicionalmente que la información contenida en el documento de identidad corresponde a la que reposa en la base de datos de la entidad bancaria. Si la validación humana realizada por el cajero arroja un resultado positivo, entenderá que en efecto la persona que está frente a la ventanilla es quien dijo ser, el titular de la cuenta. Hasta el momento la única actuación que se ha realizado en la sucursal bancaria fue la mera autenticación del usuario o validación de su identidad, pues no se ha dejado ningún soporte que valide en el futuro la operación realizada; simplemente se respondió a la duda de quien estaba al otro lado de la ventanilla.

Claro está, el modelo de autenticación humana ha evolucionado y se le han añadido otros componentes técnicos que aseguren el proceso, como requerirle la imposición de su huella dactilar en un captor biométrico[107] para efectos de comparar la información obtenida en la toma con la que reposa en la base de datos donde se almacena la información de la persona y de sus medidas biométricas (en Colombia: la Registraduría Nacional del Estado Civil). De este modo se obtiene un resultado técnico adicional a la validación humana realizada que le indica al cajero si en efecto la persona al otro lado de la ventanilla es quien dice ser.

107. Tomando las medidas físicas estandarizadas de dicha huella y así hacerla técnicamente verificable, almacenable o comparable.

Con la plena seguridad de que su cliente es el titular de la cuenta, procederá el cajero a atender su solicitud y entregará la suma de dinero requerida. No obstante, lo más probable es que deba dejar una evidencia de la transacción realizada con la cual pueda soportarla en el futuro, de tal forma que, en caso de que sea necesario, quien la verifique y analice pueda entender claramente cómo fue la operación y, en especial, la información que demuestre que en efecto fue el titular de la cuenta quien realizó la solicitud. Para ello el cajero le indicará al titular de la cuenta que diligencie su solicitud en un documento y que proceda a firmarlo estampando de su puño y letra su rúbrica, como manifestación inequívoca de que la información contenida en este fue emitida por él y no por otra persona o, más importante aún, que existió la solicitud como tal.

El valor probatorio de dicho documento dependerá en esencia de que este sea legible, entendible y, en especial, de que dicho soporte no tenga tachones o enmendaduras que pongan en duda que la voluntad del suscriptor fue alterada mediante la modificación de la información suministrada al documento. Adicionalmente, cuenta con la rúbrica del cliente, que por definición se entiende tiene cierta dificultad para ser duplicada por parte de una tercera persona, sin contar que puede ser verificada a través de pruebas tales como la grafología.

Así pues, en este último escenario, además de la autenticación realizada por el cajero, se cuenta con la firma del cliente, integrada en un soporte documental que demostrará posteriormente el origen de la solicitud (rúbrica impuesta con su puño y letra), el cual no tiene tachones o enmendaduras que supongan alguna afectación en la integridad de la información realizada después de su firmado.

En el mundo electrónico la autenticación electrónica y la firma electrónica tienen funcionalmente la misma connotación y diferencia sustancial a la expuesta en el ejemplo planteado: cuando el usuario se da de alta en un sistema a través de un código, huella biométrica, reconocimiento de voz o cualquier otra tecnología que se utilice, está realizando el ejercicio de autenticarse, es decir, logra que aquel sepa "quién está al otro lado de la pantalla", sin que esto conlleve *per se* a dejar un soporte electrónico (a menos que así se diseñe); sin embargo, si se requiere contar con dicho sustento de la operación realizada, el sistema en cuestión deberá crear un documento electrónico en cuyos equivalentes funcionales se encontrará inmersa cualquiera de las acepciones que existen de firma electrónica (lo que incluye a la firma digital), entendida como la prueba electrónica que demuestra el origen (autenticidad) e integridad de la operación realizada.

2.2 Autenticación electrónica: identificación de la persona indeterminada, validación de identidad o la habilitación ante un sistema

En medios electrónicos la autenticación puede tener varias funcionalidades por diferenciar, cuyas vertientes dependerán de la necesidad que se requiera cumplir en la máquina, programa o mensaje de datos. Estas funcionalidades se concentran en resolver las inquietudes: (i) ¿quién es usted?, (ii) ¿es usted realmente quien dice ser? y (iii) ¿está autorizado o habilitado para acceder a un dispositivo o programa, o para enviar información?

La primera se refiere a la capacidad de un sistema de evaluar la información que le es suministrada para identificar e individualizar a una persona indeterminada, sin que se le den datos relacionados a su identidad para un eventual cotejo. El segundo escenario se refiere a la verificación que en efecto se realiza sobre la persona que detalla la información relacionada a su identidad ante un dispositivo, programa o mensaje, para determinar que sea quien dice ser y no se esté configurando una posible suplantación de identidad (una persona haciéndose pasar por otra).

En la tercera pregunta, la autenticación se entiende como el mecanismo por medio del cual un dispositivo o programa permite su acceso y eventual uso, previa validación de su llave de entrada. Esta última puede estar representada por una contraseña, una validación biométrica, el uso de un dispositivo externo o, cuando se trata de la autenticación realizada entre sistemas (es decir, sin la presencia humana), a través de protocolos, certificados de confianza o cualquiera otra técnica que haya sido desarrollada y programada para tal fin y que solo pretende reconocer si la información proviene de un sistema de confianza previamente autorizado.

En relación con el acceso requerido por personas, salvo el realizado mediante herramientas inherentes a estas (tales como el cotejo biométrico), la regla general en este escenario es que, para conceder las credenciales de acceso, primero se tiene que resolver alguno de los dos primeros interrogantes. Esto se debe a que, a menos que la información de la identidad de la persona sea totalmente irrelevante para el servicio que se prestará cuando se accede al dispositivo o programa, de tal forma que ni siquiera almacene este dato, se requiere primero aclarar a quién se le permitirá adquirir la llave de acceso, por lo que se tiene una doble connotación de la autenticación: como método para identificar a la persona a la que se le otorgará la credencial de acceso y como mecanismo para acceder a un programa o dispositivo con dicha llave.

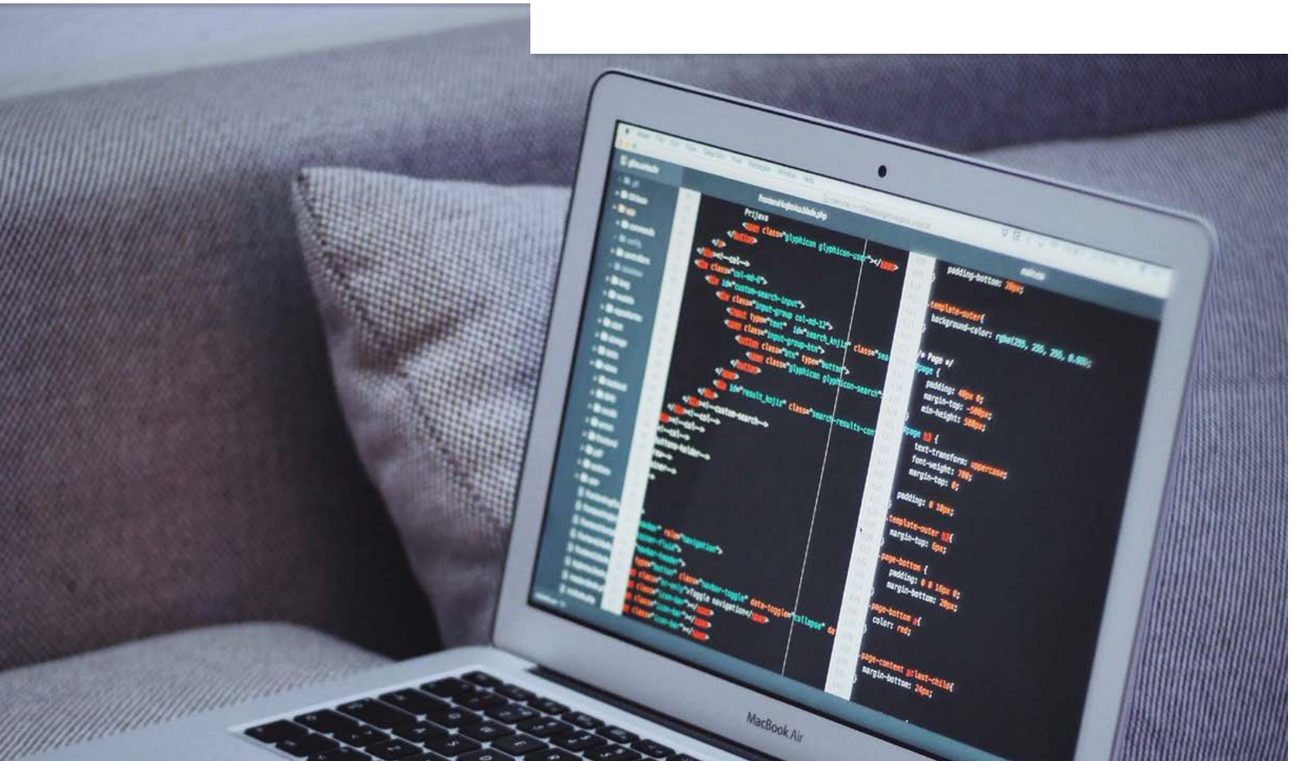
La autenticación electrónica aquí analizada excluirá la realizada por dos o más sistemas, es decir, sin intervención humana, y la realizada mediante credenciales públicas o libremente dispuestas, las cuales, sin un registro previo, permiten acceder al programa o dispositivo simplemente a quien sea el portador de aquellas, pues les es irrelevante la información de la persona con quien están interactuando.

En este orden de ideas, será pertinente mencionar inicialmente que, frente al primer interrogante que resuelve la autenticación electrónica, se debe tener en cuenta que este implica, entre otros, contar con un sistema robusto que brinde la capacidad de recopilar la información idónea, pertinente y suficiente para que al cruzarla con las bases de datos dispuestas en el entorno permita con total claridad y un alto porcentaje de certeza individualizar e identificar a una persona. Dependerá del sistema elegido cerrar la brecha de incertidumbre en el resultado obtenido, pues no será lo mismo llegar al resultado a partir de preguntas de conocimiento, claves o uso de dispositivos externos que validando biométricamente su comportamiento, físico o incluso ADN. De hecho, al recurrir a bases de datos alternas (o no oficiales) no solo se corre el riesgo de obtener información de mala calidad, sino que se convierte en una tarea virtualmente imposible, pues se debería acceder a la mayor cantidad de bases de datos posibles, de tal forma que se recopile una cantidad suficiente y apropiada de información que permita individualizar sin lugar a dudas a una persona sobre la cual no se tenía información alguna.

Por otro lado, debe tenerse en cuenta cuáles son las bases de datos pertinentes e idóneas para consultar sobre los datos intrínsecos que permiten individualizar e identificar a una persona. Lo recomendable es acceder a las que sean oficiales para este fin, pues no solo brindan seguridad jurídica en temas asociados al cumplimiento de las normas relacionadas a la protección de datos personales, sino que incrementan exponencialmente el nivel de calidad de la información.

En Colombia, por disposición constitucional (artículo 266 de la Constitución Política), la única autoridad encargada de identificar las personas es la Registraduría Nacional del Estado Civil, quienes custodian y administran la base de datos relacionada a la identidad y existencia de los colombianos. Esto cierra la brecha y asegura la calidad de la información a la que se puede acceder para el fin perseguido (por evidentes razones quedan excluidos los extranjeros). No obstante, aún se requiere un sistema demasiado potente, pues se tendrá que cotejar la información recopilada de la persona que se quiere identificar contra una base de datos correspondiente a un aproximado de 45,5 millones de personas (DANE, s.f.).

No obstante, contar con un sistema que responda a la primera pregunta puede llegar a ser más cómodo para el usuario y en algunos casos más certero y confiable con respecto a algunos que se utilizan para responder al segundo interrogante. Como se ha esbozado en términos generales, este último demanda demasiados esfuerzos para su operación, en gran medida por la gran inversión en infraestructura técnica y tecnológica que se requiere para lograr con certeza y seguridad sus objetivos de identificación e individualización de una persona indeterminada, lo cual les interesará hacer a algunos pocos actores, como por ejemplo a los organismos de seguridad del Estado. Por este motivo la tendencia general para autenticar personas se focaliza en los sistemas que responden a la pregunta ¿es usted realmente quien dice ser?".



Como se puede intuir, resolver esta inquietud implica cotejar la información recopilada por el sistema de autenticación —claves, datos biométricos, respuestas a preguntas personales, etc.— con la información de la persona que indicó ser y que reposa en bases de datos propias, ajenas, públicas o privadas a las cuales el sistema tenga acceso.

Sin importar el objetivo que se persiga o la pregunta que se vaya a solucionar, la autenticación electrónica tiene un fin: identificar electrónicamente a una persona, bien sea para determinar si es quien dice ser, para individualizarla cuando no se tiene información sobre ella, para permitir su acceso a un programa, dispositivo o la misma internet, o simplemente como componente requerido para firmar electrónicamente, motivo por el cual se revisará con mayor detalle esta funcionalidad.

2.3 Autenticación electrónica como herramienta de verificación de la identidad

2.3.1 Contexto y evolución

Verificar la identidad de las personas es una práctica no solo común sino necesaria en el mundo entero. El sector financiero, en particular, sobresale como el pionero en la adopción de metodologías y tecnologías de autenticación electrónica, si bien al día de hoy desde la suscripción a una red social hasta el pago de impuestos e incluso la búsqueda de empleo requiere de estas herramientas para cerrar las brechas de incertidumbre y mitigar los niveles de desconfianza que puedan generarse, más aún cuando las relaciones se desarrollan a través de mecanismos no presenciales.

Mantenerse en el mercado y ser competitivo demandó a la comunidad empresarial migrar a la red como foro para la realización de sus negocios. Sin embargo, esto no significó sacrificar premisas tan básicas como saber con quién realizan transacciones, pues en el mundo de los negocios la confianza es fundamental para su desarrollo, y la seguridad en las relaciones lo es todo para su éxito.

Lamentablemente, paralelo a esta migración, las prácticas criminales también han evolucionado. Ahora se trata de ciberdelincuentes dedicados a engañar a proveedores, empresarios o clientes y, en el peor de los casos, a aprovecharse de la vulnerabilidad en que se encuentran los datos personales en varios entornos, de tal forma que pueden asumir la "identidad" de una persona en la red. Ante estas prácticas se han incrementado los niveles de desconfianza en el momento de realizar validaciones de identidad electrónicas, lo que en principio llevó a los comerciantes y al sector financiero a implementar metodologías complejas que en muchas ocasiones afectaron la experiencia del usuario o le generaron cierto grado de incomodidad —como presentarse en las oficinas de la entidad para validar su identidad previo a la entrega de credenciales de acceso o dispositivos especializados que le permitan desarrollar una futura relación electrónica no presencial—.

En este sentido, quienes inician su excursión para operar en canales no presenciales (generalmente internet) deben en la mayoría de los casos tomar una de dos rutas: (i) vincular la mayor cantidad de clientes que se encuentren en el mercado, sacrificando para ello el uso de sistemas robustos de autenticación que brinden mayor seguridad y teniendo una ***suposición*** o ***lógica deducción*** de quién es la persona que se autentica, o (ii) salvaguardar la seguridad de las transacciones electrónicas, lo que implica no poder autenticar a algunos clientes afectados por la incomodidad en la metodología adoptada o simplemente porque no cumplen con los estándares y protocolos de seguridad implementados, pero con la garantía de que los resultados generan una ***razonable certeza*** de la identidad del usuario.

Lo anterior no debe llevar a inferir que existen organizaciones dispuestas a ser objeto de fraude y otras que no. Como

se expuso, los sistemas de autenticación que implementan dependerán en gran medida del resultado de los análisis de riesgos que se realicen vinculados al impacto económico, jurídico, reputacional y otros que se puedan presentar en virtud al entorno, sector u obligaciones que legalmente se deban atender.

El reto ha consistido entonces en lograr la evolución de los sistemas de autenticación de tal forma que impacten lo menos posible la experiencia de los usuarios (mediante la automatización, la funcionalidad intuitiva, la virtualidad en la relación y la inmediatez de resultados), mitigando al máximo los riesgos de fraude. Esto lleva al aumento de la seguridad y la confianza en las relaciones electrónicas.

2.3.2 Sistemas de autenticación electrónica

Antes de abordar este tema cabe compartir la siguiente reflexión: en 2017 se estrenó la película de ciencia ficción *Geo-Tormenta*, cuya idea principal estuvo basada a grandes rasgos en unos satélites de control climático cuya programación se salió de control. En un aparte de este filme se discute sobre el acceso al sistema operativo de dichos satélites para reiniciarlos, para lo cual, además de disponer de un dispositivo móvil exclusivo para su control (una tableta), demandaba el uso de una claves de acceso de conocimiento exclusivo del presidente de la nación. Sin embargo, por sospecha, no podían pedírselas a él, por lo que se planificó el método para obtener dicha información a través de un asesor de confianza. Ahora bien, dicho asesor les confirmó que le sería imposible obtener contraseña, palabra secreta o código especial de reconocimiento por parte del propietario de la información pues, parafraseando un poco, *"es imposible porque* él es la clave*"*.

La secuencia descrita de esta historia combinó los tres grandes conjuntos en que se pueden clasificar los mecanismos de autenticación que, lejos de ser ciencia ficción, se destacan en la actualidad para validar electrónicamente la identidad de una persona. Estos se encuentran en constante evolución para integrar día a día nuevos sistemas destinados a dicho fin; algunos en estado de pruebas, otros ya apropiados en países desarrollados de los cuales aún no han ingresado al entorno y algunos otros ya están madurados en el país. De cualquier forma, todos ellos cuentan con la capacidad de aportar jurídica y técnicamente a la confiabilidad de la autenticación electrónica. A continuación se describen estos grupos de autenticación y algunos ejemplos de ellos para su entendimiento.

(i) Él *sabe* la información que se requiere para autenticarse: una contraseña, las respuestas a unas preguntas, un código, etc. El nivel de fiabilidad, seguridad y certeza sobre la identificación del usuario estará determinado por que él y solo él sepa de dicha información, de manera que impida la suplantación por otra persona. En la escena descrita hubo esperanza de acceder al sistema operativo sin que se enterara su titular, pues se buscaba obtenerla a través de un asesor de confianza, ejemplificando las brechas de seguridad inmersas en este tipo de mecanismos y que en la realidad pueden ser aún más impactantes si se tiene en cuenta el mundo sobresaturado de información, con enorme facilidad para su acceso, en el que vivimos.

Los conocidos como mecanismos KBA (por sus siglas en inglés: ***Knowledge Based Authentication***), en la mayoría de los casos, verifican a los usuarios pidiéndoles que respondan algunas preguntas específicas de validación, desde la más sencilla relacionada al nombre del usuario, pasando por las creadas por él mismo en una base de datos —como lo pueden ser las claves, las contraseñas o las preguntas personales— hasta las más sofisticadas, que se realizan cotejando la información que sobre la persona reposa en bases de datos especializadas, potencializadas y debidamente estructuradas —como lo pueden ser las que se administran en el sistema financiero o por parte de las entidades de registros públicos—.

A su vez, estos mecanismos llevan inmersos diferentes niveles de seguridad y confiabilidad que permitirán suponer, deducir o tener una certeza razonable sobre la identidad del usuario. Un ejemplo evidente: no será lo mismo autenticar a un usuario solo porque responde a la pregunta más sencilla —"Indique su nombre"— o porque manifiesta ser propietario de una red social con el mismo nombre de quien dice ser (la cual a su vez tiene conocimiento de sus credenciales de acceso) que autenticarlo mediante la validación de una serie de preguntas reto construidas a partir de la información que reposa en bases de datos especializadas.

Cabe anotar que la seguridad de estos mecanismos, que impacta en su confiabilidad para validar la identidad de una persona, se encuentra adicionalmente supeditada a la responsabilidad con la que el usuario asuma la ***creación y custodia*** de ellos, en especial cuando se trata de contraseñas creadas para que a través de ellas se realice la autenticación electrónica. Sobre el particular, un estudio realizado en 2018 por la firma SplashData (especializada en asuntos de seguridad digital) estimó que el 30 % de los usuarios digitales utilizan contraseñas tales como "password", "123456", "password1234", o su nombre, apellido, nombre de la mascota, entre otros similares (SplashData, 2018). Sin embargo, son contraseñas que podrían quebrarse fácilmente utilizando simplemente la información que reposa en las redes sociales o métodos informáticos como la ***fuerza bruta***, lo que representa una obvia vulnerabilidad al mecanismo, afectado en esencia por los mismos usuarios.

(ii) Él *posee* un dispositivo que le permite autenticarse: este es un clásico método de autenticación que mantiene su vigencia toda vez que la confianza que le es brindada está interiorizada en el subconsciente de las personas pues ha hecho parte de su cotidianidad. No olvidemos que la herramienta esencial de autenticación para entrar al hogar radica en la ***tenencia*** de una llave, cuya estructura especial permitirá abrir la respectiva puerta.

Este método de autenticación buscará entonces reconocer a los clientes de forma remota utilizando herramientas móviles tales como celulares, tabletas, tarjetas con chip integrado, *tokens* que reciben contraseñas de un solo uso (OTP: ***One Time passwords***) e inclusive correos electrónicos previamente registrados como de su propiedad, a los cuales se puede enviar información para ser confirmada.

El sector financiero, pionero en materia autenticación electrónica en pro de la seguridad de sus transacciones, ha sido fuente recurrente de este tipo de herramientas. Así encontramos entre otras desde las tarjetas EMV (Europay Mastercard Visa), cuyo chip integrado no solo cerró la brecha de seguridad presentada en las tarjetas de banda magnética, sino que permitió a los terminales compatibles con el mecanismo comprobar tanto su validez como la titularidad del usuario que la presenta, llegando a migrar incluso a las ***biometric cards***, pasando por el pago mediante billeteras electrónicas instaladas en los teléfonos móviles (acercando el teléfono al datafono para la transmisión de información).

También se encuentran las transacciones realizadas a través de las redes sociales como WeChat[108], transfiriendo dinero electrónico mediante dos dispositivos móviles, y las bandas inalámbricas que realizan validaciones biométricas del ritmo cardiaco cuando se acerca el dispositivo al datáfono para registrar el pago.

Por otro lado, la alta penetración en el mercado de los teléfonos móviles y en especial de la simcard integrada a ellos, que se encuentra vinculada a una línea telefónica asignada al usuario, ha convertido a este método en uno de los más atractivos en el momento de utilizar factores de autenticación. ¿Existen dudas sobre el inseparable vínculo que se evidencia en la sociedad actual entre el ser humano y su teléfono móvil?

Generalmente usado como un segundo factor de autenticación, en la actualidad los teléfonos móviles constituyen en gran medida una segunda instancia de validación que asegura el proceso, pues se utilizan en una misma gestión de identificación dos mecanismos de autenticación: algo que sabe el usuario (ejemplo: una contraseña) y algo que tiene, como lo es confirmar en la herramienta a la que se accede un código que ha sido enviado exclusivamente al teléfono móvil. No obstante, la evolución tecnología presente en estos dispositivos está permitiendo llegar más allá de la simple autenticación, convirtiéndose así en una fuente fidedigna que abarca incluso a la firma digital móvil, pues se están aprovechando las cada vez más avanzadas funcionales integradas como las cámaras de foto y video o los sistemas de detección de voz o de reconocimiento de huellas dactilares[109]. Aunque a la fecha aún les falta desarrollo a estas herramientas para cumplir con los estándares técnicos mínimos que brinden seguridad en la captación de la información biométrica, la velocidad tecnológica cada día pone a disposición del mercado nuevos y avanzados aparatos que eventualmente serán apropiados y confiables para este fin.

(iii) Él *es* la clave: estos son técnicamente conocidos como ***mecanismos inherentes*** al ser humano pues hacen parte de lo que él es en su esencia. Este método está enfocado, pues, en la detección y reconocimiento de los rasgos físicos exclusivos o conductas únicas de las personas como características propias del individuo que lo diferencian de los demás puesto que ningún otro las podría llegar a tener. Este es el verdadero nirvana de la identificación e individualización de las personas para efectos de ser autenticadas electrónicamente.

Colombia ha incursionado exitosamente en estos sistemas. Un punto de inicio apropiado y que se institucionalizó en muchas entidades de orden nacional fue la firma biométrica. Con esta se analiza la conducta de la persona en el momento de imponer su rúbrica (firma dinámica) en un captor que verifica aspectos tales como la velocidad y aceleración para generar la imagen, la presión efectuada en el trazo, y puntos clave de la signatura en coordenadas (X,Y). Dicho servicio fue prestado por entidades de seguridad digital especializadas en la materia tales como las entidades de certificación abiertas.

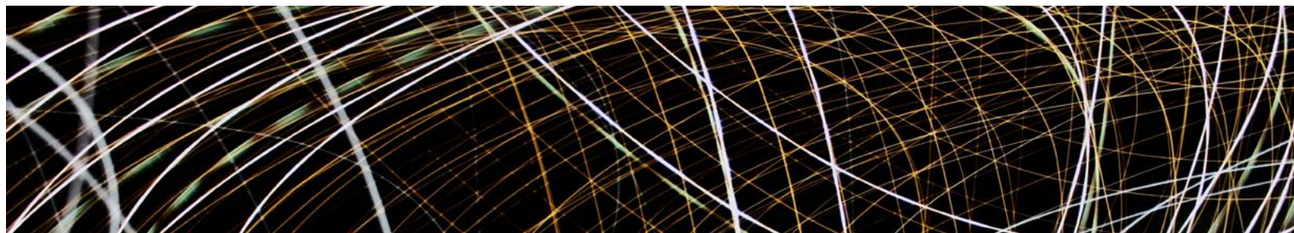
A su vez, el Estado impulsó fuertemente la apropiación y explotación de estas tecnologías. Al respecto, el Decreto Ley 019 de 2019 estableció en su artículo 18 que

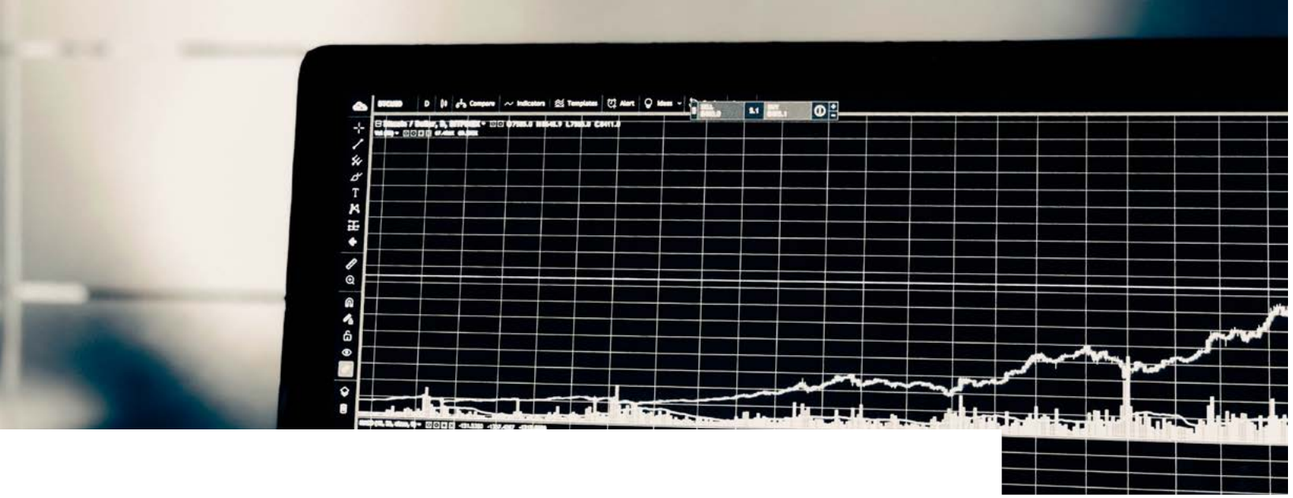
> *en los trámites y actuaciones que se cumplan ante las entidades públicas y los particulares que ejerzan funciones administrativas en los que se exija la obtención de la huella dactilar como medio de identificación inmediato de la persona, ésta se hará por medios electrónicos. Las referidas entidades y particulares contarán con los medios tecnológicos de interoperabilidad necesarios para cotejar la identidad del titular de la huella con la base de datos de la Registraduría Nacional del Estado Civil.*

Esta norma fundamental respaldó y brindó confianza a la tecnología biométrica, así como a la calidad, la pertinencia y —especialmente— la seguridad de la información que reposa en la registraduría nacional para la identificación de las personas. A su vez, esto incrementó el desarrollo de proyectos de transformación digital de las entidades públicas.

108. Sistema de mensajería instantánea chino, equivalente al WhatsApp ampliamente usado en occidente.

109. Según estudios expuestos por Goode Intelligence, para el 2016 se contaba con 770 millones de dispositivos móviles que integraban la tecnología de sensores de huella.





La autenticación biométrica de la huella dactilar es, hoy en día, una tecnología madura, robusta y recurrente en todos los sectores de la economía nacional. Entidades como cámaras de comercio, notarías públicas, bancos, empresas de telefonía celular e incluso la Registraduría Nacional del Estado Civil (RNEC) —para sus procesos electorales— la han apropiado con el fin de asegurar sus operaciones. De este modo se han realizado en 2019 un aproximado de 94,5 millones de consultas sobre la identidad de los colombianos. A su vez, la RNEC ha integrado a sus procesos los más altos estándares técnicos que blindan los datos por ella administrados. Así mismo, este entidad ha emitido las resoluciones pertinentes[110] que demandan a los operadores biométricos y a las entidades que usan este tipo de servicio el cumplimiento de protocolos y estándares técnicos que garanticen la seguridad de la información de los usuarios autenticados[111] en conjunto con las políticas colombianas de protección de datos personales.

Otros métodos tales como el reconocimiento facial, del iris o de la voz también han sido apropiado y madurados en Colombia por diversos sectores. Por ejemplo, la RNEC se encuentra en un interesante avance respecto a la implementación del reconocimiento facial como sistema adicional a la tecnología dactilar. No obstante, el uso de estos métodos no se ha masificado tanto como la huella biométrica.

Que la persona sea la clave ha conllevado a una gran revolución tecnológica sobre la verificación biométrica. Validaciones conductuales como la forma de caminar, las gesticulaciones, los tics e incluso el parpadeo inconsciente de los ojos, o el uso de procedimientos más profundos e incluso intrusivos como la verificación de la huella genética (biometría del ADN) se encuentran a la orden del día. Numerar los sistemas de autenticación biométrica es tan inocuo como clasificar los próximos avances de la ciencia; sin embargo, es una realidad que ya se está aprovechando para autenticarse, para firmar y para ser usada en cualquier escenario, como por ejemplo el financiero, donde las transacciones bancarias ya no se realizarán con clave, tarjeta o teléfono, sino que se migrará a sistemas de pago en los que se mostrará el rostro como un mecanismo de autenticación confiable y apropiado. De manera que, a futuro, "la persona será la misma tarjeta": la autenticación biométrica es el futuro materializado hoy.

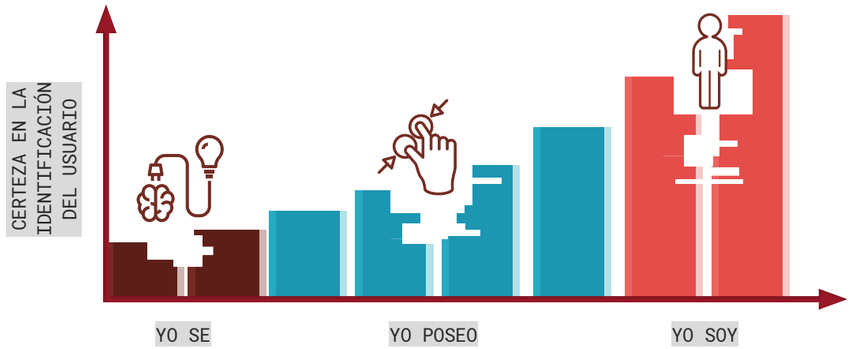
110. Ver Resolución 5633 de 2016, "Por la cual se reglamentan las condiciones y el procedimiento para el acceso a las bases de datos de la información que produce y administra la Registraduría Nacional del Estado Civil".

111. El cotejo biométrico de la huella dactilar en Colombia se realiza a través de ***operadores biométricos*** debidamente autorizados y auditados por la RNEC. Es un proceso en el cual se utiliza tecnología certificada por entidades como el FBI de Estados Unidos y que no almacena información alguna sobre las huellas dactilares de las personas, sino que en un tránsito seguro de información se obtiene como resultado una respuesta positiva o negativa respecto a la identidad de la persona sobre la cual está consultando

2.4 La actualidad de la autenticación electrónica: hacia la identidad digital

La seguridad jurídica y técnica de los sistemas de autenticación electrónica se puede graficar como se observa en la figura 3.

Figura 3



Fuente: elaboración propia.

El objetivo de lograr los máximos estándares de seguridad que aseguren la identidad de las personas y evitar el fraude ha conllevado a las organizaciones en gran medida a combinar los factores de autenticación para tal fin. Así, una clave ingresada debe ser respaldada por una OTP enviada al teléfono móvil; la validación remota del documento de identidad se compara con un video en vivo de la persona que está al otro lado de la línea (que incluye la comparación entre la foto que reposa en el documento con respecto a la persona en el video, así como la validación de la vigencia del documento, siempre y cuando cumpla con unos estándares técnicos hoy en día exigidos a este tipo de identificación); o se realiza multibiometría a diferentes aspectos inherentes a la persona que la pueden individualizar.

Sin embargo, debe tenerse cuidado cuando se realicen estas fusiones entre los sistemas. Por ejemplo, utilizar un mecanismo robusto de autenticación como la biometría para llevarlo a obtener uno básico como saber una clave, sin generar componentes apropiados de seguridad en la construcción y custodia de la credencial asignada, hará que se desperdicien los esfuerzos invertidos para responder a la pregunta: "*¿es usted realmente quien dice ser?*".

Por otro lado, la adecuada identificación de las personas en medios electrónicos no es únicamente un interés de las compañías para acrecentar sus ingresos, de los clientes para incrementar su calidad de vida o del Estado para prestar efectivamente sus servicios públicos. Es, de hecho, una necesidad mundial dada en gran medida por la globalización y la pérdida de las fronteras, especialmente cuando se habla de relaciones electrónicas no presenciales, donde se requiere iluminar muchas zonas grises que pueden camuflar asuntos como el lavado de activos o la evasión fiscal.

En la búsqueda de estos objetivos se han puesto en riesgo asuntos tan esenciales como la protección de los datos personales. La necesidad de obtener mayor cantidad de información a cambio de saber quién está en línea ha llevado a los usuarios a exponer irrestrictamente su información personal; a las organizaciones, a capturar cada vez más datos personales y/o esenciales, y a los ciberdelincuentes, a estar atentos a las brechas que se presenten para extraer información con la que puedan suplantar la identidad de las personas con fines criminales.

Extracciones ilegales de datos personales mundialmente reconocidas como las sucedidas con Verizon y Equifax en 2017 o Facebook en 2018, entre otras, han incrementado el temor de las personas sobre la información de ellos que circula en la red y los mecanismos para controlarla, pues con esto se incrementa la capacidad de terceros de autenticarse a nombre de ellos y suplantar así su identidad en la red.

Al respecto, la Unión Europea ha realizado un esfuerzo interesante con la GRPD[112] para la protección de los datos de sus ciudadanos, aun cuando se trate de sistemas extranjeros. Esto les ha demandado a proveedores norteamericanos modificar sus estándares y procedimientos para que cumplan dicha directiva, lo que ha repercutido en que las organizaciones analicen las infraestructuras y los sistemas más adecuados para la autenticación electrónica de las personas. De tal modo se ha potencializado el teléfono móvil como uno de los más atractivos, motivo por el cual se concentran grandes esfuerzos en su evolución para dicho fin.

A su vez, las nuevas tecnologías disruptivas están haciendo lo correspondiente para aportar a la autenticación electrónica con seguridad y sin comprometer los datos personales de los usuarios. El ***machine learning***, por ejemplo, permitirá que mediante el aprendizaje automático de los sistemas se puedan procesar y clasificar millones de datos de las personas sin comprometer su seguridad por la intervención humana, extrayendo solo aquellos que son apropiados y confiables para identificar a los usuarios. Así mismo, la maduración y el escalamiento del ***blockchain*** no solo ofrecen integridad a la información suministrada, sino que permitirán aprovechar su tecnología de registro distribuido (DTL) para consultar a varios operadores de confianza la información que se considere pertinente para el fin perseguido, entre otras novedosas propuestas.

No obstante lo expuesto, la biometría sigue siendo el mecanismo tanto apropiado como confiable para la autenticación electrónica, de mayor uso y confiabilidad, en especial para el sistema financiero, que estima que para el 2020 contará con alrededor de tres billones de usuarios de servicios bancarios biométricos (Goode Intelligence, 2015). Por lo tanto, se continúa trabajando fuertemente en el perfeccionamiento de estas técnicas. En particular, el reconocimiento facial, del iris o de la voz es el sistema por masificar teniendo en cuenta no solo el posicionamiento de la huella biométrica en el mercado, sino que en gran medida no depende de los desarrollos que deban hacerse en los dispositivos móviles para mejorar el desempeño del lector de huella dactilar integrado. Esto sin contar la idiosincrasia norteamericana, que considera este método como ***invasivo***, pues deben ser únicamente los criminales quienes se sometan a un escrutinio de dicha naturaleza (por la figura de la imposición de huellas dactilares como método para registrar a los criminales).

112. .General Data Protection Regulation.

Conclusiones y prospectivas

Contar con sistemas unificados y en gran medida centralizados que permitan el control de la información que reposa de las personas; el temor del usuario a seguir exponiendo cada vez más su información personal en un vasto número de dispositivos o programas; la necesidad de incrementar los estándares de seguridad y control de los negocios, como base que garantiza el crecimiento de la economía digital; saber ante qué sistemas u organizaciones se encuentran los datos de una persona[113], de tal forma que se pueda cumplir con las directrices de la GRPD tales como el derecho a ser retirado de las bases de datos, y, en esencia, lograr la interacción con el gran número de programas y dispositivos existentes en el mercado con seguridad, naturalidad e intuición demandan de los sistemas de autenticación algo más que el simple reconocimiento o identificación para saber quién está al otro lado de la línea; exige migrar a una verdadera identidad digital.

Es decir, se necesita tener un sistema que con seguridad técnica y jurídica identifique e individualice a las personas de forma concreta y certera, de manera que les permita ser reconocidas ante toda la comunidad digital sin importar dónde se encuentren navegando, a qué dispositivo estén accediendo o qué mensaje están transmitiendo. En esa misma medida deben contar con plena capacidad legal para exigir derechos y asumir obligaciones pero, sobre todo, con protección y respaldo de las instituciones, pues este método llegará a integrarse al ordenamiento jurídico como un nuevo atributo de la personalidad, inherente a la condición de persona y que por defecto contará con las mismas características legales tales como la unicidad, la inalienabilidad y la inembargabilidad.

La realidad económica, política y social demanda cada día más que las personas no estén clasificadas según el ambiente en que se desenvuelvan, teniendo una identidad única para lo presencial y una o varias para lo digital. Las relaciones humanas en los diferentes aspectos de la vida están perdiendo sus fronteras entre los dos canales, incluso con un mayor impacto en lo virtual, dada su capacidad de llegar a más personas en cuestión de segundos.

El anonimato del internet está siendo rápidamente reemplazado por la "revelación" de la verdadera identidad del usuario digital. Por este motivo, proteger su identidad en la red y procurar la unicidad de esta en los ambientes físico y electrónico será resguardar la identidad ***per se*** de la persona, de modo que los esfuerzos realizados para este último fin no deben circunscribirse únicamente al mundo presencial.

Para la protección del individuo, de los negocios, de la economía y de la sociedad misma se requiere la adopción de planes, políticas y proyectos estructurados y avanzados sobre la identidad digital

113. Hoy en día una persona puede estar autenticada de tantas formas y maneras como sistemas a los que haya accedido, lo que hace virtualmente imposible saber en cuáles debe darse de baja en caso de requerir dicha actuación, pues en el mundo presencial tiene una sola identidad, pero en el digital, infinitas.

de los ciudadanos, pues estos serán la materia prima para la estabilización de los negocios virtuales, el empoderamiento de nuevas tendencias económicas e inclusive las futuras políticas civiles, administrativas o penales que se adapten a la realidad mundial. En esa línea, la OECD[114] catalogó a la identidad digital como un herramienta ***fundamental*** para el desarrollo de la economía digital (OECD, 2011).

Fortalecer los sistemas de autenticación electrónica de las personas con mecanismos robustos que conlleven a la identidad digital aportará al acatamiento de las exigencias que se le hacen al sector financiero para evitar el lavado de activos o la financiación del terrorismo. Tal práctica será una herramienta confiable y apropiada para el desarrollo de las nuevas metodologías de cumplimiento como el KYC, la AML y la BSA[115], cuyos resultados a su vez aportan a la consecución de la identidad digital de los usuarios bancarios.

Por otro lado, se debe procurar explotar al máximo las herramientas con las que se cuenta en la actualidad. Un ejemplo de ello es la indudable contribución de la portabilidad numérica[116] a la autenticación electrónica, hasta tal punto que es claro que esta se ha convertido en una necesidad en el momento de seleccionar servicios de telefonía celular, pues las personas han optado por registrar en innumerables sistemas, programas y dispositivos sus números telefónicos para que sean utilizados como un factor adicional al validar su identidad. Se trata, así, de números de identificación electrónicos dado su vínculo con la persona propietaria, es decir, en la actualidad se cuenta con dos números de identificación: el del documento de identidad para el mundo físico y, ahora, el del teléfono móvil para lo virtual.

En este entendido, ¿podría pensarse en una evolución de dicha funcionalidad y reglamentar la exigencia de que el número de documento de identidad asignado a una persona en particular por el Estado (cédula de ciudadanía o de extranjería e incluso pasaporte) sea asociado a un número telefónico único, personal, intransferible y no asignable a nadie más? Este podría estandarizarse como un método confiable y apropiado de autenticación electrónica a través de un único número de identidad física y digital, con lo que a su vez se aprovechan las funcionalidades intrínsecas de los dispositivos móviles en pro de usarlos como herramienta para la firma digital, las transacciones electrónicas, la biometría o la simple confirmación de voz en las relaciones no presenciales. Es decir, ¿sería posible asociar un número de identidad único, irrepetible, personal e intransferible del mundo físico al funcionamiento de un dispositivo móvil con tecnología avanzada, cuya combinación conlleva a la obtención de un mecanismo robusto de identificación remota?

Es inevitable mencionar la necesidad de contar con el apoyo del Estado para lograr los fines aquí expuestos. En ese sentido, desde la promulgación de la Ley 527 de 1999 el país ha realizado importantes esfuerzos en la materia, algunos exitosos —como el Decreto 2364 de 2012 o el Decreto antitrámites 019 del mismo año— y otros que, a pesar de estar expedidos y ser de vital importancia, están en mora de materializarse —como los creados en el Decreto 1413 de 2017[117]—.

Lograr la identidad digital en los próximos 20 años no solo dependerá del avance de la ciencia y la tecnología o del apoyo del sector financiero y privado; se requerirá continuar patrocinando e impulsando los proyectos de autenticación electrónica desarrollados por la Registraduría Nacional del Estado Civil como entidad oficial que identifica a los colombianos. De igual forma serán esenciales la participación en iniciativas trasnacionales que permitan integrar sistemas de autenticación para extranjeros, la expedición de normas ajustadas a los avances y requerimientos mundiales en materia de identidad digital como las aquí ejemplificadas, la materialización de las iniciativas que ya hayan sido puestas sobre la mesa y, sobre todo, impedir el retroceso en aquello que ya se ha estandarizado en la sociedad.

114. Organización para la Cooperación y el Desarrollo Económicos.

115. Siglas en ingles de: conozca a su cliente (KYC), lucha contra el lavado de dinero (AML) y Ley de Secreto Bancario (BSA).

116. Obligatoria para las empresas que prestan servicios de telefonía móvil desde la Ley 1245 de 2008.

117. Sobre los servicios ciudadanos digitales, cuya bondadosa iniciativa busca integrar a nuestra sociedad herramientas como la cédula de ciudadanía digital para la identificación electrónica de los colombianos y, en especial, el concepto de que el ciudadano tenga una credencial única para ser reconocido virtualmente ante cualquier entidad del Estado, con la seguridad jurídica de haber sido obtenida a través de la autenticación biométrica o la mencionada cédula de ciudadanía digital, lo que cierra cualquier duda sobre la identidad del ciudadano. Este sería un paso más hacia la apropiación de la noción que hasta aquí hemos expuesto, pero después de dos años aún no ha visto la luz.

Bibliografía

AA. VV. (2017). ***Justicia y TIC.*** Bogotá D. C.: Legis.

DANE (s.f.). ***¿Cuántos somos?*** [En línea]. Recuperado de: https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivienda-2018/cuantos-somos. [Consultado el 28 de abril de 2019].

GECTI (Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática). (2005). ***Comercio electrónico.*** Bogotá D. C.: Legis.

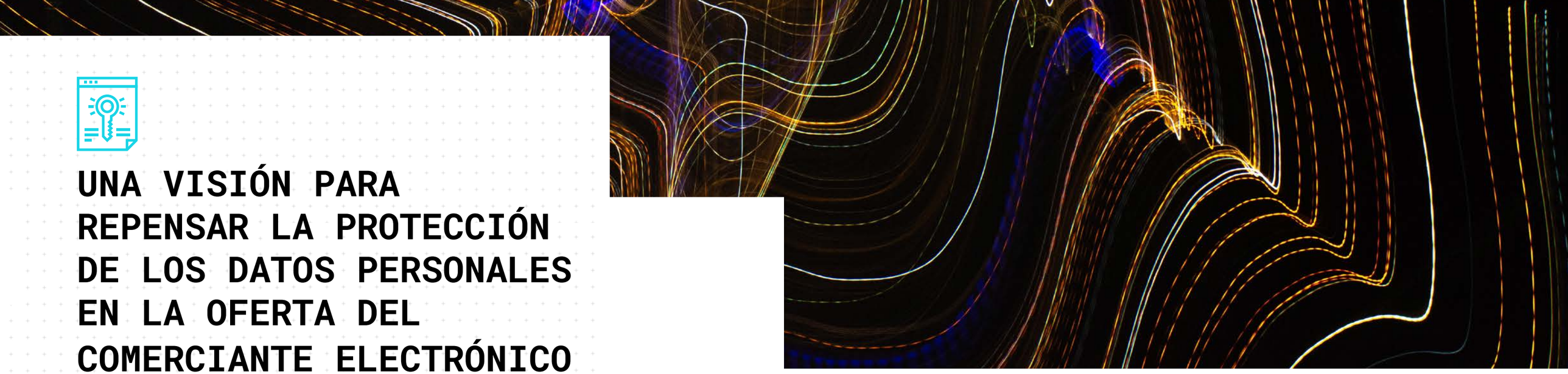
Goode Intelligence. (2015). ***Biometrics-The Must-Have Tool for Payment Security. A White Paper from Goode Intelligence***. [En línea]. Recuperado de: http://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-Intelligence-White-Paper-Biometrics-the-must-have-tool-for-payment-security.pdf. [Consultado el 22 de abril de 2019].

OECD. (2011). ***Digital Identity Management and Electronic Authentication***. [En línea]. Recuperado de: http://www.oecd.org/sti/ieconomy/digitalidentitymanagementandelectronicauthentication.htm. [Consultado el 30 de abril de 2019].

Rincón Cárdenas, Erick (2015). ***Derecho del comercio electrónico y de internet***. Segunda edición. Bogotá D. C.: Legis.

SplashData. (2018). ***SplashData Announces 100 Worst Passwords of 2018***. [En línea]. Recuperado de: https://www.sdmmag.com/articles/96013-splashdata-announces-100-worst-passwords-of-2018. [Consultado el 30 de abril de 2019].

We Are Social y Hootsuite. (2019). ***The State of Digital in April 2019: All the Numbers You Need To Know***. [En línea]. Recuperado de: https://wearesocial.com/blog/2019/04/the-state-of-digital-in-april-2019-all-the-numbers-you-need-to-know. [Consultado el 3 de mayo de 2019].



UNA VISIÓN PARA REPENSAR LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA OFERTA DEL COMERCIANTE ELECTRÓNICO

Pedro Novoa Serrano

Resumen

La sociedad de la información y el advenimiento del comercio electrónico a gran escala, que en Colombia tiene su mayor impulso con la entrada en vigencia de la Ley 527 de 1999 o Ley de Comercio Electrónico, hace de la información sobre la que se realiza algún tratamiento el gran insumo que les permite a los comerciantes acercarse a los consumidores para ofrecerles sus productos y servicios. Así, el crecimiento en el flujo de la información ha hecho que los legisladores y las autoridades del mundo enfoquen su preocupación, cada vez más, en la administración de los datos personales, teniendo como premisa fundamental para ello, principalmente en el momento de la oferta inicial, la existencia de la autorización otorgada por parte del titular de manera previa y expresa.

¿Es hora de repensar esta máxima? ¿Es la necesidad de contar con una autorización previa y expresa a cualquier tratamiento de información personal un obstáculo para el desarrollo del comercio?

A través de este escrito se invita a analizar una perspectiva que proviene desde la realidad de la oferta comercial en el comercio internacional y electrónico. Para ello se aportan diferentes recursos que abordan el problema desde el principio de la proporcionalidad entre los derechos de consumidores que buscan la protección de su información y los de empresarios que, a través de sus ventas, mantienen emprendimientos. Estos últimos, a su vez, crean millones de puestos de trabajo, por lo que su supervivencia es incontrovertiblemente necesaria para mantener el sistema de mercado predominante en las sociedades del mundo, sin cuyos aportes en materia económica no sería posible concebir nuestro actual modo de vida.

Abstract

The information society and the advent of large-scale electronic commerce, that in Colombia has its greatest impulse with the entry into force of Law 527 of 1999, better known as the Electronic Commerce Law, makes the information treatment, the great instrument that allows the merchants the approach with the consumers for the offering of their products and services. Thus, the growth in the flow of information has made lawmakers and worldwide authorities increasingly focus their concern in the management of personal data, having as a fundamental premise for this the existence of the authorization granted by the owner in a prior and express manner. Is it time to rethink this maxim? Is the need to have prior and express authorization to any treatment of personal information an obstacle to the development of trade?.

Through this paper, the readers are invited to analyze a perspective to solve that questions that comes from the reality of the initial commercial offer in the context of international and electronical trade, providing different resources that address the problem from the principle of proportionality between the rights of consumers seeking the protection of their information and those of entrepreneurs who, through their sales, maintain ventures that, in turn, create millions of jobs and whose survival is incontrovertibly necessary to maintain the worlwide predominant market system, without whose contributions, in economical terms, it would not be possible to conceive our current way of life.

01

Los aspectos generales

A partir de la entrada en vigencia de la Ley 527 de 1999 sobrevino un cambio de paradigma, un importante avance que comportó, si se permite así decirlo, "la evolución" de la venta presencial y la necesidad del papel con firma manuscrita a la negociación electrónica a través de dispositivos y plataformas que soportan el ofrecimiento y venta de productos y servicios sin necesidad de que medie un contacto físico. Este impulso ha hecho que el comercio electrónico se multiplique a ritmos agigantados, a tal punto que es posible afirmar que en unos años un almacén por departamentos no existirá físicamente y que cosas tan inconcebibles hace algunos años como la compra desde Colombia de un tapete persa en una tienda ubicada en Irán hoy en día son posibles a través de plataformas de negocios que acercan a las partes.

Así, el comercio electrónico, realizado a través de mensajes de datos, intercambio de códigos, y textos transmitidos a través de páginas de internet, redes sociales y aplicaciones conversacionales, verdaderamente internacionaliza el mercado, uniendo culturas y pueblos.

Es tal el grado de penetración que ha tenido el comercio electrónico que, para el momento en que se desarrolla este documento, se tiene establecido que tal rubro, junto con la tecnología, el petróleo y gas y la agroindustria (Gerente.com, 2019), es uno los cuatro pilares básicos por los que la economía del país será jalonada. Si esto es para el año 2019, son entonces inimaginables las perspectivas del sector para los años venideros, más aún cuando la percepción del consumidor respecto de las compras en línea ha venido mejorando sustancialmente, pasando de una lógica desconfianza inicial a la apreciación de un sinnúmero de beneficios en su utilización, tal y como se muestra en la figura 1.

Figura 1

Beneficios percibidos por comprar en línea

Base: Encuestados que utilizan internet y respondieron 2,3 o 4 en pregunta 4	664
Base: Expandida	4.333.048

Fuente: Centro Nacional de Consultoría (2019).

A lo anterior se suma el hecho de que, como es evidente por el perfil de los consumidores electrónicos, en su gran mayoría jóvenes menores de treinta años, a medida que pasen las generaciones, mayor será el uso de la tecnología para realizar las transacciones.

Esta internacionalización del mercado producto de la apertura al comercio electrónico ha conducido, por igual, a la mayor explosión de creación e intercambio de información que se haya conocido. Las cifras que se alcanzan son incomprensibles para el lector medio:

> *En 2018 había en el mundo 33 zetabytes de datos. En 2025 habrá 175, según un estudio de la consultora International Data Corporation (IDC). Un zetabyte son 1.021 bytes. Es la unidad que va después del gigabyte, terabyte, petabyte y exabyte. Todas las palabras que han sido dichas por la humanidad ocupan 5 exabytes, ni siquiera 1 zetabyte, según TechTarget. En 2010, apenas había un par de zetabytes en total* (Gerente.com, s.f.).

Es decir, en estos últimos años la humanidad ha producido, comunicado y utilizado mucha —muchísima— más información que en toda su historia pasada, y gran parte de esa información está compuesta por datos personales, entendidos estos como

> *toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

> *[…] En consecuencia, la imagen de una persona es un dato personal, al igual que lo será cualquier información que permita determinar, directa o indirectamente, su identidad, como por ejemplo, una matrícula de vehículo, una dirección IP, etc. (…)*[118].

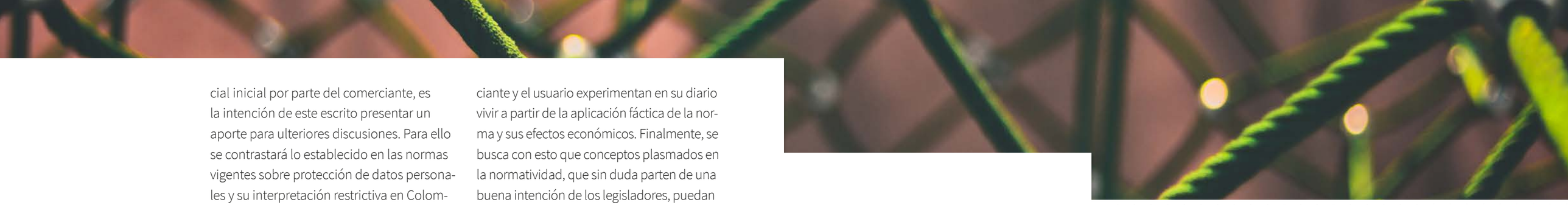
Es por tal razón que, aun cuando existe desde hace ya décadas una legislación que protege el tratamiento[119] de este tipo de información, realmente hoy su cuidado se convirtió en una preocupación principal para legisladores y autoridades de todas las latitudes. Estos han impuesto, para el efecto, reglas que cobijan desde su recolección, pasando por las formas legales de utilizarla, hasta su destrucción.

En este punto surgen una serie de inquietudes para quienes desarrollan el comercio electrónico y, por supuesto, sus usuarios, tales como: ¿contar con una autorización pormenorizada, expresa y previa para realizar cualquier tratamiento de datos personales, es como realmente se protegen los derechos de los titulares?, ¿qué derecho prima al inicio de una relación comercial: el del consumidor que no ha dado su autorización para recibir un mensaje comercial o el del comerciante que requiere dar a conocer sus productos o servicios para poder realizar sus ventas, generando para tal propósito miles de puestos de trabajo y, en consecuencia, dinamizando las economías?

Sobre estos interrogantes, particularmente en el momento de realizar la oferta comer-

118. Agencia española de Protección de Datos Personales. Tomado de Concepto del Gabinete Jurídico

119. El tratamiento es entendido como *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"* (numeral 2 del artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE —Reglamento General de Protección de Datos—, publicado en el diario oficial de la Unión Europea 4.5.2016).



cial inicial por parte del comerciante, es la intención de este escrito presentar un aporte para ulteriores discusiones. Para ello se contrastará lo establecido en las normas vigentes sobre protección de datos personales y su interpretación restrictiva en Colombia con su verificación práctica. Esto es, se examinará la regla frente a lo que el comerciante y el usuario experimentan en su diario vivir a partir de la aplicación fáctica de la norma y sus efectos económicos. Finalmente, se busca con esto que conceptos plasmados en la normatividad, que sin duda parten de una buena intención de los legisladores, puedan ser examinados y, si es posible, reconsiderados a la luz de los hechos.

02

La consideración preliminar: la necesidad de la autorización en la protección de los datos personales

Prescribe la Ley 1581 de 2012 la necesidad de contar, para el tratamiento de la información, con una autorización clara, expresa y exigible, estableciendo algunas mínimas excepciones para el efecto.

Así, los artículos 9 y 10 de la mencionada normatividad preceptúan:

ARTÍCULO 9.° AUTORIZACIÓN DEL TITULAR. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

ARTÍCULO 10. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN. La autorización del Titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
b) Datos de naturaleza pública;
c) Casos de urgencia médica o sanitaria;
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
e) Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

Frente a esto, la Corte Constitucional colombiana, en sentencia en la que se estudiaba la constitucionalidad del proyecto de ley que finalmente terminó convirtiéndose en la Ley 1581 de 2012, indicó:

Por una parte, los datos personales deben ser procesados con un propósito específico y explícito. En ese sentido, la finalidad no sólo debe ser legítima sino que la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrán recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. Cualquier utilización diversa, deberá ser autorizada en forma expresa por el Titular […].

[…] 2.6.5.2.3. Principio de libertad: El tratamiento solo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Este principio, pilar fundamental de la administración de datos, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente.

El literal c) del Proyecto de Ley Estatutaria no solo desarrolla el objeto fundamental de la protección del habeas data, sino que se encuentra en íntima relación con otros derechos fundamentales como el de intimidad y el libre desarrollo de la personalidad […][120].

Partiendo de esta premisa, la autoridad de protección de datos ha impuesto algunas medidas sancionatorias. Por citar algunas, la Resolución 788999 del 30 de noviembre de 2017, mediante la cual se impuso multa de carácter pecuniario a una empresa de domicilios[121] por realizar el tratamiento de datos sin contar o no poder probar que contaba con la autorización correspondiente; igualmente, la Resolución 13234 del 26 de febrero de 2018 impuso sanción pecuniaria, ahora a una empresa dedicada al mercadeo que, a través de marcación predictiva, realizaba encuestas telefónicas para posteriormente, si la persona contactada así lo autorizaba, adelantar un nuevo acercamiento con el fin de brindarle información de los productos o servicios de sus clientes. En este segundo caso, la Superintendencia indicó que ese primer contacto

que se tiene con los prospectos de cliente utilizando números al azar es un tratamiento sin el lleno de los requisitos impuestos por la Ley 1581 de 2012, pues la recolección de datos de sus potenciales clientes la efectuó con base en la marcación predictiva que no cambia la calidad de privacidad de estos datos más aún cuando con una llamada puede identificar al titular de la información. En este orden, es evidente que la sociedad enunciada no demostró que solicita autorización de los titulares que serán sus potenciales clientes para el tratamiento de sus datos privados […][122].

120. Sentencia C-748-11 de 6 de octubre de 2011, M. P. Dr. Jorge Ignacio Pretelt Chaljub, mediante la que la Corte Constitucional efectuó la revisión de constitucionalidad del Proyecto de Ley Estatutaria N.° 184/10 Senado, 046/10 Cámara.

121. Director de investigaciones de protección de datos personales. Resolución Número 78899 del 30 de noviembre de 2017. Radicación 15-170509.

122. Director de investigaciones de protección de datos personales. Resolución Número 78899 del 30 de noviembre de 2017. Radicación 15-170509.

Así, es claro que, de acuerdo con la aplicación que se está dando a la normatividad vigente en protección de datos personales, la autorización —no cualquiera, sino aquella previa, expresa e informada, que además se pueda demostrar— es un requisito imprescindible para realizar cualquier tratamiento sobre la información. Esto elimina de tajo las posibilidades de llevar a cabo aproximaciones para asuntos comerciales a través de datos que son obtenidos de diversas fuentes como los referidos o acudiendo a la prospectación de clientes potenciales.

En adición a lo anterior, el requerimiento de que la autorización sea informada ha llevado, a su vez, a que algunas autoridades de protección de datos personales consideren que el titular de los datos debe aceptar de forma específica y particular cada una de las finalidades para las cuales va a ser tratada su información. Tal hecho, en la práctica, se traduce en que se sugiera que quien quiera realizar un tratamiento de los datos deba obtener de su titular una aceptación expresa a cada uno de los supuestos en los que se indique el uso que se podrá darles.

Así, la exigencia de contar con una autorización y su obligatoriedad para el tratamiento de los datos ha venido constituyendo un obstáculo para la dinamización y el avance de la economía. En últimas, aunque bien intencionada, esta norma puede, además de no proteger al titular de la información —que finalmente va a terminar entregando a los grandes operadores de información todos sus datos ya sea directa o indirectamente—, hacer que las personas cuyos derechos se buscan proteger dejen de recibir información importante que puede resultar de todo su interés. Todo esto se da por cuenta de buscar garantizar de manera indiscriminada unos derechos que muy eficazmente pueden ser custodiados por otras vías, como más adelante se pretende analizar, sin crear obstáculos generalizados para el desarrollo de los negocios de pequeñas y medianas empresas de las que economías como la colombiana están conformadas.

03

Los asuntos para repasar

3.1. La internacionalización de la economía y la estandarización de los documentos en el comercio electrónico

Somos parte de la época en la que no se puede hablar de la economía de mercado sin hacer referencia a un mundo cada vez más cercano e interconectado, en el que millones de transacciones se están realizando cada día gracias al comercio electrónico. Bien lo menciona el profesor Jaime Arrubla:

> *La revolución tecnológica, y con ella, la información, ha producido una transformación en el conocimiento y en la manera en que deben trabajar las organizaciones humanas y los sistemas sociales. Se deben romper las viejas estructuras, la humanidad entera debe abrirse a los cambios de la tecnología y el saber. Pueblo o empresa que se resista al cambio, caminará indefectiblemente hacia a su aniquilación.*

> *El comercio electrónico puede contribuir en la consecución de esos fines que precisa la reorganización empresarial. Este comercio no emplea formas orales ni escritas; la contratación comercial electrónica se produce siempre entre sujetos ausentes y distantes geográficamente. Durante los tratos preliminares y al momento de la perfección del negocio jurídico, las partes se encuentran en lugares diferentes, por tanto se pasa del papel y el sonido como medios de instrumentación a los propios del comercio electrónico* (Arrubla, 2013, p. 352).

Para soportar este crecimiento sin precedentes del comercio se ha propugnado por que los comerciantes, productores y oferentes de bienes y servicios establezcan reglas claras generalizadas y precisas en el mercadeo y negociación de sus bienes y servicios.

A partir de ello se introdujeron en el mercado los contratos de adhesión, que se definen como aquellos

> *en los que una de las partes tiene una oferta inmodificable de negocio que la otra debe aceptar rechazar sin posibilidad de contraposición.*

> *También pueden entenderse como la imposición exclusiva de una única voluntad a una colectividad determinada cuyos miembros, individualmente considerados, pueden exteriorizar* a posteriori *su voluntad de aceptar la cláusula (norma) que se les impone o rechazarla, careciendo de facultad en principio para debatirla. Ejemplo: El contrato de* leasing*, fiducia, mutuo con entidad financiera, franquicia* (Peña Nossa, 2003, p. 43).

Tal tipo de contratos, dadas las particularidades de la interacción, es el de más alta utilización en las transacciones electrónicas. Para contrarrestar el posible abuso del poder que los comerciantes pueden llegar a tener sobre los consumidores individuales en estos casos, las diferentes autoridades han promovido la creación de estándares que, de ser sobrepasados en la práctica, se pueden llegar a constituir en situaciones de abuso de la posición dominante y, de ser incluidos en los contratos estandarizados, en cláusulas abusivas.

Esta es la manera como el mundo ha evolucionado en materia de protección al consumidor y es la forma que se ha encontrado más adecuada para proteger al individuo y sus derechos fundamentales en el actual ámbito de los negocios, en la medida en que permite el desarrollo de estos últimos, evitando injerencias, permisos o negociaciones previas que generen obstáculos innecesarios al desempeño de la actividad comercial.

Otras formas de negociación "antiguas" son rechazadas por resultar contraproducentes y poco eficientes, tanto para los negocios como para la propia protección de los derechos de los consumidores. Es así como todas aquellas que suponen el acuerdo concertado de aspectos puntuales de los contratos entre las partes han sido desechadas en la medida en que hacen lentos e ineficientes los procesos de comercialización y atención de las necesidades de los consumidores.

Es por tal motivo que sugerir, como punto indispensable para la protección de los datos personales, una autorización para su tratamiento que contenga la aquiescencia otorgada por parte del titular a cada una de las finalidades del uso de los datos no se compagina con el estado actual de las cosas. No es posible imaginar la carga que tal exigencia impone a entidades con grandes volúmenes de clientes que acuden a ellas buscando ser atendidos de manera expedita.

Instituciones financieras, grandes superficies, redes sociales de internet, entidades: todas ellas, que han buscado la estandarización de sus contratos basados en la evolución e internacionalización del comercio, precisamente con el fin de poder brindar un servicio adecuado, ágil, generalizado y en condiciones igualitarias a sus clientes, se verían sometidas, en caso de acoger este requerimiento, a volver a prácticas que se pensaban desechadas, en donde la discusión y el cierre de cada acuerdo tardaban días y meses, por cuenta de la presunta protección de los datos personales de esos mismos clientes a los que se buscaba prestar un mejor servicio.

Lo anterior se observa cuando de los "grandes" jugadores del mercado se trata, pero qué decir de pequeñas y medianas empresas, sin poder de negociación, a las cuales la obtención de una autorización para un acercamiento comercial les queda casi imposible.

Ahora considérese por un momento que se obtiene la autorización para el tratamiento de los datos y supóngase, por traer a colación una situación de la vida real, que se trata de una entidad que cuenta con dos millones de personas como clientes y otro millón como potenciales. No son imaginables los aprietos en que tal empresa se vería inmersa para realizar cualquier tipo de contacto si requiriera determinar en cada caso con cuál de sus clientes actuales o potenciales se podría o no comunicar en determinado sentido o con determinado fin.

3.2. La oferta comercial en el mundo globalizado del comercio electrónico

Ya clara la existencia de la globalización en el comercio internacional y su incompatibilidad con la negociación personalizada de cláusulas en los contratos, es necesario, para continuar el estudio de la aplicación práctica de la normatividad que busca proteger los datos personales, abordar ahora uno de los aspectos más relevantes para el desarrollo de las actividades mercantiles: la oferta inicial.

Bien señala el profesor Nelson Remolina: *"La red de redes no sería lo que es hoy sin la información. Los motores de búsqueda, las redes sociales digitales, el marketing y los negocios se nutren, viven, enriquecen o dependen de los datos personales. Los datos personales son el negocio de los negocios"* (Remolina, 2013).

Indica el mismo autor haciendo referencia a otros estudiosos del tema:

Barrera Duque, refiriéndose a los modelos de negocios en internet, señala que "nos preocupamos por el data protection en la medida en que los nuevos modelos de negocios online implican la utilización de información privada de los clientes con miras a segmentar y personalizar la oferta de servicios y productos. Hay mas información sobre nuestras vidas en el mercado de bienes y servicios". En otras palabras, internet es la plataforma de información más grande del mundo. Contiene enormes e incalculables cantidades de datos personales que son utilizados entre otros para fines comerciales y de negocios.

Recalca el citado autor que "las bases de datos son las fuentes de ventajas competitivas dentro de la economía digital. Identifica grupos homogéneos y permite realizar ofertas adecuadas a cada segmento o inclusive personalizadas" (Remolina, 2013).

En un pasado —no muy lejano, por cierto, y obviamente guardando las proporciones de las posibilidades al acceso y análisis de la información—, la persona que tenía un establecimiento de comercio ubicado en un determinado punto geográfico conocía a cada uno de sus clientes actuales y potenciales y sus necesidades. Tenía información de dónde vivían, cómo estaban conformadas sus familias, sus números de teléfono, sus gustos y costumbres de compra. El conocimiento de estos datos le permitía realizar ofertas de los nuevos productos a través de llamadas, volantes o recomendaciones entregadas de viva voz.

La anterior constituía una práctica que, en realidad, no difiere de lo que ahora sucede, solo que a escalas diferentes gracias al advenimiento de la sociedad de la información, a la cual debemos acostumbrarnos. Esto desmitifica prácticas que incluyen la

recolección y el análisis de datos con base en las que productores y comercializadores realizan ofertas de bienes y servicios y a partir de las cuales muchos, más cada vez, hemos adquirido productos, asistencias y asesorías que resultan de todo nuestro interés y contribuyen a nuestro bienestar. Son "mercancías" de cuya existencia y beneficios ni siquiera hubiésemos tenido noticia de no ser por la oferta inicial.

Tal es lo que se conoce en el mundo del mercadeo como "ventas en frío", de las cuales pueden encontrarse cientos de definiciones al constituir una de las prácticas de ventas más extendidas y utilizadas en la actualidad. Solo como una mención a esas definiciones se puede citar la siguiente, obtenida como resultado de una búsqueda rápida en la internet:

Venta en frío o "cold calling" es un proceso de mercadotecnia ("marketing", identifica las necesidades y deseos del mercado objetivo y se adapta para ofrecer las satisfacciones deseadas por el mercado de forma más eficiente que la competencia). La llamada en frío es típicamente el inicio del proceso de ventas conocido como telemarketing, mercadeo a la distancia o venta a distancia. Busca que el vendedor haga un empuje o "push" en un producto o servicio de un producto a un cliente que no espera esa interacción" (Thomas, 2015).

Posibilitando la realización de esas "ventas en frío", nuestro vigente Código de Comercio trata los aspectos propios de la oferta comercial de manera general, mencionando que esta puede hacerse a persona determinada o indeterminada, sin exigir previa aprobación de su parte para el efecto, e indica distintas consecuencias jurídicas según se haga de una u otra forma. Específicamente, el artículo 847 de dicho cuerpo normativo prescribe que la oferta de mercaderías a personas determinadas será obligatoria para el oferente si en el momento de realizarla no efectúa salvedad alguna sobre el particular.

Lo interesante aquí es notar que la oferta inicial a persona determinada debe realizarse dirigida a una dirección física o de correo electrónico o a un número de teléfono establecido. Datos que, a partir de la corriente que basa la protección de los datos personales de las personas naturales en la preexistencia de una autorización expresa para su tratamiento, no sería posible utilizar para realizar acercamientos básicos a los clientes potenciales.

Es decir, por cuenta de una muy bien intencionada búsqueda de la protección de los derechos de los titulares de datos personales, es posible afirmar que se decretó la muerte de las "ventas en frío", con las afectaciones económicas y sociales que esto conlleva para miles de comerciantes y trabajadores de muy diversas condiciones que derivan su sustento, precisamente, de la posibilidad de realizar acercamientos iniciales a los posibles adquirentes de los productos y servicios que ofrecen. Se trata de sujetos cuyos derechos fundamentales al desarrollo de la libre empresa y al trabajo deberían ser apreciados al determinar en cuáles instancias realmente se presenta una violación palmaria de los derechos de los titulares de los datos personales y si esta amerita una sanción.

04

Las alternativas por considerar en un mercado electrónico globalizado frente a la protección de los datos personales

Frente a estos asuntos tratados de forma sucinta y acudiendo a términos que puedan ser adecuadamente comprendidos por todos aquellos que no tienen una formación jurídica, a continuación se presentan posibles alternativas que han tenido aplicación práctica en diversas jurisdicciones. Su adaptación a nuestro entorno permitiría, a la vez que se continúa avanzando en la protección de los datos personales, eliminar obstáculos que por el hecho de basar su tratamiento en la existencia de una autorización se han generado para el comercio en la actualidad.

4.1 Veamos el principio de proporcionalidad y el análisis individual de los casos

Supongamos el caso de una persona que padece una grave enfermedad para cuyo tratamiento debe consumir medicamentos poco comunes y costosos en el mercado. Ella hace una compra por internet de sus medicinas y, a partir de esta, le comienza a ser remitida información con contenidos publicitarios de grandes descuentos para la adquisición del medicamento.

A partir de un análisis inicial de la situación, se diría que existe una absoluta y total violación de los derechos de este titular de la información. Pero, ¿no resulta de todo el interés de la persona presuntamente afectada recibir esta información?, y ¿no es aún más creíble que a partir de ella adquirirá los productos con un descuento, lo que reportará grandes beneficios para su situación económica y de salud?

Ejemplos como este se pueden contar por millones. Hace poco tiempo, mientras desarrollaba este escrito, tuve por casualidad acceso a un filme del año 1999, *Swin Vote*[123], en el que un recién nombrado magistrado de la Corte Suprema de los Estados Unidos de América se vio en la encrucijada de tener el voto decisivo en torno a la definitiva penalización o despenalización del aborto en ese país. Este juez, no obstante sus condiciones personales vida y dejando sus propias y arraigadas convicciones a un lado, dedicó su tiempo a oír y entender las posiciones de cada uno

123. Película estrenada en 1999, protagonizada por Andy García y dirigida por David Anspaugh. https://en.wikipedia.org/wiki/Swing_Vote_(1999_film)

de los extremos, esto es, aquel que abogaba por la vida del que está por nacer y aquel que abogaba por las libertades y los derechos de las mujeres gestantes. Finalmente, luego de analizar la controversia entre dos derechos igualmente válidos y necesarios, vida vs. libertad, este juez profirió su decisión apelando a ***la proporcionalidad*** entre los dos.

En el caso de la oferta en el comercio electrónico sin contar con la previa autorización del titular de la información, guardando las justas proporciones, ocurre algo similar: existe la confrontación de derechos a la que ya se aludió. Por un lado, el del titular de la información quien, sin duda, tiene derecho a su intimidad, privacidad y, por supuesto, ***habeas data***; por el otro, el del empresario que tiene derecho al desarrollo su empresa —¿de qué otra forma podría hacerlo si no es dando a conocer y ofreciendo sus productos y/o servicios?—, que se une al de miles de trabajadores que, en ejercicio de su derecho al trabajo, realizan los contactos a los posibles clientes de esos bienes con datos que han sido recogidos, ya sea de fuentes públicas, de referencias, o aun de estudios que conllevan análisis de la información.

De aquí que se plantee realizar el estudio de cada caso, basándose para el efecto en el principio del legítimo interés, que ya en el ámbito europeo ha sido llevado a norma regional a través del artículo 6 (1) (f) del Reglamento (UE) 216/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos-RGPD) que traía una similar prescripción en su artículo 7 (f):

Artículo 6
Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones[124].

Según lo establecido por el máximo órgano consultivo en materia de protección de datos de la Unión Europea[125],

el concepto de "interés" está estrechamente relacionado con el concepto de «finalidad» mencionado en el artículo 6 de la Directiva, aunque se trata de conceptos diferentes. En términos de protección de datos, "finalidad" es la razón específica por la que se tratan los datos: el objetivo o la intención del tratamiento de los datos. Un interés, por otro lado, se refiere a una mayor implicación que el responsable del tratamiento pueda tener en el tratamiento, o al beneficio que el responsable del tratamiento obtenga —o que la sociedad […]

[…] La naturaleza del interés puede variar. Algunos intereses pueden ser apremiantes y beneficiosos para la sociedad en general, tales como el interés de la prensa en publicar información sobre la corrupción gubernamental o el interés en llevar a cabo investigación científica (sujetos a las garantías adecuadas). Otros intereses pueden ser menos apremiantes para la sociedad en su conjunto o, en cualquier caso, el impacto de su búsqueda en la sociedad puede ser más dispar o controvertido. Esto puede, por ejemplo, aplicarse al interés económico de una empresa en aprender tanto como sea posible sobre sus potenciales clientes con el fin de orientar mejor la publicidad sobre sus productos y servicios.

124. Es de aclarar, para evitar equívocos sobre el particular, que en relación con este literal y su aplicación a lo que hace referencia a comunicaciones comerciales por correo electrónico u otras vías de comunicación electrónica equivalentes se discute en el ámbito europeo la necesidad de realizar una modificación sobre la Directiva 2002/58/CE del Parlamento y del Consejo Europeo —directiva sobre la privacidad y las comunicaciones electrónicas—, en el sentido en que, para poder aplicar lo descrito sobre el legítimo interés en la normativa general de protección de datos personales a ese tipo de comunicaciones, es necesario realizar una revisión sobre la directiva, que es de carácter especial, eliminando lo establecido en ella respecto de la necesidad de contar con el consentimiento previo del titular de los datos para que le sean enviadas ofertas comerciales y otras comunicaciones comerciales a través de medios electrónicos.

125. Tomado del Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE del Grupo de Trabajo del Artículo 29 recientemente reemplazado a nivel europeo por la Junta Europea de Protección de Datos (EDPB).

Tal principio tiene como base tres postulados que legitiman el uso de la información y sobre los que debe recaer cada estudio particular:

1. Identificar el interés legítimo.
2. La necesidad de procesar los datos para hacerlo posible.
3. Realizar el balance entre ese interés legítimo y los intereses de los individuos, sus libertades y derechos.

A partir de lo anterior, es dable proponer que en cada una de las situaciones se realice un estudio particular comparando la posibilidad de ejercicio de unos derechos existentes a favor del comerciante y sus trabajadores —ya sea internos o externos— frente al grado de afectación que una llamada o mensaje a través de diversos canales supone para los derechos del titular de la información.

Para esto se considera imprescindible que, como parte del análisis puntual, se tengan en cuenta las posibilidades ya existentes a favor del titular como la que trae el artículo 15 del título V de la Ley 1581 de 2012. Allí se indica que la persona puede, en ejercicio de su ***habeas data***, solicitar la supresión de su información de una determinada base de datos o para una determinada finalidad. De manera que cualquier comunicación posterior a esa petición para los fines desautorizados se considera, esta sí con razón, una inminente violación a los derechos del solicitante, que daría lugar a sanciones para el comerciante que desatiende tal requerimiento sin necesidad de entrar en discusión probatoria, más allá de la existencia de la solicitud de retiro de la base de datos y la existencia de la posterior comunicación con desautorizada[126].

126. Superintendencia de Industria y Comercio. Resolución sancionatoria 4082 del 21 de febrero de 2019, en la que se impone sanción pecuniaria a una importante entidad financiera basada en la desatención a la solicitud de eliminación de posibilidad de enviar información con la finalidad de presentar contenido comercial.

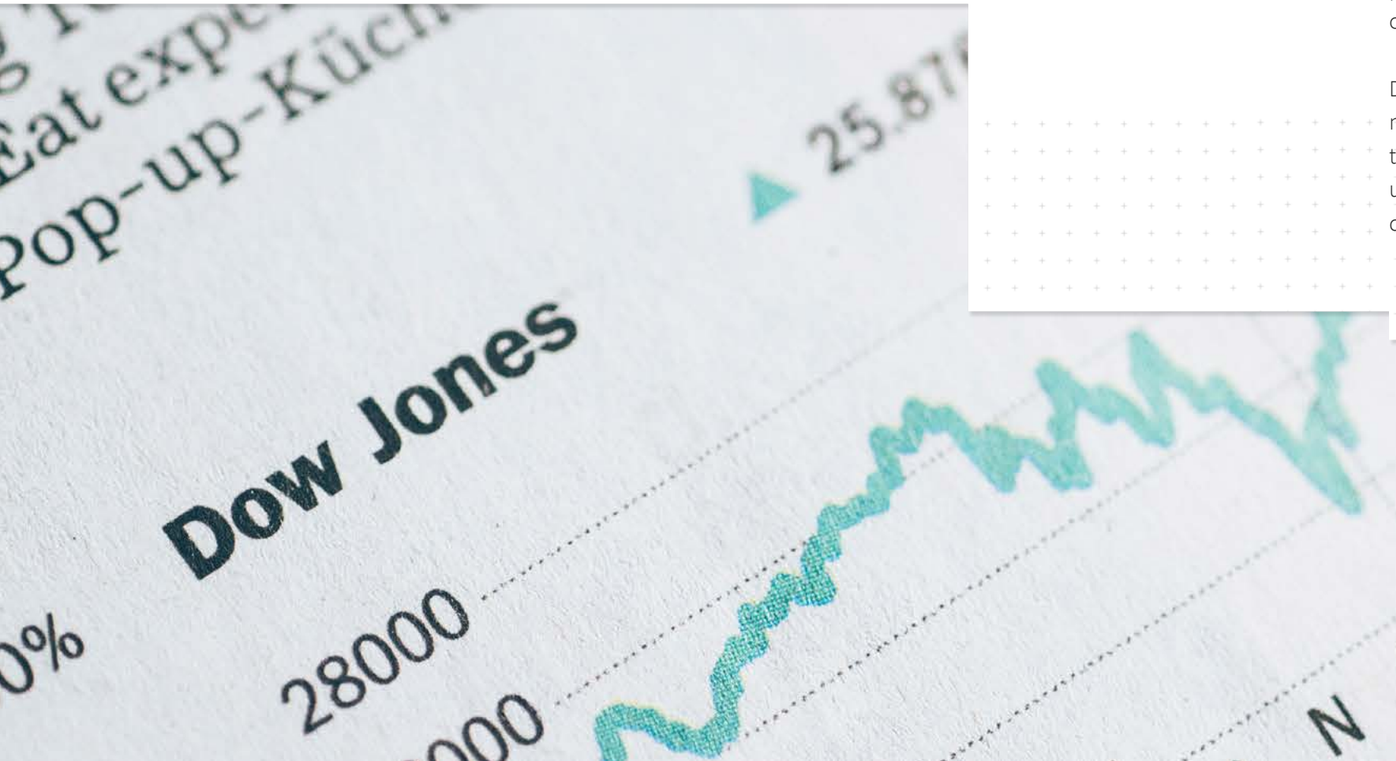
4.2. La legislación debe brindar a los consumidores herramientas que permitan su defensa sin partir de suponer su incapacidad de decisión

Como ya se vio, son incontables los casos en los que el comerciante, a partir del conocimiento de algún dato de contacto del cliente potencial, ha podido acercarse a él otorgándole la potestad de adquirir sus productos o servicios de acuerdo con su libre decisión. Así inicia toda la ruta de la realización de la oferta a través de un mensaje de datos o llamada que bien puede —o no— culminar en una negociación electrónica.

En esa medida, en lugar de generar requisitos o situaciones que puedan obstaculizar el desarrollo del comercio a través de prohibiciones generales, como la de hacer contactos a partir de información obtenida en canales públicos o actividades de referenciación sin tener una previa y expresa autorización por parte del titular de la información, valdría la pena abogar por otorgarle a ese consumidor la misma posibilidad para decidir de quién particularmente no quiere recibir comunicaciones de carácter comercial o, aún más, la potestad de escoger no ser receptor de cualquier tipo de comunicación de ese tipo.

De aquí que la propuesta sea la de optar por soluciones que permitan al consumidor tomar decisiones informadas y conscientes, tal y como sucede en el caso de las listas ***opt-out***[127], a partir de cuya utilización quien toma la decisión de no recibir información futura de una determinada empresa o marca es el propio consumidor.

127. La lista ***opt-out*** es una lista de contactos obtenida por diferentes vías de forma manual (fuentes accesibles al público, contactos de tarjetas de visita, contactos obtenidos de correspondencia propia, tomados a mano en promociones, reuniones, por teléfono) en la que se da por hecho que se disponemos de un consentimiento para realizar campañas de ***email*** marketing. En caso de utilizar estas listas, es el destinatario quien tiene la obligación de denegar (***opt-out***: optar por no) este consentimiento en caso de recibir alguna promoción a través de una campaña de ***email*** marketing (Teenvio, 2012).

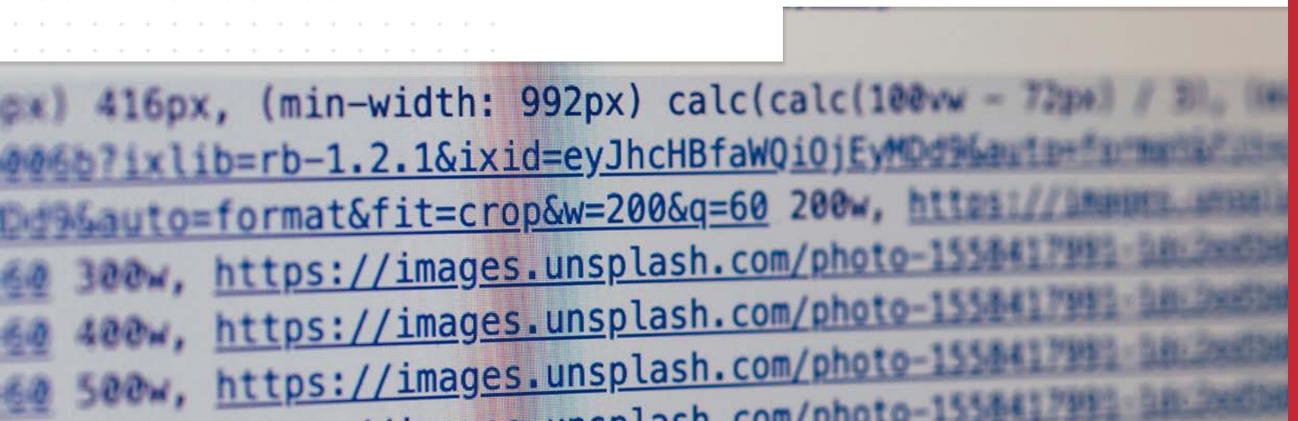


Así mismo, se plantea promover y profundizar en la implementación de otras soluciones actualmente existentes en otros territorios, como son el desarrollo de listas "Do Not Call" ("no me llames"), "listas Robinson", "lista de números prohibidos", o como quiera que se les quiera denominar, a partir de cuya construcción se otorgue al consumidor el verdadero derecho a decidir no recibir notas de mercadeo a partir del reconocimiento de su individualidad y capacidad de decisión.

Tales listas, además de proteger el derecho del consumidor de manera real y apelando a su voluntariedad, pondrían en cabeza de las partes cuyos derechos están "enfrentados" algunos deberes, y la inobservancia de estos haría que de forma automática la contraparte pudiera actuar. Esto se concreta en tomar la decisión de que, sin la actividad positiva por parte del consumidor de incluir su número en las listas "restrictivas", el comerciante pueda comunicar y ofrecer sus productos y/o servicios al titular de la información y por su parte, que en caso de inclusión de su número en las listas "restrictivas", el titular pueda acudir a las autoridades solicitando la imposición de sanciones inmediatas al comerciante que desatienda la decisión voluntaria de no recibir comunicaciones de carácter comercial o publicitario.

Es de anotar sobre este particular que, a la fecha, Colombia ya cuenta con una parcial y poco difundida lista de números excluidos, referida exclusivamente al caso de envío de mensajes de datos SMS con fines publicitarios o comerciales, la cual es regulada a través de la Resolución CRC 3066 de 2011, compilada en la Resolución CRC 550 de 2016[128] y es administrada por la Comisión de Regulación de Comunicaciones. Sin embargo, como ya se manifestó, es limitada a mensajes de datos cortos de texto, a lo que se suma que para mayo de 2019 solo se encontraban 278.703 líneas celulares registradas, menos del uno por ciento de las líneas activas en Colombia a la fecha.

128. Respuesta a consulta con radicado 2019510369 de fecha 2 de mayo de 2019 de la Comisión de Regulación de Telecomunicaciones.



4.3. Trasladar el fundamento de la protección de los datos personales de la autorización a su adecuado manejo

Antes de entrar en materia, es necesario advertir, con el fin de evitar equívocos sobre el particular, que de ninguna manera se propone la eliminación irracional de la autorización previa para el tratamiento de datos personales, particularmente cuando se trate de datos que se consideran sensibles. En tal caso estoy totalmente de acuerdo con lo prescrito por el artículo 6 de la vigente Ley 1581 de 2012, que establece:

ARTÍCULO 6.º TRATAMIENTO DE DATOS SENSIBLES. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

Dicho esto, cabe considerar que no todo tratamiento de información constituye una indebida intromisión a los derechos de los titulares de esta, tal y como sucede con la obtención de los datos de contacto de medios públicos, actividades de referenciación y marcaciones predictivas para la comunicación de ofertas de carácter comercial a través de tecnologías de la información.

Frente a tales puntos, se enfatiza que la obligatoriedad de contar con autorizaciones previas, lejos de proteger los derechos de los titulares de la información, hace que estos pierdan oportunidades de adquirir productos y servicios que satisfagan sus necesidades, al tiempo que crea un obstáculo para el desenvolvimiento de la economía de mercado, que tiene como uno de sus postulados la posibilidad para el comerciante de buscar un acercamiento a sus posibles compradores.

Al tiempo, tal obligatoriedad afecta principalmente a los pequeños y medianos comerciantes —fundamento del crecimiento de las economías en desarrollo—. A diferencia

de los grandes jugadores en el mercado, aquellos no tienen las posibilidades financieras ni la infraestructura ni mucho menos el poder para obtener de quienes conforman su mercado objetivo las autorizaciones previas que les permitan posteriormente ofrecer sus productos y servicios. Con esto se generan distorsiones en el mercado, pues mientras que grandes compañías nacionales y multinacionales trabajan con contratos estandarizados y de adhesión —pues no de otra manera podrían funcionar en la moderna economía— y obtienen autorizaciones para el tratamiento de la información sin mayores inconvenientes, el comerciante con menor capacidad de negociación queda aún más rezagado en la materia, siendo así el directamente afectado al no poder realizar una serie de actividades que tienen como insumo datos personales.

Ante tal realidad, sería recomendable abandonar como presupuesto, al menos en lo que tiene que ver en actividades comerciales electrónicas, la existencia de autorizaciones previas y expresas. De este modo podríamos centrarnos en el verdadero problema: el manejo inadecuado de la información que es obtenida por los comerciantes y la mínima existencia de procesos, políticas y controles que garanticen la seguridad en el su tratamiento y el ejercicio fehaciente del habeas data por parte de los titulares que consideren que sus derechos podrían verse afectados.

Lo anterior va de la mano del cumplimiento del principio de responsabilidad demostrada[129], según el cual, en caso de considerarse que se ha vulnerado el habeas data de los titulares de la información, corresponde a quien está realizando el tratamiento de los datos demostrar que ha implementado todas la medidas en materia documental y de procesos, capacitaciones y herramientas de seguridad que le permitan garantizar una adecuada labor en ese sentido.

Así que, luego de poner en manos del consumidor titular de la información las herramientas que le permitan de forma voluntaria solicitar la abstención de realizar con sus datos cualquier tipo de acercamiento comercial o publicitario, se debe proceder a la imposición de las sanciones de tipo administrativo, y aun penales, en caso de verificación del incumplimiento de ese principio.

129. *"[…] Principio según el cual una entidad que recoge y hace tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos […] En uno de los apartes más relevantes del Decreto 1377 de 2013, en el artículo 26, el regulador introdujo en el sistema colombiano de protección de datos el criterio de responsabilidad demostrada como una obligación en cabeza de los Responsables del Tratamiento. Igualmente, dispuso que los responsables deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012".* Tomado de la *Guía para la Implementación del Principio de responsabilidad Demostrada (Accountability)* de la Superintendencia de Industria y Comercio, pág. 5.

Conclusiones

Es cierto que en nuestros días la información es el gran tesoro que una compañía, cualquiera que sea el bien o servicio que pretenda comercializar, tiene a su haber. Su adecuado manejo para propósitos de desarrollo del negocio se vuelve esencial, particularmente en el de las operaciones virtuales, que en buena hora fueron promovidas en nuestro país por la en ese momento visionaria Ley 527 de 1999, cuyos veinte años de vigencia conmemoramos en esta publicación.

Es por tal motivo que, en materia de protección de los datos personales, Colombia, siguiendo el ejemplo de otras naciones, optó por imponer un completo cuerpo legislativo que incluye para quienes hacen su tratamiento serias sanciones de carácter, tanto administrativo como penal, en caso de incumplir los lineamientos trazados para su recolección y uso.

Tales directrices encuentran su sustento en dos principios que se han considerado básicos en cuanto a la posibilidad de manejar información que pueda tener un carácter personal: a) la libertad del titular, que se traduce en la posibilidad que tiene de permitir o no la recolección y/o uso de sus datos, y b) la finalidad del tratamiento, que conlleva, para el custodio de la información, la obligación de hacer con ella únicamente aquello para lo que ha obtenido una aprobación, ya sea por la ley o por el titular de la información.

Tales principios básicos dan lugar a un sistema regulatorio basado en la autorización para el tratamiento de la información, sin cuya previa existencia no resulta posible almacenar, mantener, usar o transmitir datos personales, tal y como lo indican pronunciamientos de nuestras autoridades que ya han sido traídos a colación.

Sin embargo, este hecho, cuyo buen propósito de cuidado del consumidor no se puede poner en duda, encamina a dos postulados con los que debo estar en profundo desacuerdo por las implicaciones que tienen:

El consumidor es incapaz de pensar, tomar decisiones y actuar en consecuencia, por lo que el Legislador, en su "sabiduría", debe crear escudos que impidan el acercamiento de los comerciantes abusadores de su minusvalía.

El comerciante que usa los datos personales de contacto para ofrecer sus productos a un consumidor potencial es, al menos, un probable delincuente que puede, por lo mismo, incluso ser condenado penalmente[130]. Así pues, de forma alguna puede realizar directamente o a través de terceros actividades de acercamiento a potenciales clientes que puedan involucrar datos personales, sin tener una previa y expresa autorización por parte del destinatario de sus actividades de comercialización de sus servicios.

En torno al primero de los postulados, es de recordar que una de las ventajas del comercio electrónico es que quienes desarrollan sus actividades comerciales a través de este tienen la posibilidad de obtener un conocimiento profundo del consumidor mediante las tecnologías de la información. Esto a su vez les otorga grandes posibilidades de

130. Artículo 269F del Código Penal Colombiano: *"ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".*

satisfacer sus reales necesidades, entre otras cosas, con ofertas de productos y servicios que el consumidor beneficiado, si no fuera porque recibe una oferta inicial por parte de parte de un tercero, podría no llegar a conocer. Así, crear para el consumidor una externa y previa protección que define su posibilidad de recibir información que puede llegar a ser de su interés y beneficio no resulta lógico.

Es mucho más racional dejar que sea el propio consumidor quien, en uso de su libre albedrío y criterio, decida si desea o no recibir ofertas de productos o servicios y, de recibirlas, que sea él quien tenga la posibilidad de determinar si quiere continuar recibiéndolas de una determinada empresa o definitivamente rechazarlas. Mientras eso sucede, se exhorta a concebir la idea de que no todo uso de la información es malo en sí mismo, aun sin contar con la autorización para su tratamiento.

Así mismo, se debe considerar realizar el análisis para cada caso en particular y sopesar la existencia de una real vulneración del derecho a la protección de los datos personales de los titulares de la información. Para ello, es preciso partir del examen de algo ciertamente importante en el mundo de los negocios: el principio de la buena fe, el cual ***"tiene especial campo de acción en el campo del derecho electrónico, precisamente por la inmaterialidad, en principio, de las manifestaciones de voluntad y de los mismos contratos"*** (Arrubla, 2013, p. 359).

De manera que propongo que la investigación del comportamiento del comerciante al tratar datos personales para ofrecer sus productos y servicios se centre en si está validado por un fin legítimo, que adicionalmente tiene una previsible utilidad en la posibilidad de satisfacer expectativas a los consumidores titulares de la información.

Todo esto con un mensaje claro: propugno por la eliminación de la exigencia generalizada de una autorización previa y expresa como principal fundamento para poder realizar el tratamiento de datos personales en materia de la oferta comercial. En cambio, abogo por que la protección de los titulares de la información se fundamente en: a) la ampliación y difusión por parte del estado de herramientas que permitan su aislamiento voluntario (listas de no llamar); b) la exigencia a los empresarios de contar con verdaderas y documentadas políticas y procesos que permitan al titular de los datos ejercer frente a ellos su derecho al ***habeas data*** bajo la perspectiva de ser penados con importantes sanciones en caso de no cumplirlo, y c) la valoración particular en el juzgamiento de cada uno de los casos que se pongan en conocimiento de las autoridades con base en la proporcionalidad entre los derechos pugna.

Bibliografía

Arrubla, Jaime Alberto (2013). ***Contratos mercantiles. Contratos contemporáneos***. Tercera edición.

Centro Nacional de Consultoría. (2019). ***Medición de indicadores de consumo del Observatorio eCommerce***. [En línea]. Recuperado de: https://www.mintic.gov.co/portal/604/articles-98220_Inf_eCommerce.pdf.

Gerente.com (s.f.). La industria del eufemismo: quién tiene y cuánto cuestan tus datos. Artículo publicado en la revista gerente. [En línea]. Recuperado de: http://gerente.com/co/new-rss/la-industria-del-eufemismo-quien-tiene-y-cuanto-cuestan-tus-datos/.

Gerente.com (2019). Los cuatro sectores que más empleo generarán en Colombia en 2019. [En línea]. Recuperado de: http://gerente.com/co/sectores-mas-empleo-generaran-colombia-2019/. [Consultado el 31 de marzo de 2019].

Peña Nossa, Lisandro (2003). ***De los contratos mercantiles. Negocios del empresario***. Primera edición. Ediciones Universidad Católica de Colombia.

Remolina Angarita, Nelson (2013). ***Tratamiento de datos personales***. Primera edición.

Teenvio.com (2012). ***Listas Opt-out, Opt-in y doble Opt-in, qué son y cómo funcionan***. [En línea]. Recuperado de: https://www.teenvio.com/es/consejos/listas-opt-out-opt-in-doble-opt-in-que-son-como-funcionan/.

Thomas, Katrina (2015). ***Venta en frío***. [En línea]. Recuperado de https://prezi.com/oywwtpgums7l/venta-en-frio/.

LAS SOCIEDADES ESPECIALIZADAS EN DEPÓSITOS Y PAGOS ELECTRÓNICOS COMO UNA INNOVACIÓN EN EL SISTEMA FINANCIERO COLOMBIANO

The specialized companies in electronic deposits and payments as a innovation in the Colombian financial system

Sergio Rodríguez Azuero[131]

Resumen

El sistema financiero es de vital importancia para el desarrollo de la economía del país. Esto se sustenta en la medida en que por intermedio de este confluyen las necesidades de los agentes deficitarios y superavitarios, permitiendo así una asignación eficiente de los recursos. Por ende, es trascendental trabajar en el diseño de una política de inclusión financiera, en aras de que un mayor grupo poblacional pueda acceder a servicios y productos financieros. Atendiendo a esta necesidad, y teniendo en cuenda el desarrollo tecnológico que permite utilizar nuevas vías de acceder al sector, en el año 2014 se crearon las sociedades especializadas en depósitos y pagos electrónicos. Estas constituyen un pilar fundamental para que sectores de la población tradicionalmente no bancarizada puedan acceder formalmente al sistema financiero y así volverlo más robusto, profundo y eficiente. Bajo ese marco, el presente artículo tiene por objeto estudiar el régimen legal de las sociedades especializadas en depósitos y pagos electrónicos. A su vez, se pretende analizar cómo, a partir de su creación, se amplió el panorama del sistema financiero.

Palabras clave: inclusión financiera; sistema financiero; servicios financieros transaccionales; sociedades especializadas en depósitos y pagos electrónicos.

131. Abogado de la Universidad del Rosario. Profesor emérito y honorario. Autor de los libros ***Contratos bancarios*** y ***Negocios fiduciarios. Su significación en América Latina***. Miembro de la Academia Colombiana de Jurisprudencia, del Instituto Iberoamericano de Banca y Finanzas y de The International Academy of Estate and Trust Law. Socio fundador de CMS Rodríguez-Azuero.

Abstract

The financial system has a vital importance for the development of the economy of the country. The above, since through this system confluence the needs of the deficit and surplus agents, allowing an efficient allocation of resources. Thus, it is necessary to work in the design of a financial inclusion policy, which consents to the need to facilitate access to financial services and products to most of the population.
Attending to this need, in 2014 they were created the specialize companies in electronic deposits and payments as a fundamental pillar so that traditional unbanked population could access to the financial system and in this way, move towards a robust, deep and efficient financial system.
This paper has for purpose analyzes the legal regime of the specialized companies in electronic deposits and payments and how the financial system was modified with its creation in order to move towards the objective of financial inclusion.

Key words: financial inclusion, financial system, transactional financial services, specialized companies in electronic deposits and payments.

Introducción

A pesar de que la banca en Colombia ha logrado importantes avances en materia de acceso a productos financieros, todavía es común que en ciertos sectores de la población se recurra a mecanismos informales como el ahorro en efectivo y los denominados préstamos "gota a gota", en lugar de acudir formalmente al sistema financiero. Esta realidad de la población no bancarizada puede obedecer a diferentes motivos, dentro de los cuales se destacan la falta de educación financiera, el andamiaje regulatorio propio del sistema financiero que hace difícil su acceso, los elevados costos y los bajos niveles de cobertura del sistema.

Adicionalmente, aún persiste el reto de que los consumidores financieros utilicen activamente sus productos y no se limiten a abrir una cuenta sin realizar movimientos a través de esta. Para el año 2015, en la región de América Latina y el Caribe cerca del 58,4 % de los productos financieros registrados se encontraban en estado inactivo (Asociación Bancaria de Colombia, 2015), y en Colombia, según cifras entregadas en la 53.ª Convención Bancaria, había 41 millones de cuentas de ahorro —tradicionales y electrónicas— que se encontraban inactivas y abandonadas (El Tiempo, 2018).

Con este panorama, el desafío que enfrenta Colombia es mejorar y promocionar los servicios financieros transaccionales[132] con el fin de que los dineros que ya han ingresado al sistema financiero circulen de forma recurrente y no sean utilizados únicamente como medio para convertirlos en efectivo y realizar las transacciones bajo esta modalidad. Con esto mente, se crearon las sociedades especializadas en depósitos y pagos electrónicos (SEDPE) como compañías dedicadas exclusivamente a servir como instrumento puramente transaccional.

Dentro de ese marco, el presente artículo tiene por objeto estudiar el régimen legal de las SEDPE, al tiempo que analiza cómo, a partir de su creación, se modificó el panorama del sistema financiero. Para este efecto, el artículo se dividirá en cinco secciones: (i) naturaleza legal de las SEDPE, (ii) regulación prudencial aplicable a las SEDPE, (iii) diferencias de las SEDPE con los establecimientos de crédito, (iv) las SEDPE como una figura innovadora en el sistema financiero colombiano y (v) conclusiones.

132. De acuerdo con la exposición de motivos de la Ley 1735 de 2014, hacen parte de los denominados servicios financieros transaccionales los giros, las transferencias y los pagos.

01

Naturaleza legal de las SEDPE

Las SEDPE fueron creadas en el año 2014 a partir de la expedición de la Ley 1735. Esta tuvo un impacto importante no solo a nivel del sistema financiero, sino también a nivel social, pues se conoció como la ley a partir de la cual se promovía el acceso electrónico a los servicios financieros transaccionales. De este modo la regulación se veía como un instrumento adecuado para facilitar el acceso al sistema y luchar contra la exclusión, la marginalidad y la inequidad social en el país[133]. El espíritu del Legislador de la época era, pues, el de poner en marcha la estrategia de inclusión financiera incluida en el Plan Nacional de Desarrollo 2014-2018 (Asociación Bancaria de Colombia, 2015), siguiendo al efecto los esfuerzos que desde hace varios años vienen haciéndose en ese sentido.

Así, para darles nacimiento legal a las SEDPE y cumplir con los objetivos descritos anteriormente, se optó porque estas sociedades tuvieran la calidad de instituciones financieras cuyo objeto exclusivo estaría compuesto por cuatro actividades: (i) captar recursos del público a través de depósitos electrónicos, (ii) realizar pagos y traspasos, (iii) tomar préstamos dentro y fuera del país destinados específicamente a la financiación de su operación, y (iv) enviar y recibir giros financieros[134]. Al respecto, es necesario hacer unos breves comentarios.

En primer lugar, el hecho de que el Legislador haya decidido que las SEDPE tuvieran la calidad de instituciones financieras necesariamente implica que les sean aplicables las normas generales consagradas en el Estatuto Orgánico del Sistema Financiero (EOSF)[135]. Así, las normas relativas al procedimiento de constitución de instituciones financieras consagrado en el artículo 53 del EOSF, los regímenes de fusión, adquisición, conversión, escisión y cesión de activos, pasivos y contratos consignados en los artículos 55 a 68 del EOSF, y las reglas sobre administración y control de las instituciones financieras establecidas en los artículos 72 a 79 del EOSF, entre otras, resultan aplicables para estas nuevas instituciones financieras.

Adicionalmente, teniendo en cuenta que las operaciones autorizadas para las SEDPE constituyen una actividad financiera relacionada con el manejo de recursos captados del público, y dado el carácter de interés público que tienen estas actividades de acuerdo con el artículo 335 de la Constitución Política, las SEDPE estarán sujetas a la inspección, vigilancia y control de la Superintendencia Financiera de Colombia y, para poder entrar a operar, necesitarán de autorización previa del Estado[136].

En segundo lugar, de las operaciones autorizadas para las SEDPE y que constituyen su objeto social, se infiere que estas instituciones están ideadas para proveer servicios financieros transaccionales, es decir, servicios destinados a la gestión de actividades operativas como la gestión de pagos y la realización de transacciones. Esto resulta ser de suma importancia

133. Exposición de Motivos de la Ley 1735 de 2014.

134. Artículo 1 de la Ley 1735 de 2014.

135. Las normas que resulten aplicables dependerán, en todo caso, de la naturaleza y las operaciones autorizadas para las SEDPE.

136. Sobre este particular, se debe señalar que, para la autorización previa del Estado, se tomó la decisión de crear una nueva licencia financiera de tipo simplificado a la que pueden acceder las sociedades que desean operar como SEDPE en el sistema financiero colombiano.

puesto que este tipo de servicios son necesarios para el adecuado funcionamiento del sistema por cuanto permiten que el dinero fluya dentro del marco del sistema financiero y no por fuera de este, a través de mecanismos informales.

Como se anticipó, las SEDPE están ideadas para incluir en el sistema financiero a las personas tradicionalmente alejadas de este. Por tal razón, el Regulador estableció en el Decreto 1491 de 2015[137] un trámite simplificado para que las personas naturales que cumplan con cierto perfil tengan facilidad para acceder a los servicios prestados por las SEDPE. Así, quienes depositen un máximo de tres salarios mínimos legales mensuales vigentes, el monto acumulado de sus operaciones debito en un mes calendario no supere tres salarios mínimos legales mensuales vigentes y sean titulares de un solo deposito electrónico por entidad, podrán sujetarse al trámite simplificado.

Este tipo de límites para facilitar el acceso al sistema financiero no es algo nuevo en la regulación; corresponde a una muy vieja tradición. En efecto, en la legislación bancaria colombiana, con la promulgación de la Ley 25 de 1923, se introdujeron las denominadas secciones de ahorro. Con esto se habilitó a los establecimientos bancarios de la época para abrir y mantener secciones especiales mediante las cuales se recogieran las pequeñas economías de la colectividad para invertirlas en obligaciones con intereses (Ángel, 1959). Lo interesante del caso es que en el artículo 114 de la Ley 25 de 1923 se señaló que "El monto de los depósitos de la sección de ahorros al crédito de un individuo, en cualquier tiempo, no podrá exceder de tres mil pesos ($3.000). […]".

Así, a lo largo de la historia el sistema financiero ha contado con instrumentos ideados para tal fin. Hemos señalado, por ejemplo, que la noción de los depósitos de ahorro se vincula a la necesidad de brindar a los pequeños ahorristas la posibilidad de depositar su dinero en condiciones que estimulen su tendencia a ahorrar frente a otras opciones más enfocadas a la generación de renta, como sucede con otro tipo de productos como los depósitos a término (Rodríguez Azuero, 2013).

Ahora, lo anterior no significa que las personas que por sus condiciones económicas sobrepasen estos límites no puedan hacer parte del sistema financiero. Puntualmente, en lo que a las SEDPE se refiere, si se exceden los límites establecidos en el Decreto 1491 de 2015, la persona no podrá hacer uso del trámite simplificado de vinculación, sino que deberá surtir el trámite ordinario, pero, en todo caso, podrá hacer uso de los servicios prestados por las SEDPE.

En tercer lugar, llama la atención la prohibición establecida en el parágrafo primero del artículo 1 de la Ley 1735, según el cual "En ningún caso las sociedades especializadas en depósitos y pagos electrónicos podrán otorgar crédito o cualquier otro tipo de financiación". Esta prohibición parecería tener sustento al analizar la transacción de una SEDPE cuando opera a través de corresponsales. Teniendo en cuenta el funcionamiento y la estructura de la operación, se podría pensar que la SEDPE está otorgando un crédito al corresponsal ya que, en este supuesto, existe un lapso entre el momento en que corresponsal recibe los recursos de un cliente y en que el corresponsal entrega los recursos a la SEDPE. Sin embargo, esta interpretación resulta ser errónea, pues se trata de un manejo operativo, sustentado contractualmente a través de un mandato, por lo que este argumento no serviría para justificar la prohibición del parágrafo primero[138].

Así las cosas, si se tiene en cuenta que lo que está expresamente proscrito en la legislación colombiana es la captación sin autorización del Estado —y esta actividad se les permitió a las SEDPE—, no hay una razón técnica ni jurídica que explique por qué los dineros captados por ellas deban mantenerse en depósitos a la vista[139], y que se consagre la expresa prohibición que tienen las SEDPE para otorgar créditos.

Ahora bien, teniendo en cuenta que en Colombia el gravamen a los movimientos financieros se ha constituido en un mecanismo perverso que induce a la realización de operaciones en efectivo, hay un punto que, pese a no ser de la naturaleza legal de las SEDPE, consideramos de importancia y, por ende, se trae a colación en la presente sección.

Nos referimos al tratamiento tributario, particularmente en lo que respecta al gravamen a los movimientos financieros, aplicable a las transacciones de retiro y disposición de los dineros depositados en depósitos electrónicos. Sobre este particular, el inciso 3 del artículo 2 de la Ley 1735 de 2014 señala que "[…] Los retiros o disposición de recursos de estos depósitos estarán exentos del gravamen a los movimientos financieros en los términos del numeral 25 del artículo 879 del Estatuto Tributario".

Lo anterior es de resaltar pues pone en evidencia la intención del Legislador de conformar un entorno verdaderamente favorable para promover la inclusión financiera en el país. No solo se limita a innovar en materia de regulación financiera, sino que, paralelamente, introduce disposiciones de tipo fiscal al ordenamiento jurídico en aras de reducir las transacciones en efectivo y promover la utilización de los servicios prestados por las SEDPE. Y esto, repítase, favoreciendo a depositantes de pequeños recursos por definición.

De lo expuesto, resulta claro que la naturaleza legal de las SEDPE es la de una institución financiera, sujeta a las normas generales del EOSF, diferente a los establecimientos de crédito, a las sociedades de servicios financieros, a las sociedades de capitalización y a las entidades aseguradoras, bajo la inspección, vigilancia y control de la Superintendencia Financiera de Colombia, con una licencia financiera de tipo simplificado para operar, con un régimen de regulación prudencial especial y con un beneficio fiscal, en lo que al gravamen a los movimientos financieros se refiere, para los depositantes que retiren o dispongan de estos recursos.

137. Artículo 4 del Decreto 1491 de 2015.

138. Esta posición la sostuvo la Unidad de Regulación Financiera en el documento ***Reglamentación complementaria de las Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPE)***, publicado el 10 de febrero de 2017.

139. Esto podría ser una justificación en la medida en que una de las principales características de los depósitos a la vista es que la exigibilidad de los saldos, por parte del depositante, puede producirse en cualquier momento y sin previo aviso. Con lo cual, teniendo en cuenta que las SEDPE deben tener los recursos captados en depósitos a la vista, podría existir el riesgo de que la SEDPE no tenga los recursos disponibles cuando le sean exigidos. Sin embargo, la solución a esta problemática está en la figura del encaje bancario, por lo que estimamos que este argumento no es correcto.

02

Regulación prudencial aplicable a las SEDPE

Como ha quedado expuesto en la sección anterior, las SEDPE constituyen una nueva institución financiera diferente a las existentes que, dados su carácter simplificado, sus actividades autorizadas y su finalidad, requieren de un régimen de regulación prudencial especial.

En ese sentido, es importante señalar que, aunque el proceso de concreción de la política de inclusión financiera es necesario para el desarrollo de la economía del país, este debe realizarse de forma ordenada y armónica. Así, tal y como lo señala el Banco Mundial en el World Financial Development Report, todas las iniciativas regulatorias que propendan a impulsar la inclusión financiera deberán realizarse preservando la estabilidad del sistema y la protección del consumidor financiero.

En atención a lo anterior, la regulación colombiana ha diseñado un régimen de regulación especial que se adapta a las necesidades de esta nueva figura pero que, al mismo tiempo, vela por los intereses de los demás participantes del mercado.

Así, en lo que se refiere a las reglas de capital mínimo, se debe advertir que en materia de constitución de SEDPE estas son mucho menos exigentes que, por ejemplo, las aplicables para la constitución de un establecimiento de crédito. Esto se justifica en el hecho de que las actividades autorizadas para una y otra institución son muy diferentes y, por ende, el respaldo patrimonial necesario también lo es. Ahora bien, esto necesariamente implica la presencia de una reglamentación clara respecto de los límites máximos para las transacciones que se realicen a través de una SEDPE, puesto que, en todo momento y con el fin de proteger la estabilidad del sistema, debe existir una relación proporcional para la razón entre patrimonio y los depósitos captados por la entidad, en tanto y en cuanto que, de no ser así, se podrían configurar eventos que repercutirían en afectaciones no solo a los depositantes, sino al sistema financiero en general[140].

En cuanto a los riesgos a los que están expuestas las SEDPE, vale decir que estos son muy diferentes a los de la mayoría de las instituciones financieras, máxime cuando, a diferencia de los intermediarios, no asume el natural riego del sector que es el crediticio. Sin embargo, hay un punto de total relevancia que es compartido hoy por todas las instituciones del sistema financiero, el cual es el riesgo de lavado de activos y financiación del terrorismo. Sobre este particular, consideramos pertinentes los siguientes comentarios.

En primer lugar, es necesario destacar que, de acuerdo con el artículo primero de la Ley 1735, las SEDPE deberán cumplir con las mismas disposiciones aplicables a las demás instituciones financieras en materia de lavado de activos y financiación del terrorismo. Esto resulta evidente en la medida en que, siendo el sistema financiero el canal para que fluya formalmente el dinero, y las SEDPE, las instituciones especializadas en prestar servicios financieros transaccionales, el riesgo de que ingresen dineros provenientes de ilícitos es muy alto. Por este motivo, lo mínimo que se le podría exigir regulatoriamente a una SEDPE es que tenga un adecuado sistema de administración del riesgo de lavado de activos y financiación del terrorismo.

En segundo lugar, y en línea con lo señalado anteriormente, consideramos que una debida estructura de límites transaccionales es un mecanismo idóneo para mitigar, en gran medida, el riesgo de lavado de activos y financiación del terrorismo. Por lo tanto, las SEDPE, en la estructuración de los sistemas de administración de este riesgo, deberán dejar expresamente señalados los límites aplicables a las transacciones. Sin embargo, dado que los montos que se manejan por clientes y operaciones son de suyo modestos, hay que entender que el riesgo nace mitigado por esa circunstancia, por lo que es necesario establecer otros mecanismos de control probablemente ligados no tanto al límite natural de las operaciones, sino al número y frecuencia de ellas. También es preciso entender que esa misma circunstancia conduce a que si el monto de las operaciones realizadas en el mes "super[a] 3 salarios mínimos legales mensuales vigentes", el titular deba someterse a un procedimiento más complejo de revelación ante el banco para hacer efectivo una especie de mandato socrático contemporáneo que se le impone, esto es, "Conoce a tu cliente". Solo así podrá entender el porqué de la naturaleza y frecuencia de las operaciones llevadas a cabo.

Paralelamente al riesgo de lavado de activos y financiación del terrorismo, las SEDPE también están expuestas a sufrir riesgos operativos y de seguridad en el manejo de efectivo que reciban, por lo que también los deberán monitorear y controlar efectivamente. Así las cosas, si bien las SEDPE no están sometidas a sufrir riesgos como lo son el de crédito, de liquidez, de mercado y de contraparte, entre otros, como lo están otras instituciones pertenecientes al sistema financiero, sí están expuestas a otro tipo de riesgos que, dada su naturaleza, son igualmente importantes

140. Estos límites quedaron establecidos en el Decreto1491 de 2015, en virtud del cual se modificó el Decreto 2555 de 2010 con el fin de incluir la reglamentación aplicable a las SEDPE.

y se deben gestionar a través de sistemas de administración de riesgos.

De otra parte, en lo que se refiere a la protección al consumidor financiero —tema no menor, y más si se trata de personas tradicionalmente excluidas y marginadas del sistema financiero que probablemente no tienen mucha experiencia en la materia—, se deben realizar algunos comentarios.

La Ley 1328 de 2009 creó el régimen de protección al consumidor financiero, el cual incluye derechos y deberes de los consumidores y de las entidades financieras, pero con un claro enfoque de proteger a los primeros. Este régimen, al cual están sujetos tanto los consumidores como las entidades vigiladas por la Superintendencia Financiera de Colombia, se edificó a partir de tres elementos esenciales: (i) suministro de información, (ii) debida diligencia en la prestación de los servicios y (iii) incorporación de la figura de la defensoría del cliente.

En nuestro sentir, teniendo en cuenta lo dispuesto por la Ley 1328 de 2009, el régimen de protección al consumidor financiero es aplicable para las SEDPE y para sus clientes, posición que fue acogida por el Regulador, el cual incluyó como una obligación de las SEDPE la de contar con un defensor del consumidor financiero[141].

Por otra parte, pero también como una herramienta diseñada para la protección del consumidor financiero, la Ley 1735 señaló expresamente en el parágrafo segundo del artículo 1 que los depósitos captados por las SEDPE estarán cubiertos por el seguro de depósito administrado por el Fondo de Garantías de Instituciones Financieras.

Así pues, es claro que la creación de las SEDPE como un instrumento más para alcanzar las metas de inclusión financiera se diseñó de tal forma que no se fueran a ver afectados ni el sistema financiero ni los agentes que participan en él.

141. Artículo 2.34.2.1.1 del Decreto 2555 de 2010.

142. Artículo 2.34.1.1.1 del Decreto 2555 de 2010.

03

Diferencias de las SEDPE con los establecimientos de crédito

Debido a la posibilidad que tienen las SEDPE de captar recursos a través de depósitos electrónicos, estas instituciones podrían llegar a confundirse con los establecimientos de crédito. Más aún si se tiene en cuenta que por expresa disposición legal es posible que las SEDPE puedan prestar su red a otras entidades financieras[142] para que estas la aprovechen y para que los establecimientos de crédito pueden participar en el capital social de las SEDPE[143].

Por ello es claro que no es posible equiparar a las SEDPE con los establecimientos de crédito. En primer lugar, por cuanto fueron creadas como instituciones financieras independientes, pero, al margen de esta categorización, existen diferencias sustanciales en las actividades autorizadas para una y otra entidad que las separan. Veamos.

La actividad de captación está autorizada tanto para SEDPE como para establecimientos de crédito. Sin embargo, mientras las SEDPE únicamente están autorizadas para captar a través de depósitos electrónicos, los establecimientos de crédito lo pueden hacer por esta vía pero también a través de otras modalidades clásicas; por ejemplo, a través de cuentas corrientes, cuentas de ahorro o depósitos a término. En ese mismo sentido, si bien las SEDPE están autorizadas para hacer pagos y traspasos, no lo están para realizar cobros de deudas, como sí es el caso de los establecimientos de crédito, quienes incluso tienen áreas especializadas dedicadas a ejercer esta labor[144].

En cuanto a la actividad autorizada de las SEDPE de actuar como agente de transferencia para recibir y entregar dinero —realizar pagos y traspasos—, también existen diferencias importantes con los establecimientos de crédito, por cuanto estos últimos tienen autorizado el registro de bonos u otras constancias de deuda[145].

Quizás la diferencia más notoria entre estos dos tipos de instituciones financieras radica en que, como ya se resaltó, las SEDPE tienen prohibido otorgar créditos e invertir los recursos captados, mientras que estas son operaciones inherentes a la naturaleza de los establecimientos de crédito.

143. Artículo 4 de la Ley 1735 de 2014.

144. La explicación de la prohibición de r ealizar cobros está en la exposición de motivos, en el apartado en el que se explica el literal c) (pág.8).

145. Exposición de motivos de la Ley 1735 de 2014.

04

Las SEDPE como una figura innovadora en el sistema financiero colombiano

Así las cosas, lo cierto es que con la expedición de la Ley 1735 de 2014 se creó una institución financiera completamente novedosa dentro del sistema financiero, pues para tal fecha no existía en el esqueleto del sistema financiero una entidad especializada en la prestación de servicios financieros transaccionales utilizando instrumentos electrónicos.

Todo esto forma parte de la apuesta por los productos transaccionales electrónicos. Según cifras de la Asociación Bancaria de Colombia, para el año 2015 había "[…] más de cinco millones de cuentas de productos transaccionales desarrollados por la banca: las Cuentas de Ahorro Electrónicas (CAE) ascendieron a 3,3 millones, las Cuentas de Ahorro de Trámite Simplificado (CATS) a cerca de 104 mil y los Depósitos Electrónicos a 2.3 millones de cuentas […]" (Asociación Bancaria de Colombia, 2015).

La verdadera importancia que representó la creación e incorporación de las SEDPE en el sistema financiero consistió en que, a la fecha de su creación, existían productos electrónicos, de acceso y trámite simplificado, mediante los cuales se buscaba ampliar la cobertura del sistema financiero y llegar a todos los rincones de la geografía nacional, pero no se contaba con una institución financiera especializada en la prestación de dichos servicios financieros transaccionales para pequeños depositantes.

Con la creación de las SEDPE el panorama del sistema financiero colombiano cambió en la medida en que un jugador diferente a los tradicionales ingresó al sistema para captar recursos del público y fungir como agente para las transacciones de personas generalmente excluidas de tal entorno. Esto, sin lugar a duda, modificó la estructura de las entidades autorizadas por el Estado para realizar la actividad de captación.

Así mismo, y con la posibilidad que se le otorgó a las SEDPE de acudir ante la Superintendencia Financiera de Colombia para solicitar una licencia simplificada con miras a ejercer sus operaciones, se dio un paso muy importante hacia la flexibilización del acceso de las compañías para realizar actividades financieras, bursátiles y aseguradoras. Esto es de gran importancia para permitir que emprendimientos de prestación de servicios financieros surjan y no queden a la deriva por falta de autorización estatal o actúen a la sombra del marco regulatorio.

Con todo, las SEDPE no solo modificaron el panorama del sistema financiero al incorporarse como nuevas instituciones financieras, sino que a partir de su autorización se dio un mensaje muy importante referente a la intención de la legislación colombiana de permitir que compañías tecnológicas empiecen a migrar hacia el sector financiero con la finalidad de contribuir a su desarrollo.

Conclusiones

Sin lugar a dudas, la creación de las SEDPE constituyó una novedad para el sistema financiero colombiano, no solo porque permitió que más personas accedieran formalmente al sistema, sino por las consecuencias inmediatas que esto trae. Con el acceso masivo de nuevos agentes es posible crear un historial de pagos, hacer una trazabilidad de las operaciones y, lo de mayor importancia, se construye el peldaño para que, en un futuro próximo, las nuevas personas incluidas en el sistema migren hacia otros productos financieros más complejos, lo cual significa mayor nivel de inclusión financiera.

Es de resaltar que con la creación de esta nueva institución financiera se busca contar con un canal de acceso para pequeños depositantes, lo que constituye una adecuada respuesta a las necesidades sociales del país, sin dejar de lado la necesidad de salvaguardar la estabilidad del sistema financiero y la protección a los consumidores. Esto se vio reflejado en una regulación prudencial apropiada que propende a que las SEDPE monitoreen, gestionen y administren adecuadamente los riesgos a los que están expuestas, sin asignarles mayores cargas regulatorias que las que les corresponden en razón a su naturaleza.

Consideramos que si bien las SEDPE son instituciones financieras más livianas y con menores requerimientos regulatorios, es necesario un esfuerzo importante por parte del ente supervisor. Principalmente, porque las SEDPE se montan sobre estructuras tecnológicas previamente establecidas y generalmente se desarrollan, en un primer estadio, al margen de todo el marco regulatorio que les aplica. Por tal razón, es probable que las SEDPE tengan un conocimiento avanzado en aspectos técnicos, tecnológicos y de uso de redes, y no en temas financieros y de cumplimiento normativo, por lo que el rol formativo del supervisor es trascendental a la hora de prevenir la concreción de riesgos.

Finalmente, aunque en Colombia se ha venido trabajando arduamente en profundizar el sistema financiero y ampliar su cobertura, y se han ideado productos e instituciones novedosas para tal fin, nos encontramos en una etapa en la que se requieren mayores esfuerzos. No basta con que la población marginada ingrese al sistema financiero mediante la apertura de algún tipo de producto de trámite simplificado, sino que lo realmente importante es que, a partir de este producto, se empiecen a realizar las transacciones que día a día se venían llevando a cabo en efectivo.

Es ahí precisamente donde radica el reto que tiene que afrontar el sistema financiero colombiano: que las SEDPE como instituciones financieras livianas y de fácil acceso cumplan un rol preponderante para permitir que, en la mayoría de las transacciones y de acuerdo a los topes máximos establecidos, las operaciones se canalicen con su participación.

Bibliografía

Ángel, Carlos Julio (1959). ***Legislación bancaria colombiana.*** Quinta edición. Editorial Minverva Ltda.

Asociación Bancaria de Colombia. (2015). ***Reglamentación prudencial de las SEDPE: clave para la estabilidad del sistema y para un verdadero impulso a los procesos de inclusión financiera***. Revista Económica.

Banco Mundial. (2014). ***Global Financial Development Report 2014:*** Financial Inclusion.

El Tiempo. (23 de agosto de 2018). ***Los tres retos para asegurar el crecimiento potencial de la economía***. [En línea]. Recuperado de: https://www.eltiempo.com/economia/sectores/retos-para-el-crecimiento-de-la-economia-en-convencion-bancaria-259222. [Consultado el 14 de mayo de 2019].

Rodríguez Azuero, Sergio. (2013). Contratos bancarios. ***Su significación en América Latina. Sexta edición. Legis.***

Unidad de Proyección Normativa y Estudios de Regulación Financiera. (10 de febrero de 2017). ***Reglamentación complementaria de las Sociedades Especializadas en Depósitos y Pagos Electrónicos*** (SEDPE).

Jurisprudencia

Decreto 1491 de 2015, *"por el cual se modifica el Decreto número 2555 de 2010 en lo relacionado con la reglamentación aplicable a las Sociedades Especializadas en Depósitos y Pagos Electrónicos, (SEDPE) y se dictan otras disposiciones".*

Exposición de motivos de la Ley 1735 de 2014.

Ley 1328 de 2009, *"por la cual se dictan normas en materia financiera, de seguros, del mercado de valores y otras disposiciones".*

Ley 1735 de 2014, *"por la cual se dictan medidas tendientes a promover el acceso a los servicios financieros transaccionales y se dictan otras disposiciones".*

Superintendencia Financiera de Colombia. ***Concepto 2016128451-001del 19 de diciembre de 2016. Sedpe, captación exclusiva mediante depósitos electrónicos.*** 19 de diciembre de 2016.

II PARTE

PROSPECTIVA DEL COMERCIO ELECTRÓNICO: HACIA LA REVOLUCIÓN 4.0

LOS PRINCIPALES DESAFÍOS EN MATERIA DE REGULACIÓN DE LAS *FINTECHS*

Erick Rincón Cárdenas

Resumen

Las *fintechs* se constituyen como el cambio de paradigma dentro de la industria financiera tradicional. A través de sus modelos novedosos, estas contribuyen con la disminución considerable de costos de operación y, por otro lado, aportan a la bancarización de la sociedad. En esa medida, el presente artículo tiene por objeto identificar los principales desafíos regulatorios que enfrenta la industria *fintech*, no sin antes presentar una breve descripción de los conceptos básicos que esta tiene, así como sus principales características, siguiendo con un análisis de los procesos de regulación *fintech* que se han presentado a nivel internacional durante los últimos años y, por último, los desafíos en materia de regulación a los que se enfrenta tal industria en Colombia.

Palabras clave: ecosistema *fintech*; servicios financieros; ***startups***; innovación tecnológica; aplicaciones.

Abstract.

The Fintech industry is considered as the paradigm shift within the traditional financial industry, which, through its novel models affected with the considerable decrease in operating costs and, on the other hand, contributes to the banking of society. To this extent, the purpose of this article is to present the main regulatory challenges facing the Fintech industry, but not before presenting a brief description of the basic concepts presented by the industry, as well as the main characteristics of the industry, following a analysis of the Fintech regulation processes that have been presented internationally during the last years and finally, the regulatory challenges facing the Fintech industry in Colombia.

Key words: Fintech ecosystem, financial services, Startups, technological innovation, applications.

Introducción

Las nuevas tecnologías y su aplicabilidad e impacto en diferentes instituciones sociales afectan la forma en la que nos relacionamos con distintas industrias. La tecnología ha liderado el ritmo en el que se han desarrollado nuevos productos y nuevas formas de hacer negocios. En consecuencia, el sector financiero, que tradicionalmente se ha considerado conservador, ha tenido que mantener este ritmo de desarrollo y adoptar estas nuevas tecnologías. De manera que las *fintechs* ingresan a la industria financiera como un modelo disruptivo y diferente, y se imponen como un nuevo actor en la industria que genera un impacto directo en la forma en que los reguladores del sector visualizan el mercado futuro.

Según el informe ***Fintech en América Latina 2018: crecimiento y consolidación***, presentado por Finnovista y el BID, se observa en la región un alto índice de personas y empresas que no pueden acceder a un crédito a través del sistema financiero tradicional. Dicha situación ha permitido el surgimiento de nuevas soluciones de financiamiento alternativo desintermediado a través de aplicaciones electrónicas, que favorece a la inclusión financiera en una región donde apenas el 37 % de su población se encuentra bancarizada. Así, gracias a las *fintechs*, los reguladores están enfrentando nuevos retos en la regulación de estas nuevas modalidades de servicios financieros que se prestan a través de medios electrónicos y tecnológicos. Por lo tanto, el presente artículo presenta una descripción general de la industria *fintech* y de su regulación a nivel tanto nacional como itrnacioal, así como los desafíos a los que se enfrenta la industria

01

Que es *fintech*

El término "***fintech***" se deriva de las palabras "***finance technology***" y se utiliza para denominar a las empresas que ofrecen productos y servicios financieros haciendo uso de tecnologías de la información y comunicación. Este concepto surgió de la necesidad de encontrar soluciones simples a operaciones financieras y de inversión complejas haciendo uso de la tecnología más avanzada para crear productos financieros innovadores y de bajo costo. Entre estos se incluyen soluciones para pagos móviles, herramientas para inversión y ahorro, moneda virtual, identificación y autentificación biométrica de clientes, utilización de algoritmos, ***big-data***, inteligencia artificial, entre otros.

Así, el desarrollo de servicios financieros basados en la innovación tecnológica es el objetivo principal de las ***fintechs***, quienes buscan ofrecer diferentes servicios financieros de manera eficiente, ágil, cómoda y confiable. Dentro de esta industria se pueden destacar los siguientes modelos de negocio: (i) los medios de pago y las transferencias a través de plataformas de pagos y transferencias internacionales, (ii) la infraestructura para servicios financieros conformada por: evaluación de clientes y perfiles de riesgo, prevención de fraudes, verificación de identidades, API bancarias, agregadores de medios de pago, ***big data & analytics***, inteligencia de negocios, ciberseguridad y contratación electrónica, (iii) la creación digital de créditos a través de plataformas electrónicas, (iv) soluciones financieras para empresas a través de softwares para la contabilidad e infraestructuras de facturación y gestión financiera, (v) finanzas personales y asesoría financiera, que incluye administración de finanzas personales, comparadores y distribuidores de productos financieros, educación financiera, asesores automatizados y planeación financiera, (vi) servicios digitales de intermediación de valores, instrumentos financieros y divisas, (vii) ***crowdfunding***, (viii) ***insurtech***, como la tecnología aplicada a la prestación de servicios en el sector asegurador, (ix) desarrolladores de soluciones basadas en el ***blockchain***, intermediarios y mercados de activos digitales, entre otras.

02

Conceptos básicos de *fintech*

Para una mejor comprensión del presente artículo, se presentan a continuación los conceptos más importantes y básicos que se utilizan dentro de la industria ***fintech***.

Analítica:

herramienta empleada para medir patrones y tendencias en los datos.

Antilavado de dinero (AML: Anti Money Laundering):

legislación que lucha contra el blanqueo de los fondos provenientes de actividades ilegales, que a su vez pueden ser utilizados para actividades terroristas o criminales.

***Application Programming Interface* (API):**

interfaz de programación de aplicaciones que permite al propietario de un servicio en red dar acceso universal a este a los consumidores. Entre sus usuarios se encuentran los desarrolladores de tecnologías o entidades financieras.

B2C (*Business to Consumer*):

es la relación que surge entre un comerciante y un consumidor final. Es la más utilizada por las empresas con presencia en internet.

B2B (*Business to Business*):

la abreviatura B2B proviene de lo que en inglés se conoce como ***business to business*** o, si se traduce, comerciante a comerciante. Esta relación se fundamenta en los principios de la buena fe y de confianza comercial, y les permite a quienes intervienen en ella obtener informaciones referentes a la solvencia de sus proveedores, la rentabilidad de sus inversiones, el conocimiento de pedidos de compras, facturas, entre otros, que ayuden a dinamizar y asegurar el comercio electrónico.

C2C (*Consumer to Consumer*):

identifica la relación determinada entre dos partes que tienen la misma calidad de consumidores finales. Ejemplo de este tipo de relación es la compra o intercambio de productos (bienes o servicios) directamente, como las tiendas de segunda mano o el intercambio de archivos ***Peer to Peer*** (P2P).

B2G (Business to Government o empresario a Gobierno):

esta relación permite establecer un lazo más transparente y eficiente entre los interesados en contratar con la administración pública en todos sus niveles.

Base de datos:

programa que permite organizar información de manera eficiente en una plataforma.

Big data:

cantidades voluminosas de datos estructurados o no estructurados que las organizaciones pueden minar y analizar para obtener beneficios empresariales.

Billetera electrónica:

software que permite a los usuarios realizar pagos electrónicos y compras, y almacenar criptomonedas *online*.

Bitcoin:

moneda virtual que puede ser intercambiada de manera digital entre personas a través de técnicas criptográficas para validar transacciones y realizar cambios en un registro distribuido.

Blockchain:

estructura particular de tecnología en red distribuida que une bloques de transacciones. Ofrece un historial completo de todos los activos e instrucciones llevadas a cabo empleando compleja criptografía.

Cloud computing:

servicios ofrecidos a través de un modelo que permite el acceso en red de manera ubicua, conveniente y bajo demanda a un grupo compartido de recursos informáticos compartidos (ej., redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser fácilmente proporcionados y liberados con un esfuerzo mínimo de gestión.

Criptomoneda:

tipo particular de moneda virtual que opera a través de la criptografía.

Crowdfunding:

sistema de financiamiento de un proyecto o empresa que recauda pequeñas cantidades de dinero pertenecientes a un gran número de personas. Generalmente se lleva a cabo a través de registros a través de internet que facilitan la recolección de dinero para el prestatario (préstamo) y para el emisor (*equity*).

Data:

información empleada para analizar o evaluar un posible resultado o tendencia.

Insurtech:

hace referencia a la unión entre *insurance* y *technology* y define al sector que engloba a: las compañías tradicionales de seguros que se transforman para adaptarse al nuevo contexto tecnológico, las empresas tecnológicas y las *startups* que aprovechan los avances tecnológicos para ofrecer productos y servicios innovadores en el sector.

KYC (Know Your Customer):

Conjunto de normas que las entidades deben cumplir referidas a la identidad de sus clientes y la legalidad de sus fondos.

Nube:

infraestructura virtual que retiene una cantidad ilimitada de datos e información.

Pasarela de pago:

proveedor de servicios que facilita las transacciones con tarjeta para negocios *online*.

Préstamos P2B (Peer to Business):

relaciones entre particulares y empresas que consisten en la obtención de financiamiento a través de préstamos o créditos aportados normalmente a pequeñas y medianas empresas (pymes) por pequeños inversores organizados a través de portales *web* específicos.

Sandbox regulatorio:

los *sandboxes* regulatorios ofrecen a las instituciones financieras y compañías no financieras espacios controlados donde pueden poner a prueba soluciones *fintech* innovadoras con el apoyo de una autoridad durante un periodo limitado de tiempo. Esto permite validar y probar su modelo de negocio en un entorno seguro.

Softwares-as-a-Service (SaaS):

licencia software y modelo de entrega a través del cual se licencia un software mediante una suscripción y gestionado de manera centralizada.

Startup:

empresa en su etapa temprana. A diferencia de una pyme, la *startup* se basa en un negocio que será escalable más rápida y fácilmente haciendo uso de tecnologías digitales.

Tecnología de registros distribuidos (DLT: Distributed Ledger Technology):

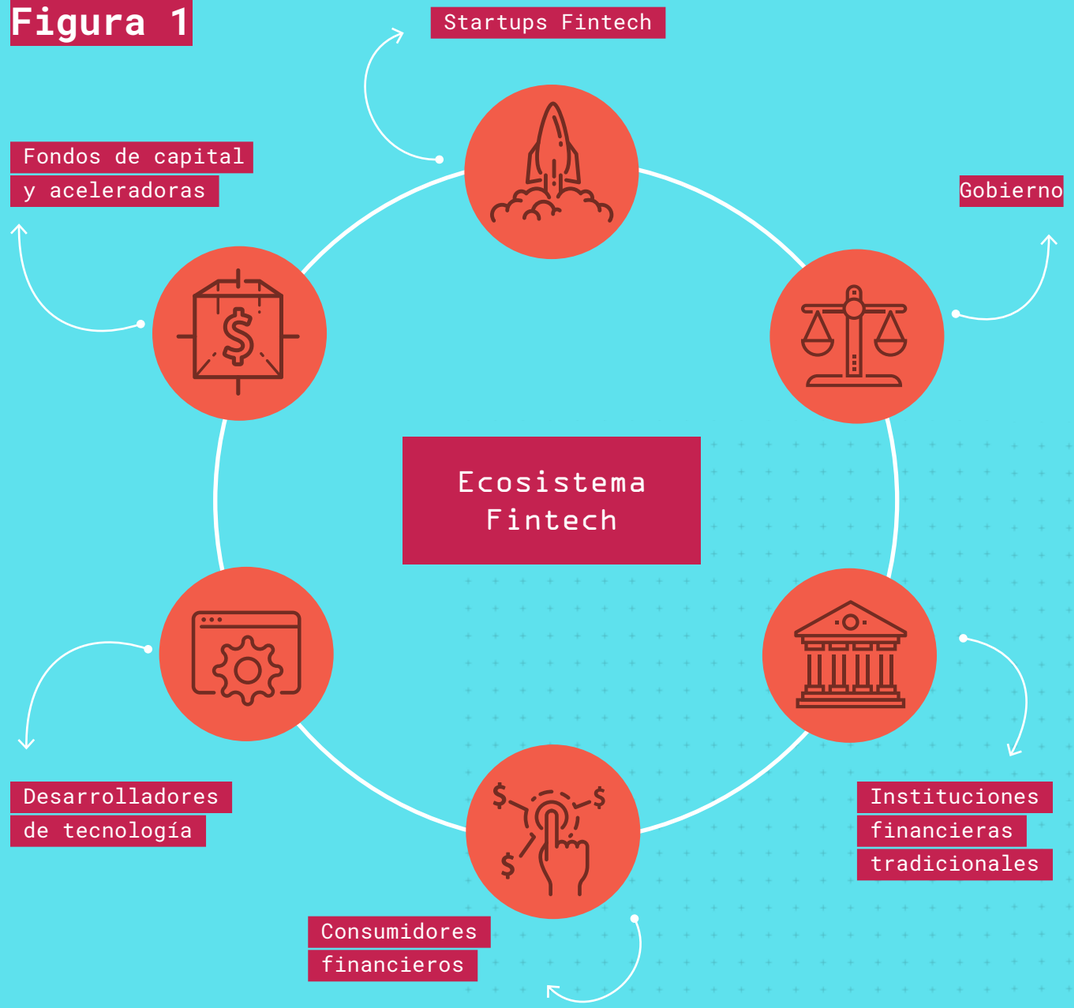
los registros distribuidos utilizan ordenadores independientes (conocidos como nodos) para registrar, compartir y sincronizar las transacciones en sus respectivos registros electrónicos (en vez de almacenar la información de manera centralizada, como en un registro tradicional).

03

Industria *fintech*

El Banco Nacional de Comercio Exterior de México expone en su artículo "***Fintech*** en el mundo. La revolución digital de las finanzas ha llegado a México" que el ***fintech*** es un ecosistema heterogéneo e instrumental donde conviven emprendedores, Gobierno, fondos, aceleradoras e instituciones financieras tradicionales. Así identifica seis elementos principales que lo conforman.

Figura 1



Fuente: https://www.bancomext.com/wp-content/uploads/2018/11/Libro-Fintech.pdf.

Las ***startups fintech***, en su mayoría, son emprendimientos, es decir, empresas de apenas unos cuantos empleados e impulsadas básicamente por alguna idea innovadora en los ámbitos financieros. Abarcan nichos específicos de mercado, proporcionando servicios más personalizados y eficientes que los que ofrecen las instituciones financieras tradicionales, e incluso sus acciones han generado un fenómeno que trasciende los servicios financieros y ha afectado la participación de aquellas. En particular, su habilidad de desagregar los servicios financieros representa su mayor disparador de crecimiento.

Así pues, ahora los consumidores, en lugar de depender de una única institución financiera para sus necesidades, están comenzando a escoger y a elegir los servicios que aprecian de una variedad de compañías de ***fintech*** (Lee,2018). Quienes desarrollan las tecnologías proveen plataformas digitales para redes sociales, análisis de ***big data***, inteligencia artificial, desarrollo de aplicaciones móviles, etc., con el objetivo de generar un ambiente favorable para que las ***startups*** puedan lanzar al mercado servicios innovadores. Así, por ejemplo, tecnologías de ***big data*** pueden ser utilizadas para tener un conocimiento constante de los clientes y sus patrones de consumo y, por tanto, proveer servicios personalizados para ellos; la compaginación en la nube (***cloud computing***), por su parte, permite a las ***startups*** contar con los recursos necesarios para lanzar sus productos a una cuarta parte del costo.

Los algoritmos son una constante en estos emprendimientos dadas su capacidad de aprendizaje y la adaptabilidad de sus productos y servicios. Es así como, por ejemplo, existen asesores robotizados en firmas de gestión patrimonial. Las redes sociales, por su parte, favorecen el crecimiento de las comunidades en las plataformas de ***crowdfunding*** y de préstamos de persona a persona (P2P ***lending***), añadiendo transparencia y democratizando el acceso a fuentes de financiamiento alternativas. Los dispositivos móviles a su vez sustituyen la distribución física de los productos y servicios que estas ***startups*** ofrecen.

El rol de los Gobiernos en este escenario es proveer una regulación favorable para los emprendimientos ***fintech***. Así, dependiendo de su plan de desarrollo económico nacional y de las políticas económicas que prevalezcan en el país del que se trate, diferentes Gobiernos proporcionan diferentes niveles de regulación para fomentar la innovación y la competencia (ej., licencias, certificaciones, incentivos fiscales, disminución de requerimientos de capital, entre otros). En algunos casos, se han diseñado regulaciones laxas que han permitido a las ***startups*** ofrecer servicios

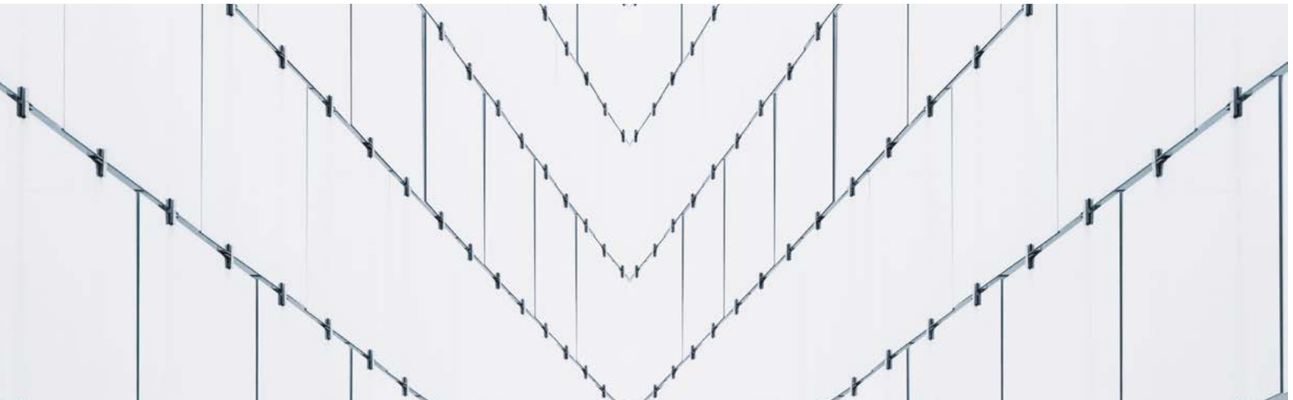
personalizados, menos costosos y de fácil acceso para sus clientes. Sin embargo, una gran mayoría de ecosistemas aún no cuentan con una regulación específica, lo que impide el avance de muchos proyectos que deben regirse por la regulación impuesta (Lee, 2018).

Por otro lado, los clientes financieros representan la fuente de ingresos para las firmas ***fintech***. El ingreso dominante del ecosistema proviene de clientes individuales, así como de pymes. Sin embargo, el futuro demográfico de estas compañías se percibe favorable en términos de que en las siguientes décadas se logre la inclusión de un mayor número de personas que hoy se encuentran en situaciones de exclusión financiera, sobre todo en economías emergentes. Las instituciones financieras tradicionales también son una fuerza motriz importante en el ecosistema.

A nivel mundial, se estima que en los últimos tres años el sistema ***fintech*** creció 50 %, lo que corresponde al mayor crecimiento a las ***fintechs*** chinas, que en 2015 movieron más de USD 22 mil millones. Según el *Ranking 2018 Fintech 100*[146], cuatro empresas chinas ocuparon los primeros cinco lugares de un grupo de veintitrés países. Esta lista se elabora desde hace tres años sobre la base de cinco indicadores: capital, tasa de aumento del capital, diversidad geográfica, diversidad sectorial, y un factor adicional que incluye el grado de innovación en los productos, servicios y modelos de negocio. Estados Unidos concentra el mayor número de ***fintechs***, seguido de Reino Unido, Australia, China, Canadá e Israel. Estos seis países representan las dos terceras partes de las 100 ***fintechs*** más grandes del mundo. A nivel latinoamericano destacan Brasil, México y Colombia, que presentan los mejores resultados con ubicaciones entre el puesto 16 y el 60 de la lista.

Estos negocios se caracterizan por la rapidez y eficiencia para solucionar problemas frente a las rigideces de la banca y de las compañías de seguros tradicionales, así como por crear programas que privilegian el volumen en la captación de clientes antes que el precio o la tarifa y, mediante el uso de la tecnología, prescindir de oficinas o de la contratación de personal excesivo. En este contexto de rápido crecimiento de las ***fintechs*** surge el dilema sobre el rol que debe cumplir el Regulador. Es decir, ante la aparición de nuevos actores en el mercado, se hace necesario revisar las reglas de juego para asegurar un nivel de competencia adecuado.

146. https://assets.kpmg/content/dam/kpmg/xx/pdf/2016/10/fintech-100.pdf.



04

Regulación *fintech* a nivel internacional

La financiación ***fintech*** ha crecido rápidamente en todo el mundo durante los últimos años, pero su tamaño presenta notables variaciones entre economías. Las diferencias reflejan el desarrollo económico de un país y la estructura de sus mercados financieros: cuanto mayor es la renta de un país y menos competitivo es su sistema bancario, mayor es la actividad de financiación ***fintech***. Los volúmenes de esta también son mayores en los países con una regulación bancaria menos estricta (Claessens ***et al.***, 2018).

Para las economías emergentes, las finanzas tecnológicas resultaron ser una alternativa de desarrollo económico. En la región Asia-Pacífico, por ejemplo, surgieron las aceleradoras más productivas de ***startups fintech***. Así, Hong Kong y Singapur cuentan con las mayores concentraciones de firmas ***fintech*** en el mundo (Banco Nacional de Comercio Exterior, s.f.).

Asimismo, de acuerdo con el informe trimestral presentado por BPI en septiembre de 2018, el papel de la financiación ***fintech*** parece mayor en determinados segmentos del mercado. Por ejemplo, en el Reino Unido constituía alrededor del 15 % del flujo de préstamos bancarios comparables a consumidores y pymes en 2016 (CCAF, 2017), y en Estados Unidos llegó a representar el 36 % de los préstamos personales no garantizados concedidos en 2017 (Levitt, 2018, citando datos de TransUnion)[147]. En cambio, en Japón, Países Bajos, Singapur y varios mercados más prevalece el préstamo a empresas. En Australia y en Italia, el anticipo de facturas representa un porcentaje relativamente elevado. El préstamo a empresas suele ser el principal tipo de préstamo concedido por las plataformas de financiación ***fintech*** que mantienen los préstamos en sus balances (panel derecho).

Experiencias sobre regulación en otros países Reino Unido, Australia y Estados Unidos[148] muestran que estos son los países que más han avanzado en materia de regulación. En el Reino Unido, en abril de 2013, se creó la Autoridad para la Conducta Financiera, que redujo los requisitos de entrada al mercado de estas empresas; luego, en octubre de 2014, creó un espacio de experimentación o ***sandbox*** donde, bajo determinadas reglas, se desarrolla un producto y permite ver cómo se enfrenta a dichas regulaciones antes de obtener el permiso final de funcionamiento.

El Banco de Inglaterra es uno de los bancos centrales que más han trabajado en proyectos ***fintech***, y en especial en ***blockchain***. Desde 2015, empezó a evaluar esta última como tecnología recomendada para

147. En Alemania, Nueva Zelandia y Estados Unidos, los consumidores son, con mucha diferencia, los mayores prestatarios.

148. http://www.centrodeinnovacionbbva.com/noticias/tipos-de-regulacion-fintech-activa-pasiva-y-restrictiva.

mejorar sus servicios de infraestructura de pagos, liquidaciones y acuerdos. Además, las regulaciones de esta entidad se han orientado a asegurar el funcionamiento legal de las ***fintech*** para que los fondos que manejan no provengan ni sean utilizados en actividades ilícitas. Entre dichas regulaciones se incluye la creación del Comité de Política Financiera, que evalúa estos nuevos riesgos para la estabilidad financiera.

Igualmente se destacan Singapur y Japón. En el Banco Central de Singapur se creó una unidad ***fintech*** para estudiar a partir de casos reales las medidas regulatorias necesarias para lograr un equilibrio entre seguridad e innovación. Asimismo, el Banco Central de Japón ha establecido su propio centro ***fintech*** en el departamento de pagos y sistemas de liquidación y está desarrollando la tecnología ***blockchain*** (Delta Financiero, 2016).

En Estados Unidos, a partir de la ley JOBS[149] (por sus siglas en inglés de ***Jumpstart Our Business Startups***), el Congreso aprobó extender la participación en ***startups***, reservada tradicionalmente para inversionistas institucionales, a personas naturales. Con ello se facilitó el crecimiento del ***crowdfunding*** al eliminarse la obligación del registro del inversionista en la Comisión de Bolsa y Valores y crearse la figura del intermediario autorizado (***funding portals***), con una regulación más flexible.

149. Promulgada por el expresidente Obama en 2012, adoptada por la Comisión de Bolsa y Valores en 2015 y aprobada recientemente por el Congreso.

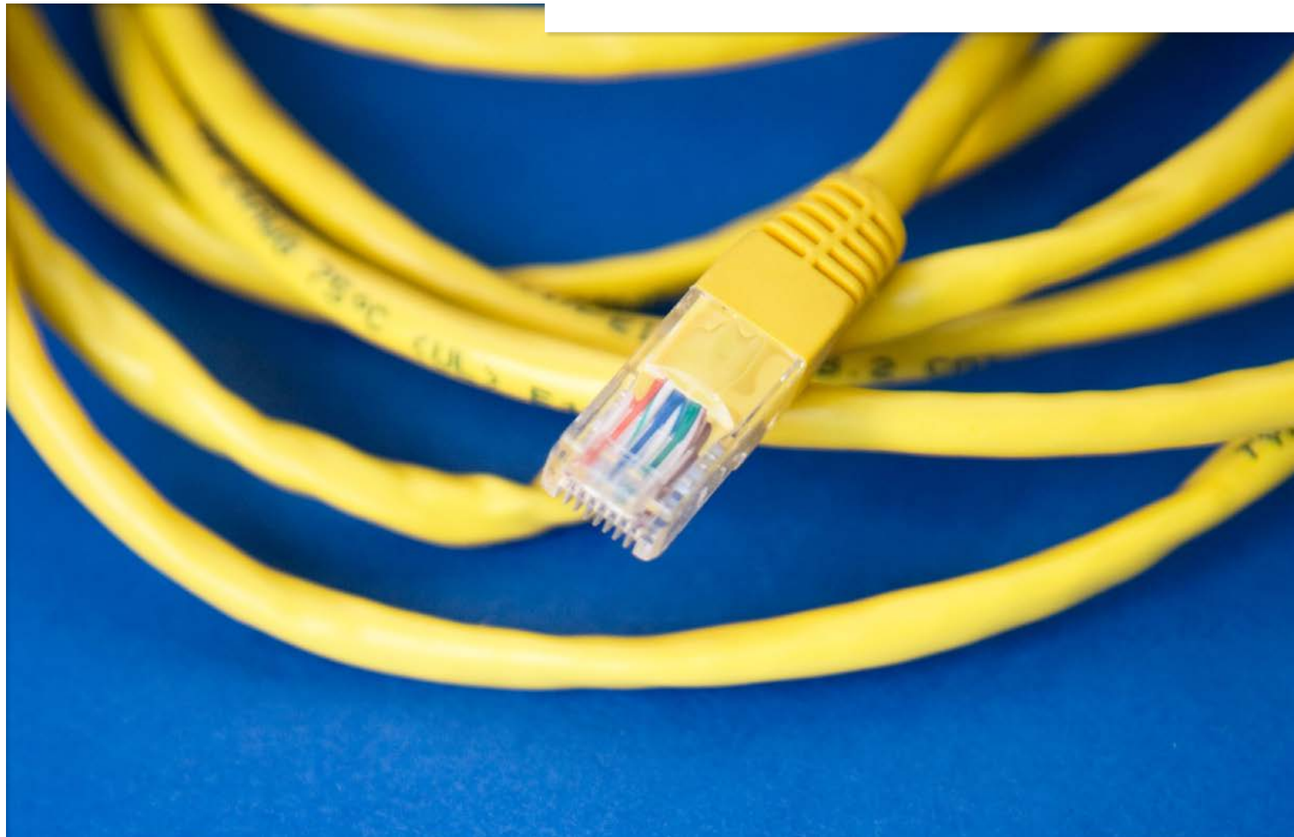
Tabla 1: Regulación de *fintech* a nivel internacional

	Brasil	México	Colombia	Argentina	Chile	Perú	Reino Unido	Singapur
Nº *Fintechs*	230	180	84	72	65	46	350-500	310
Asosiación *Fintech*	ABFintechs	Asociación Fintech México	Colombia Fintech	Cámara Argentina Fintech	Asociación de empresas de innovación Financiera	Asociación Fintech Perú	Innovación Financiera	Singapur Fintech
Regulación Fintech	✗	Proyecto de ley Fintech	Consulta	Ley de emprendedores	Proyecto de ley	✗	✓	✓
Grupo de trabajo (*Fintech* + regulador)	✗	✓	✓	✓	✗	✗	✓	✓
Sandbox regulatorio	✗	✗	✗	✗	✗	✗	✓	✓

En el caso de Chile, el Ministerio de Economía encargó un estudio al BID-FOMIN sobre el desarrollo de la industria de ***crowdfunding***. En este se recomienda modificar la ley de valores para que haya una clara distinción entre la oferta pública y la oferta de ***crowdfunding***. Además, se sugiere (i) fomentar las asociaciones entre bancos y plataformas de ***crowdfunding*** para alentar la inclusión financiera, (ii) crear cuentas individuales de ahorro separadas y libres de impuestos para los que quieren prestar dinero, e (iii) insertar el ***crowdfunding*** en el ecosistema pyme.

En Argentina, el Senado aprobó la Ley de Emprendedores[150], cuyo objetivo es facilitar el crecimiento de los negocios agilizando los trámites burocráticos y reduciendo el tiempo que toma la apertura de una empresa, que va de 6 a 12 meses en la actualidad, a 24 horas. También otorga beneficios tributarios a inversionistas y presenta diferentes tipos de financiamiento para los que inicien un emprendimiento. Así mismo se crea el Registro de Instituciones de Capital Emprendedor y un Fondo Fiduciario para el Desarrollo del Capital Emprendedor (FONDCE), con el cual se pueden financiar emprendimientos de forma conjunta con el sector privado. Por primera vez en este caso, el Estado destina fondos públicos para inversiones conjuntas con el sector privado, para lo cual se crean 10 fondos con un aporte público del 40 % y un capital mínimo conjunto de USD 30 millones.

150. http://www.produccion.gob.ar/wp-content/uploads/2016/11/ley-deemprendedores/LeyEmprendedores.pdf.



Regulación *fintech* en Colombia

Finnovista ha establecido que Colombia se consolida como el tercer ecosistema ***fintech*** de América Latina, con un crecimiento neto del 45 % en año y medio y 78 nuevas ***startups fintech***. Esto se ve impulsado por el auge de los segmentos de tecnologías empresariales para instituciones financieras (ETFI), gestión patrimonial, ***trading*** y mercados de capitales, préstamos y gestión de finanzas personales.

Actualmente, los siete segmentos principales en Colombia son: (i) pagos y remesas, con 48 ***startups***, un 27 % del total; (ii) préstamos, con 36 ***startups***, abarcando el 20 % del total; (iii) gestión de finanzas empresariales, que con 25 ***startups*** supone el 14 % del total; (iv) ETFI, con 15 ***startups***, un 8 % del total; (v) gestión de finanzas personales, con 12 ***startups*** que representan un 7 % del total; (vi) seguros, con 10 ***startups***, correspondientes a un 5,50 % del total, y (vii) puntaje, identidad y fraude, también con 10 ***startups***, un 5,50 % del total.

En 2017 la Superintendencia Financiera de Colombia (SFC) conformó el Grupo de Trabajo de Innovación Financiera y Tecnológica para investigar, promover, experimentar y apoyar el uso de la tecnología en el sector financiero. Este fue conformado a través de tres mecanismos: el ***Hub***, con el objetivo de apoyar y asesorar a entidades relacionadas con la innovación financiera y tecnológica; La Arenera, que permite realizar experimentos o pruebas tecnológicas; y el espacio RegTech, con el objetivo de aprovechar los desarrollos tecnológicos para apalancar la innovación interna de la SFC. Recientemente, este organismo dio a conocer que se había aprobado el primer proyecto para realizar una prueba piloto en La Arenera. En concreto, se trata de la ***fintech*** Tpaga, que permitirá *"que se use el canal de la billetera virtual de la Fintech para la vinculación de clientes al FIC de la comisionista, por medio de un trámite simplificado para bajos montos, similar a lo que se aplica hoy para CAT y CAE"*.

En 2018 también se aprobó el decreto que regula la actividad del ***crowdfunding***, si bien, como hemos visto, es necesario que la nueva regulación no se convierta en una barrera más para las ***startups*** que ofrecen este tipo de financiación. Dada la complejidad en el acceso a crédito, pues de acuerdo con el Banco Mundial en Colombia tan solo el 14,5 % de la población recibió financiamiento de una entidad financiera, es necesario permitir el avance en el uso de la tecnología y la innovación para facilitar el acceso y uso de servicios financieros por parte de la población. Por otro lado, el Gobierno presentó su Plan Nacional de Desarrollo 2018-2022, donde el apoyo a la evolución ***fintech*** está presente en varias ocasiones. Por un lado, se buscará en los próximos años fortalecer el acceso a financiamiento para el emprendimiento y para pymes a través de iniciativas como el abaratamiento del microcrédito empresarial o la puesta en marcha de una serie de beneficios para ángeles inversionistas que financien ***startups*** en materia de ciencia, tecnología e innovación.

Conclusiones

Se puede concluir que las ***fintechs*** constituyen un nuevo participante que representa un cambio de paradigma dentro de la industria financiera tradicional, ofreciendo modelos novedosos a partir de la atención determinante a las necesidades de las personas, disminuyendo considerablemente los costos operacionales y aportando a la bancarización de la sociedad. Como se pudo evidenciar, en América Latina la industria ***fintech*** está creciendo exponencialmente en los últimos años, ubicando a Brasil como el país con más emprendimientos de esta categoría (377), seguido de México (334) y Colombia (124). En esa medida, el ingreso de las ***fintechs*** constituye una oportunidad de inclusión y desarrollo económico a través de servicios financieros asequibles, efectivos y seguros que fomentan no solo un crecimiento equitativo, sino también la innovación, la promoción y la implementación de nuevas tecnologías.

Bibliografía

Banco Nacional de Comercio Exterior, México. (s.f.). Fintech en el mundo: La revolución digital de las finanzas ha llegado a México. [En línea]. Recuperado de: https://www.bancomext.com/wp-content/uploads/2018/11/Libro-Fintech.pdf.

Claessens, Stijn, Frost, Jon, Turner, Grant y Zhu, Feng. (2018). Mercados de financiación fintech en todo el mundo: tamaño, determinantes y cuestiones de política. [En línea]. Recuperado de: https://www.bis.org/publ/qtrpdf/r_qt1809e_es.pdf.

Delta Financiero. (25 de agosto de 2016). El Banco Central de Japón pone el foco en la industria Fintech. [En línea]. Recuperado de: http://deltafinanciero.com/265-El-Banco-Central-de-Japon-pone-el-foco-en-la-industria-Fintech-.

Lee, I. (2018). Fintech: Ecosystem, Business Models, Investment Decisions, and Challenges. Business Horizons.

¿EN DÓNDE ESTOY COMPRANDO BITCOIN? UN ANÁLISIS DEL IMPACTO DE LA REGULACIÓN EN LAS PLATAFORMAS DE NEGOCIACIÓN DE ACTIVOS DIGITALES

Carlos Andrés Atuesta[151]

Resumen

El propósito de esta investigación es identificar la relación existente entre las plataformas de intercambio de activos digitales y su jurisdicción de incorporación, buscando explicar cómo la regulación de su domicilio influencia su funcionalidad y estructura. Para este efecto, primero, se identificaron los distintos prototipos de plataformas y, luego, la causalidad entre la regulación aplicable en los lugares de incorporación y los prototipos de plataformas.

El estudio provee evidencia sobre la existencia de dos modelos de plataformas: aquellas cuya finalidad se encuentra ligada al financiamiento de proyectos, y otras dedicadas al intercambio entre moneda de curso legal y activos digitales. Igualmente, se muestra cómo la regulación, sea directa o indirecta, en materia de activos digitales, es un factor fundamental sobre la funcionalidad y estructura de las plataformas. Mientras que las jurisdicciones en que la definición de activo digital se ha limitado al concepto de criptomonedas generan plataformas focalizadas en el intercambio de este tipo de activos digitales por FIAT, aquellas otras en que el concepto de activo digital se ha hecho extensivo a otros activos (***i.e.***, ***token*** de utilidad o ***stablecoins***) promueven la generación de plataformas útiles en el financiamiento de proyectos.

Este artículo resulta de utilidad para Gobiernos y entidades regulatorias, sociedades administradoras de plataformas e inversionistas en activos digitales al evidenciar los efectos de distintos modelos regulatorios sobre el funcionamiento del mercado de activos digitales.

Palabras clave: *blockchain*; activos digitales; criptoactivos; plataformas de intercambio; regulación.

151. El autor agradece toda su colaboración y comentarios en la elaboración de este artículo a Sebastián Cortés, CEO de Digital Assets Exchange Solutions (DAEXS) (www.daexs.com).

Abstract

The purpose of this research is to identify the relationship between the Crypto Assets Exchange and their place of jurisdiction, aiming to explain how the regulation affects the functionality and structure of the Exchanges. For this purpose, first, the prototypes of the Exchanges were identified and, then, the causality between the regulation in the places of incorporation and the prototypes. The study provides evidence on the existence of two models of Exchanges, those linked to the financing of projects and others dedicated to the exchange between real currency and virtual assets. Likewise, the study shows how the regulation applicable to virtual assets, whether direct or indirect, is a fundamental factor to determine the functionality and structure of the platforms. While in jurisdictions in which the definition of digital asset has been limited to the concept of cryptocurrencies generates Platforms focused on the exchange of this type of digital assets by FIAT, in those in which the concept of digital asset has been extended to others assets (i.e. utility tokens or stablecoins) promotes the generation of useful platforms in the financing of projects. This article is useful for governments and regulatory entities, platform management companies and investors in digital assets, evidencing the effects of different regulatory frameworks on the structure of the digital asset market.

Key Words: blockchain; virtual assets; cryptocurrency; crypto exchanges; regulation.

Introducción

Desde la invención de ***bitcoin*** en 2008, el crecimiento del mercado de activos digitales ha crecido vertiginosamente. Según información de Coinmarketcap, a 31 de mayo de 2019 tan solo la capitalización de mercado de ***bitcoin*** se estima en USD 141 mil millones. Igualmente, el número de activos digitales[152], como también su tipología y funcionalidad, han aumentado considerablemente. A 31 de mayo de 2019, Coinmarketcap reportaba la existencia de más de 2.200 activos digitales, los cuales varían en su clase y entre los que se encuentran las criptomonedas (***e.g.***, ***bitcoin***), los ***tokens*** de utilidad (***e.g.***, ***maker***), los ***tokens*** de valor (***e.g. blockchain capital***), ***stablecoins*** (USD ***tether***), entre otros.

152. No existe una definición unificada de activo digital. Para efectos de este artículo, por tal se entenderá la representación digital de valor o de derechos contractuales asegurados criptográficamente, empoderada mediante tecnología de registro distribuido (DLT por sus siglas en inglés), la cual es almacenada y transferida electrónicamente.

Tabla 1: Tipología de los activos digitales

Tipo	Definición
Criptomonedas	*Usados generalmente como (a) repositorio de valor, (b) mecanismo de intercambio y/o (c) medio de pago de bienes y servicios.* *También son usados para facilitar el funcionamiento de servicios de pago.* *No son emitidos por una autoridad central.* *No son considerados dinero, divisa o moneda de curso legal (FIAT).*
Tokens **de utilidad**	*Permite la redención de productos y servicios típicamente provistos mediante tecnología de registro distribuido (DLT por sus siglas en inglés).* *Sirven como instrumento de levantamiento de capital mediante venta anticipada de bienes y/o servicios.*
Tokens de valor	*Proveen derechos de propiedad, repago de una suma de dinero o participación en utilidades.* *Generalmente se enmarcan dentro del concepto de valor, instrumentos financiero previstos por la regulación existente en materia financiera o del mercado de valores.* *Sirven como instrumento de levantamiento de capital.*
Stablecoins	*Son un tipo de token de utilidad.* *Están respaldadas por una moneda de curso legal.* *La relación entre la moneda de curso legal y los tokens es 1:1.* *El emisor tiene la custodia de la moneda de curso legal que respalda el token.*
Tokens **representativos de activos**	*Es un tipo de token de utilidad.* *Representan un derecho de propiedad sobe un activo subyacente, generalmente un bien genérico como el oro o el petróleo, entre otros.* *El emisor tiene la custodia del activo.*

Fuente: basado en FCA (2019), Euler (2018), FCA (2018), Girasa (2018) y PWC (2018).

El intercambio de los activos digitales se puede realizar de diferentes maneras, como son transacciones directas entre las personas, plataformas ***consumer to consumer*** (***e.g.***, ***local bitcoins***) o plataformas de intercambio, comúnmente denominadas ***crypto-exchanges***.

Las plataformas de intercambio de activos digitales (en adelante las "plataformas") se han venido popularizando debido a sus mayores niveles de liquidez, oferta de activos digitales, profundidad del mercado y seguridad en los intercambios, constituyéndose de esta manera en el mercado por excelencia de los activos digitales en todo mundo. A inicios de 2019, el número de plataformas se estimaba en 230 aproximadamente (FCA, 2019), situación a la que no es ajena la región, donde varias plataformas prestan sus servicios (mapa 1).

Mapa 1: Plataformas de intercambio de activos digitales en Latinoamérica

Fuente: Ortiz (2018).

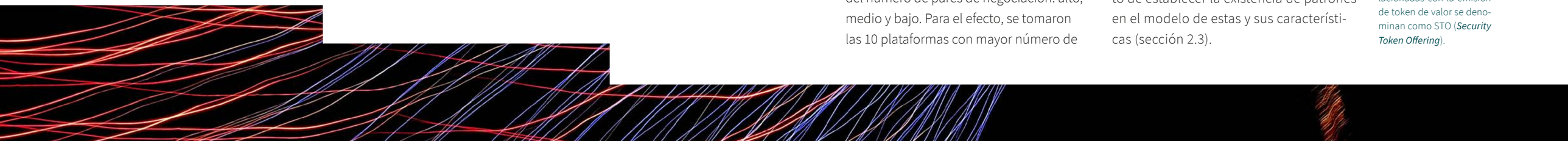
A nivel mundial, la oferta y estructura de las plataformas es diversa. Así nos encontramos, por un lado, con Binance, una de las de mayor reconocimiento, que solo ofrece la posibilidad de intercambio entre activos digitales, y por el otro, BitFlyer, la más grande por volumen de negociación reportado en Japón, cuyo intercambio de activos digitales es exclusivo por la monedad de curso legal japonesa.

El número de pares de negociación disponibles varía considerablemente. Mientras que en HitBTC, plataforma operada en Hong Kong desde inicios de 2014, ofrece aproximadamente 800 distintos pares de negociación, itBit, plataforma incorporada en Nueva York (EE. UU.) y Singapur, la cual inició operaciones desde el 2013, cuenta tan solo con cuatro pares. Algunas, por ejemplo, como el caso de Kucoin, ofrecen más de 10 idiomas a sus usuarios, mientras que otras, como es el caso de Coinbase, solo ofrecen sus servicios en un idioma.

La vinculación y el acceso a las plataformas es completamente en línea, pudiendo de esta manera atender a cualquier mercado con independencia de su lugar de domicilio. Esto es muy similar a lo que sucede en otros mercados ***online***, como es el caso de Airbn, y resulta aún más visible cuando, como es el caso de varias plataformas (***e.g.***, Binance, Poloniex, Huobi Global), su modelo de negocio se circunscribe al intercambio de activos digitales entres sí, sin hacer uso de FIAT. Aunque esto nos podría llevar a suponer que la jurisdicción no sería relevante, más allá de asuntos tributarios, algunas experiencias conocidas en la industria sugieren lo contrario.

Es muy conocido en la industria el caso de Binance, la cual se ha reincorporado en varias ocasiones (Amber, 2018). Esta fue fundada en China en 2017, pero desde entonces ha trasladado su domicilio en tres ocasiones: a Japón (2017) a Taiwán (2018) y luego aparentemente a Malta (2019). Aunque la salida de China se puede explicar fácilmente por la declaración de ilegalidad de ICO (Chen y Luu, 2017), su partida de Japón no tendría una razón igualmente evidente, más cuando se observa que otras plataformas como BitFlyer, BTCBOX y BitBank siguen operando en dicho país con relativo éxito, desarrollo que se ha visto impulsado por la expedición de regulación expresa en materia de plataformas y activos digitales en el mismo 2017.

En este orden de ideas, consideramos oportuno preguntarnos ***si hay motivos de índole regulatorio que motiven que una plataforma prefiera una jurisdicción en lugar de otra*** y, aún más importante, ***qué relación hay entre la regulación de la jurisdicción que la plataforma adopte y su estructura de servicios.*** Antes de dar respuesta a estas preguntas, consideramos oportuno determinar si dentro de la diversidad de plataformas existen modelos de negocio definidos que luego nos sirvan para identificar la relación entre ellos y la jurisdicción de incorporación y ley del contrato aplicable.



01

Metodología para la caracterización de las plataformas

Para efectos de determinar si existen distintos modelos de negocio, hemos decidido tomar como punto de partida el número de activos digitales disponibles en las plataformas. Para estos efectos asumimos que cuanto mayor sea el número de activos digitales, mayor es la funcionalidad que tienen las plataformas con la financiación de proyectos, tal como a continuación se explica.

1.1. Número de activos digitales listados

La financiación de proyectos mediante activos digitales se realiza a través de las denominadas ***coin offerings***[153] (FCA, 2018). Bajo este mecanismo las compañías levantan capital mediante la emisión de activos digitales. Así las cosas, es de esperarse que las plataformas cuya vocación esté inclinada a la financiación de proyectos cuenten con un mayor número de activos listados, lo que se ve fielmente reflejado en el número de pares de negociación. En otras palabras, un mayor número de pares de negociación supone necesariamente un mayor número de activos digitales dispuestos para la compra y venta en la plataforma y, por tal vía, un mayor número de proyectos que potencialmente se han financiado, sea vía capital o deuda (***i.e.***, STO) o mediante ingresos por ventas de bienes o servicios futuros (***i.e.***, ICO).

Con motivo de lo anterior, las plataformas fueron divididas en tres grupos en razón del número de pares de negociación: alto, medio y bajo. Para el efecto, se tomaron las 10 plataformas con mayor número de pares de negociación (Alto), aquellas con menores pares de negociación (Bajo) y aquellas cinco inmediatamente superiores y cinco inferiores a la media (Medio), conforme a la publicación de las primeras 100 plataformas por volumen transaccional ajustado reportado por Coinmarketcap del 7 de mayo de 2019. Para cada una de las plataformas se identificaron el lugar de incorporación y la ley del contrato, de conformidad a la información disponible en los términos y condiciones, o cualquier otro documento de tipo legal, publicados en la página ***web*** de cada una de estas. Así mismo se consideraron la posibilidad de intercambio moneda de curso legal por activos digitales y la disponibilidad de un activo digital respaldada por una monedad de curso legal (***stablecoin***) (tabla 2).

Los resultados individuales fueron agrupados en razón del tipo de categoría de las plataformas (sección 2.1), con el objeto de establecer la existencia de patrones en el modelo de estas y sus características (sección 2.3).

153. La denominación de las ***coin offerings*** varía dependiendo del tipo de activo digital objeto de emisión. Así, mientras que aquellas ligadas a la emisión de ***token*** de utilidad son denominadas ICO (***Initial Coin Offering***), las relacionadas con la emisión de token de valor se denominan como STO (***Security Token Offering***).

Tabla 2: Plataformas según el número de pares de negociación disponibles

Plataforma	Clasificación	Pares de negociación	FIAT	Stablecoin	Idioma	Incorporación	Ley del contrato	Lanzamiento
Hitbtc	*Alto*	*795*	*No*	*Sí*	*5*	*Hong Kong*	*Hong Kong*	*2014, Febrero*
Yobit	*Alto*	*497*	*Sí*	*No*	*3*	*NA*	*NA*	*2014, Agosto*
Binance	*Alto*	*467*	*No*	*Sí*	*15*	*NA*	*Singapur*	*2017, Julio*
Huobi Global	*Alto*	*435*	*No*	*Sí*	*13*	*Seychelles*	*Seychelles*	*2013, Septiembre*
KuCoin	*Alto*	*406*	*No*	*Sí*	*12*	*NA*	*Seychelles*	*2017, Agosto*
OkEx	*Alto*	*398*	*No*	*Sí*	*4*	*Seychelles/ Malta*	*Seychelles/ Malta*	*2014, Enero*
Hotbit	*Alto*	*396*	*Sí*	*Sí*	*6*	*NA*	*NA*	*2018, Enero*
Huobi Korea	*Alto*	*387*	*Sí*	*Sí*	*3*	*Corea del Sur*	*Corea del Sur*	*2018, Marzo*
Gate.io	*Alto*	*376*	*No*	*Sí*	*12*	*NA*	*Islas Caimán*	*2018, Enero.*
Bittrex	*Alto*	*345*	*Sí*	*Sí*	*1*	*Malta/Washington (EE. UU.)*	*Malta/Washington (EE. UU.)*	*2014, Febrero*
Coineal	*Medio*	*48*	*No*	*Sí*	*4*	*Seychelles*	*Seychelles*	*2018, Abril*
Coinbase	*Medio*	*47*	*Sí*	*No*	*1*	*Inglaterra/California (EE. UU.)*	*Inglaterra/ California (EE. UU.)*	*2014, Mayo*
Coinone	*Medio*	*45*	*Sí*	*No*	*2*	*Corea del Sur*	*Corea del Sur*	*2014, Enero*
Coindeal	*Medio*	*43*	*Sí*	*No*	*6*	*Malta*	*Malta*	*2018, Marzo*
Kryptono	*Medio*	*43*	*No*	*Sí*	*8*	*Islas Caimán*	*Singapur*	*2018, Enero*
EtherFlyer	*Medio*	*41*	*No*	*No*	*3*	*NA*	*NA*	*2016, Diciembre*
TOPBTC	*Medio*	*41*	*No*	*Sí*	*12*	*NA*	*China*	*2016, Enero*
C2CX	*Medio*	*39*	*No*	*Sí*	*2*	*NA*	*NA*	*2016, Diciembre*
Hubi	*Medio*	*39*	*No*	*Sí*	*4*	*NA*	*China*	*2018, Enero*
Bitibu	*Medio*	*37*	*No*	*Sí*	*1*	*NA*	*NA*	*2018, Enero*
Chaince	*Bajo*	*10*	*No*	*Sí*	*4*	*NA*	*NA*	*2018, Enero*
BitBank	*Bajo*	*8*	*Sí*	*No*	*2*	*Japón*	*Japón*	*2014, Mayo*
Cryptonex	*Bajo*	*7*	*Sí*	*No*	*16*	*Escocia (RU)*	*Reino Unido*	*2017, Octubre*
Tidebit	*Bajo*	*7*	*Sí*	*No*	*3*	*NA*	*Hong Kong*	*2015, Enero*
Coinsbank	*Bajo*	*6*	*Sí*	*No*	*1*	*Estonia*	*Legislación internacional (ICC)*	*2016, Abril*
BBX	*Bajo*	*4*	*No*	*Sí*	*6*	*NA*	*NA*	*2018, Abril*
itBit	*Bajo*	*4*	*Sí*	*No*	*1*	*Nueva York (EE. UU.)/Singapur*	*Nueva York (EE. UU.)/ Singapur*	*2013, Enero*
Negocie Coins	*Bajo*	*4*	*Sí*	*No*	*1*	*Brasil*	*Brasil*	*2013, Noviembre*
BitFlyer	*Bajo*	*3*	*Sí*	*No*	*4*	*Japón*	*Japón*	*2014, Enero*
BTCBOX	*Bajo*	*1*	*Sí*	*No*	*3*	*Japón*	*Japón*	*2014, Marzo*

1.2 Tipo de volumen transaccional revelado por las plataformas

Los resultados anteriores fueron contrastados con los obtenidos por Bitwise Asset Management (2019) en materia de tipo de volumen reportado por las plataformas a Coinmarketcap. Bitwise Asset Management, en marzo 19 de 2019, presentó ante la Security Exchange Commision de los Estados Unidos (SEC) los resultados del estudio denominado ***El mercado real de bitcoin***, que revela que la mayoría del volumen transaccional reportado por las plataformas es aparente. En su concepto, de los seis billones de dólares americanos de transacción de ***bitcoin***[154] reportados a Coinmarketcap el 9 de marzo de 2019, solo el 5 % que corresponde a transacciones es real. Esta situación obedece, según la investigación, principalmente al incentivo que tienen las plataformas de atraer el listamiento de nuevos activos digitales mediante la presentación de mercados más líquidos y más profundos de lo que realmente son.

Sin embargo, no todos las plataformas reportan volúmenes de transacción por encima del realmente negociado. Después de analizar el comportamiento del libro de órdenes, el tamaño y la distribución de las transacciones y los patrones de comportamiento de las transacciones de 81 plataformas, el estudio concluye que 10 de ellas reportan volúmenes de transacción real. Estas son las que se observan en la figura 1.

Figura 1

Fuente: adaptación de Bitwise Asset Management (2019).

154. Solo se tomaron en cuenta los pares de negociación contra moneda legal y criptomonedas estables (Bitwise Asset Management, 2019).

En consecuencia, para efectos del presente estudio, resulta necesario establecer si existe una relación entre el tipo de volumen reportado, real o aparente, y el número de activos listados en las plataformas. Así entonces, las plataformas fueron divididas en dos grupos: (a) con volumen transaccional real y (b) con volumen transaccional aparente.

En la primera categoría, como es de suponerse, se agruparon las 10 plataformas identificadas por Bitwise Asset Management con volumen transaccional real, mientras que la segunda categoría incluye las 10 plataformas con mayor volumen transaccional de ***bitcoin*** reportado el 19 de marzo de 2019, misma fecha tomada por Bitwise Asset Management, excluyendo aquellas incluidas en el grupo anterior.

Las dos categorías quedaron conformadas tal como se observa en la tabla 3.

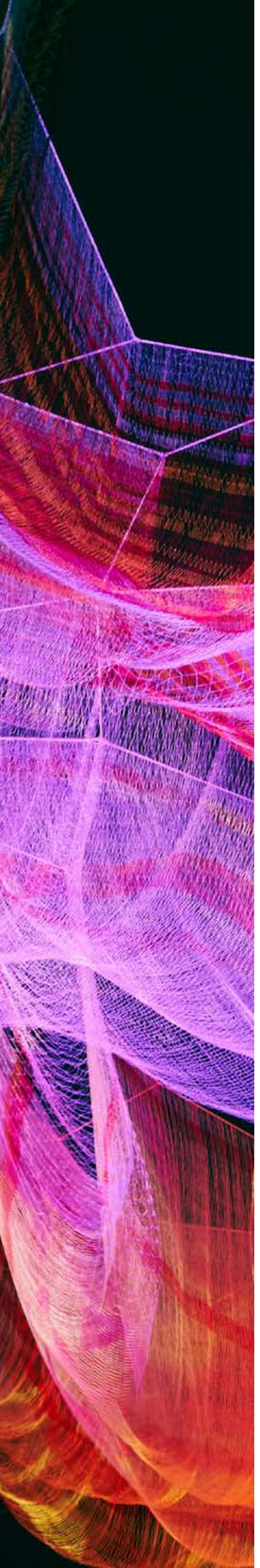
Tabla 3: Agrupación de las plataformas según el tipo de volumen de negociación reportado

Volumen transaccional	
Real	**Aparente**
Binance	Bibox
Bitfinex	BitForex
bitFlyer	BW
Bitstamp	CoinBene
Bittrex	Coineal
Coinbase	DgiFinex
Gemini	IDAX
itBit	OEX
Kraken	OKEx
Poloniex	ZBG

Para cada plataforma se identificó: (a) la posibilidad de intercambio de moneda de curso legal por activos digitales, (b) la disponibilidad de una ***stablecoin***, (c) número de idiomas disponibles en la plataforma, (d) el volumen de transacción diario reportado al 28 de marzo de 2019, (e) el número de jurisdicciones en que está incorporada la compañía responsable de la plataforma, (f) el país de incorporación, y (g) la ley del contrato que regula la relación contractual entre la plataforma y el cliente (tabla 4). Los resultados obtenidos bajo los dos modelos fueron integrados con el objetivo de establecer los arquetipos de modelos de negocio desarrollados por las plataformas (secciones 2.2 y 2.3).

Tabla 4: Plataformas según el tipo de volumen de negociación reportado

Plataforma	Volumen (clasificación)	FIAT par	Stablecoin Par	Idiomas	Volumen reportado (USD)	Pares de negociación	Jurisdicción	Incorporación	Ley del contrato
Binance	*Real*	*No*	*Sí*	*15*	*1.361.815.093,00*	*460*	*1*	*No es claro*	*Singapur*
Bitfinex	*Real*	*Sí*	*Sí*	*4*	*157.511.205,00*	*117*	*2*	*BVI/California (EE. UU.)*	*BVI/California (EE. UU.)*
bitFlyer	*Real*	*Sí*	*No*	*4*	*12.212.007,00*	*3*	*1*	*Japón*	*Japón*
Bitstamp	*Real*	*Sí*	*No*	*1*	*55.714.991,00*	*14*	*2*	*Inglaterra/ Luxemburgo*	*Inglaterra/ Luxemburgo*
Bittrex	*Real*	*Sí*	*Sí*	*1*	*54.586.358,00*	*341*	*2*	*Malta/Washington (EE. UU.)*	*Malta/ Washington (EE. UU.)*
Coinbase	*Real*	*Sí*	*No*	*1*	*77.792.906,00*	*38*	*2*	*Inglaterra/ California (EE. UU.)*	*Inglaterra/ California (EE. UU.)*
Gemini	*Real*	*Sí*	*Sí*	*1*	*12.045.847,00*	*12*	*1*	*Nueva York (EE. UU.)*	*Nueva York (EE. UU.)*
itBit	*Real*	*Sí*	*No*	*1*	*5.862.578,00*	*4*	*2*	*Nueva York (EE. UU.)/ Singapur*	*Nueva York (EE. UU.)/ Singapur*
Kraken	*Real*	*Sí*	*No*	*1*	*76.852.224,00*	*72*	*1*	*California (EE. UU.)*	*California (EE. UU.)*
Poloniex	*Real*	*No*	*Sí*	*1*	*16.584.704,00*	*121*	*1*	*Massachusetts(EE. UU.)*	*Massachusetts(EE. UU.)*
Bibox	*Aparente*	*No*	*Sí*	*6*	*772.699.709,00*	*184*	*1*	*Estonia*	*Singapur*
BitForex	*Aparente*	*No*	*Sí*	*5*	*816.602.200,00*	*165*	*1*	*No es claro*	*No es claro*
BW	*Aparente*	*No*	*Sí*	*4*	*878.660.955,00*	*40*	*1*	*No es claro*	*No es claro*
CoinBene	*Aparente*	*No*	*Sí*	*9*	*818.930.915,00*	*186*	*1*	*Vanuatu*	*Vanuatu*
Coineal	*Aparente*	*No*	*Sí*	*4*	*834.636.232,00*	*58*	*1*	*Seychelles*	*Seychelles*
DgiFinex	*Aparente*	*No*	*Sí*	*9*	*922.920.990,00*	*163*	*1*	*Singapur*	*Singapur*
IDAX	*Aparente*	*No*	*Sí*	*4*	*5.684.13.293,00*	*145*	*1*	*Mongolia*	*Mongolia*
OEX	*Aparente*	*No*	*Sí*	*4*	*232.505.601,00*	*23*	*1*	*No es claro*	*No es claro*
OKEx	*Aparente*	*No*	*Sí*	*9*	*999.654.891,00*	*379*	*2*	*Seychelles /Malta*	*Seychelles /Malta*
ZBG	*Aparente*	*No*	*Sí*	*6*	*912.755.137,00*	*19*	*1*	*No es claro*	*China*



02

Caracterización de las plataformas

Los resultados del análisis de los modelos de (a) número de activos digitales listados y (b) tipo de volumen reportado se presentan y discuten a continuación.

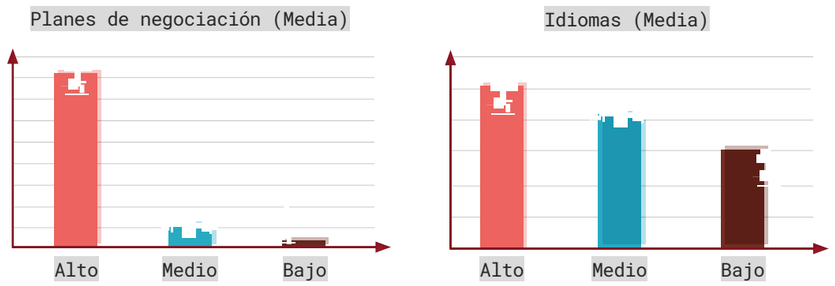
2.1 Plataformas según el número de activos digitales listados

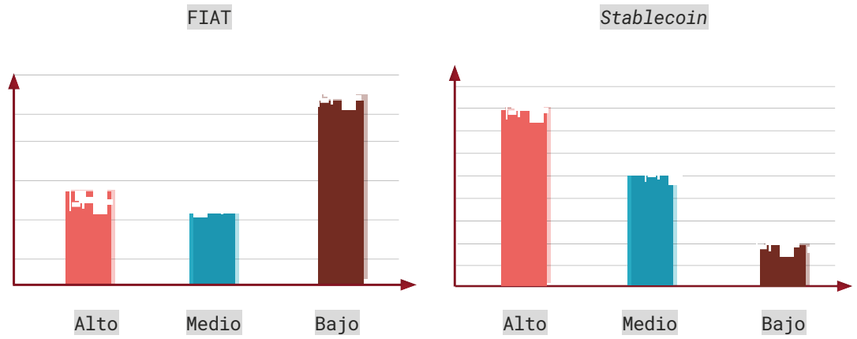
El número de pares de negociación difiere sustancialmente entre los tres grupos. Mientras que la media de pares de negociación en el grupo Alto es de 402, en el grupo Medio baja hasta 42, y en el grupo Bajo no supera los cinco. Esta relación se traslada a la disponibilidad de *stablecoin* en las plataformas, de modo que aquellas con mayor número de pares de negociación son también las que permiten mayoritariamente la adquisición de activos digitales mediante *stablecoins*. De esta manera, mientras que el 80 % de las plataformas del grupo Alto permiten el uso de *stablecoins,* en el grupo Bajo dicha posibilidad solo se tiene en el 20 %.

La situación se invierte cuando se trata de aceptación de FIAT, pues esta se presenta mayoritariamente (80 %) en las plataformas con el menor número de pares de negociación, mientras que los grupos con el mayor número de pares de negociación tan solo la tienen en el 40 %.

Finalmente, se observa que el número de idiomas aumenta en la medida en que las plataformas ofrecen un mayor número de pares de negociación. El promedio de idiomas disponibles en las plataformas con menor número de pares de negociación es de cuatro, y sube a seis en el grupo con mayor número de pares de negociación. La comparación de los tres grupos de plataformas para cada una de las variables aquí analizadas se muestra en la figura 2.

Figura 2: Comparación de las plataformas según el número de pares de negociación





Lo anterior nos permite evidenciar que las plataformas con mayor número de negociación de activos cuentan con mecanismos que facilitan la participación de inversionistas alrededor del mundo, lo que se refleja en el uso generalizado de *stablecoin* y en un mayor número de idiomas en la plataforma. Esta situación se invierte muy claramente en el caso de las plataformas con un menor número de pares de negociación, cuyo uso de *stablecoin* no supera el 20 % y donde el número de idiomas disponibles es menor. Este último tipo de plataformas, muy por el contrario, están focalizadas a servir como mecanismo de intercambio entre FIAT y moneda local, como sucede en el 80 % de la muestra correspondiente.

2.2 Tipo de volumen transaccional revelado por las plataformas

A los resultados arrojados en la sección anterior, donde preliminarmente se evidencia la existencia de dos tipos de plataformas, se suma una variable adicional: el tipo de volumen transaccional reportado. En este sentido, tal como se mencionó en la sección 1, las plataformas tienden a reportan un mayor volumen transaccional al real con el propósito de capturar aquellas compañías interesadas en la emisión de activos digitales para la financiación de proyectos, lo que sugiere que las plataformas que reportan volúmenes transaccionales superiores a los existentes estarán focalizadas en actividades de financiamiento, enmarcándose dentro del prototipo establecido en la sección 2.1.

Antes de entrar a analizar la relación existente el número de pares de negociación y el tipo de volumen reportado por la plataforma, se debe advertir que Binance sobrepasa ampliamente a las otras plataformas agrupadas en la categoría de volumen real reportado. Así supera ampliamente a su inmediatamente anterior (Bitfinex) en más de 1,2 billones de dólares reportado y en más de 100 pares de negociación a quien le sigue en este aspecto (Bittrex). Estas diferencias resultan aún mayores cuando se compara con otras plataformas dentro del

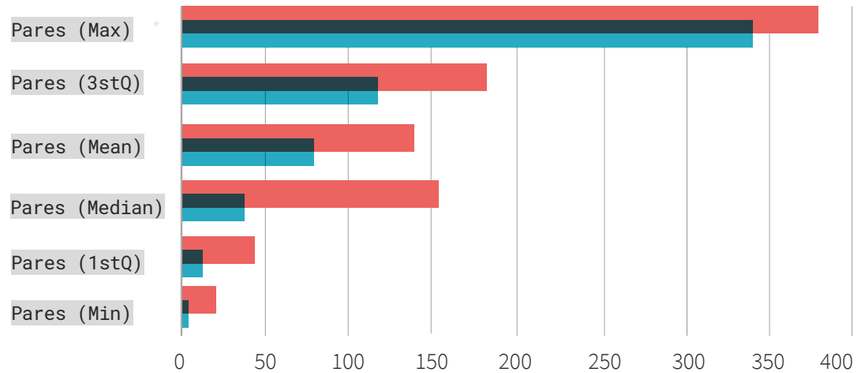
mencionado grupo. En consecuencia, con el propósito de no distorsionar los resultados del grupo de plataformas de volumen real, se excluyó a Binance de la medida de volumen diario reportado y número de activos listados (figura 3).

Figura 3: Distribución de las plataformas por volumen de negación reportado

Al observar las diferencias entre el volumen reportado entre uno y otro grupo, se tiene que el de las plataformas de volumen aparente es sustancialmente mayor al de las de volumen real. En la figura 3 se evidencia cómo el volumen reportado por las primeras es mayor —en promedio 14 veces— a través de toda la muestra. Incluso, el valor mínimo de negociación reportado en el caso de una plataforma de volumen aparente supera al mayor volumen reportado por una plataforma de volumen real.

Por otro lado, en la figura 4 se observa que el número de pares de negación es generalmente superior en el caso de las plataformas de volumen aparente. La media de pares de negociación de las plataformas con volumen real es de 38, mientras que en el caso de los de volumen aparente supera los 150 (figura 4). En consecuencia, y sin que el análisis que aquí se hace pretenda reemplazar un examen estadístico, el cual por demás no resultaría aplicable en razón del tamaño de la muestra, podemos concluir que las plataformas con volumen aparente cuentan con mayor número de activos digitales dispuestos para adquisición del público.

Figura 4: Distribución de las plataformas por número de pares de negociación



	Pares (Min)	Pares (1stQ)	Pares (Mediano)	Pares (Mean)	Pares (3stQ)	Pares (Max)
Aparente	19	44	154	136	179	379
Real sin binance	3	12	38	80,2	117	341

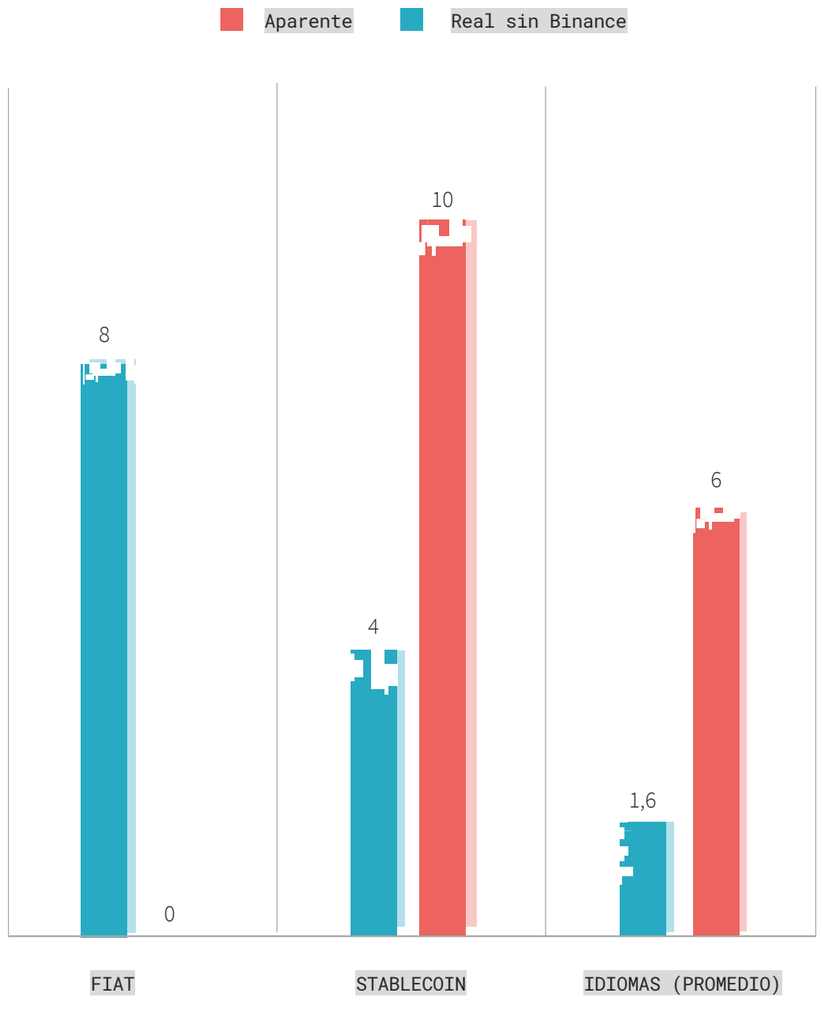
Aparente Real sin Binance

Las plataformas de volumen transaccional aparente no solo cuentan con volúmenes de negociación reportados superiores para atraer a compañías interesadas en la emisión de activos digitales como mecanismo de financiación. A similitud del análisis anterior, estas cuentan con mecanismos que facilitan la participación de inversionistas tales como el uso generalizado de ***stablecoins*** y un mayor número de idiomas disponibles. Así, el 44 % de las plataformas con volumen real están habilitadas para realizar negociaciones mediante el uso de ***stablecoin***s, mientras que todas las de volumen aparente disponen de tal recurso. De la misma manera, en tanto que el promedio

de idiomas disponibles es de seis en las plataformas de volumen aparente, en las de volumen real el promedio no supera los dos idiomas (figura 5).

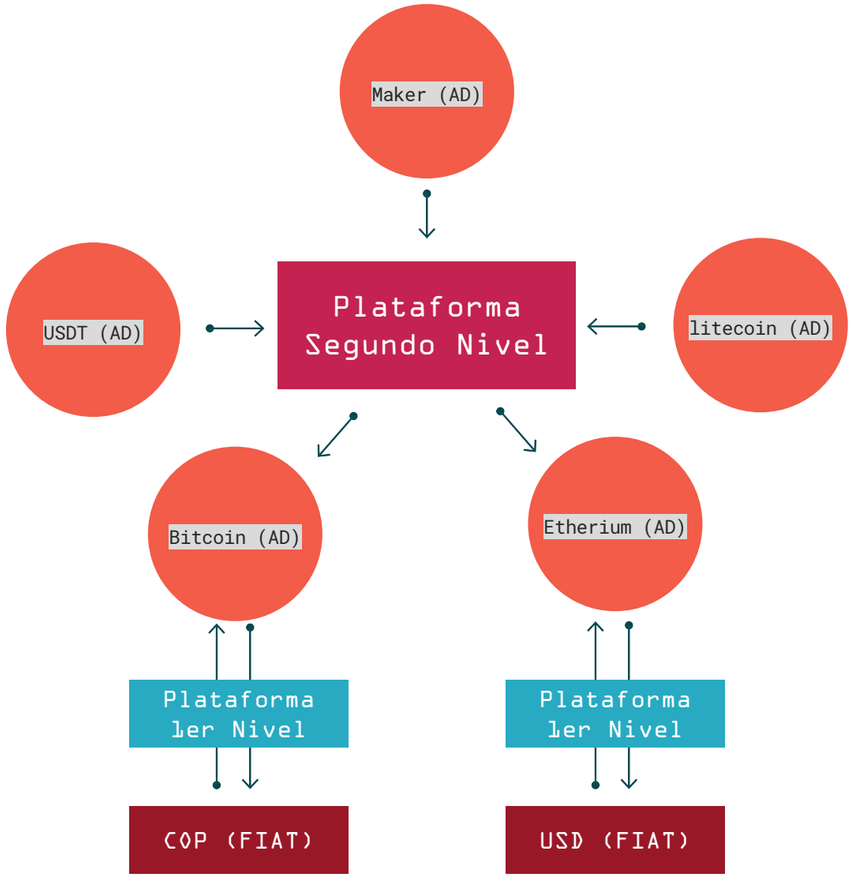
Por otro lado, las plataformas con volumen real están enfocadas a servir como mecanismo de intercambio entre FIAT y activos digitales, siendo más del 80 % plataformas de primer nivel (figura 6). Este resultado contrasta con el de las plataformas de volumen aparente, ninguna de las cuales tiene a su disposición la posibilidad de intercambio de activos digitales por FIAT, siendo exclusivamente plataformas de segundo nivel.

Figura 5: Comparación de las plataformas según el tipo de volumen de negociación reportado



Lo anterior nos permite corroborar la existencia de dos tipos de plataformas distintas en su estructura y finalidad. Las primeras sirven principalmente como mecanismo de financiación de proyectos, lo cual se ve representado en un alto número pares de negociación donde se pueden adquirir los activos digitales por estas emitidos. En este caso los inversionistas alrededor del mundo no tienen restricciones, por lo menos territoriales, al poder adquirir y disponer de dichos activos digitales mediante otros activos digitales como *bitcoin* y cuentan con un mayor número de idiomas a su disposición. Se trata por lo general de plataformas de segundo nivel en las que no se requiere de FIAT y, por ende, tampoco demanda canales bancarios para su funcionamiento de cara al cliente. Por otro lado, las segundas plataformas parecieran servir principalmente al mercado de intercambio de FIAT por activos digitales y viceversa, constituyéndose así en plataformas de primer nivel (figura 6).

Figura 6: Plataformas de primer nivel y de segundo nivel



2.3 Resultados

Nuestro análisis evidencia la existencia de dos prototipos de plataformas según su funcionalidad, los cuales podemos resumir en la tabla 5.

Tabla 5: Tipos de plataformas según su funcionalidad: características

Plataforma Característica	Financiación	Intercambio FIAT-activos digitales
Pares de negociación	Muchos (>100)	Pocos (<10)
Uso de stablecoin	Sí	No
Aceptación de FIAT	Sí	No
Idiomas	Muchos (>5)	Pocos (<5)
Reporte	Mayor al real	Real

Las plataformas analizadas fueron clasificadas dentro de alguno de algunos de los dos prototipos identificados. Así mismo, aquellas que cumplen ambas funciones, permitiendo el intercambio de FIAT por activos digitales y el ofrecimiento masivo de activos digitales, fueron clasificadas dentro una tercera categoría (tabla 6).

Tabla 6: Plataformas según su funcionalidad

Financiación	Intercambio FIAT-activos digitales	Ambos
Binance	bitFlyer	Bitfinex
Poloniex	Bitstamp	Huobi Korea
Bibox	Coinbase	Bittrex
Bitforex	Gemini	Yobit
Coinbene	itBit	
Coineal	Kraken	
Dgifinex	Bitbank	
Idax	Cryptonex	
Okex	Tidebit	
Hitbtc	Coinsbank	
Huobi global	Negocie Coins	
Kucoin	Btcbox	
Gate.io	Coinone	
	Coindeal	

03

¿A dónde van las plataformas?

Una vez clasificadas las plataformas según su funcionalidad, se examinó (a) el lugar de incorporación de la sociedad que administra la plataforma y (b) la ley del contrato que regula la relación contractual de la plataforma con sus usuarios.

Los resultados se resumen en las figuras 7 y 8. En este punto debe advertirse que, para aquellas plataformas que tienen dos domicilios (*i.e.*, Okex, Bittrex, Coinbase, itBit, Bitfinex y Bitstamp), se computó cada uno de estos de manera independiente.

Figura 7: Distribución de las plataformas en razón de su domicilio

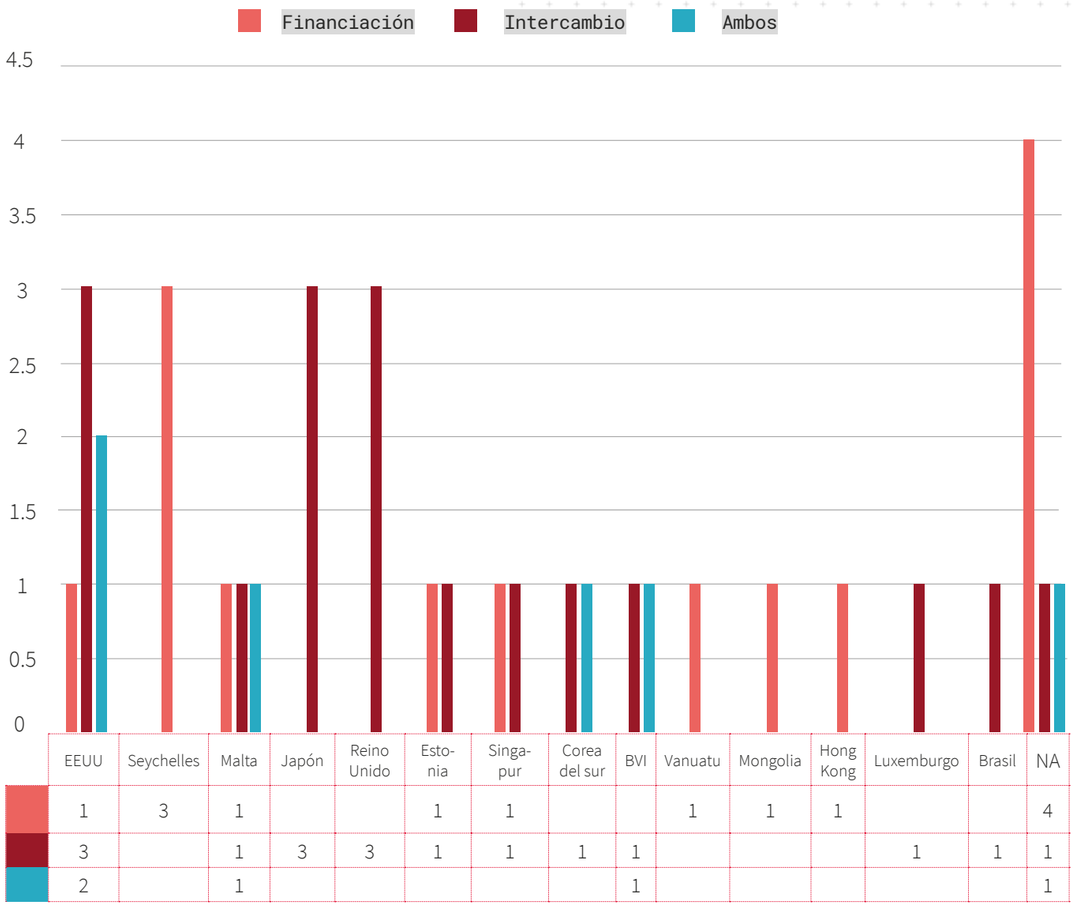
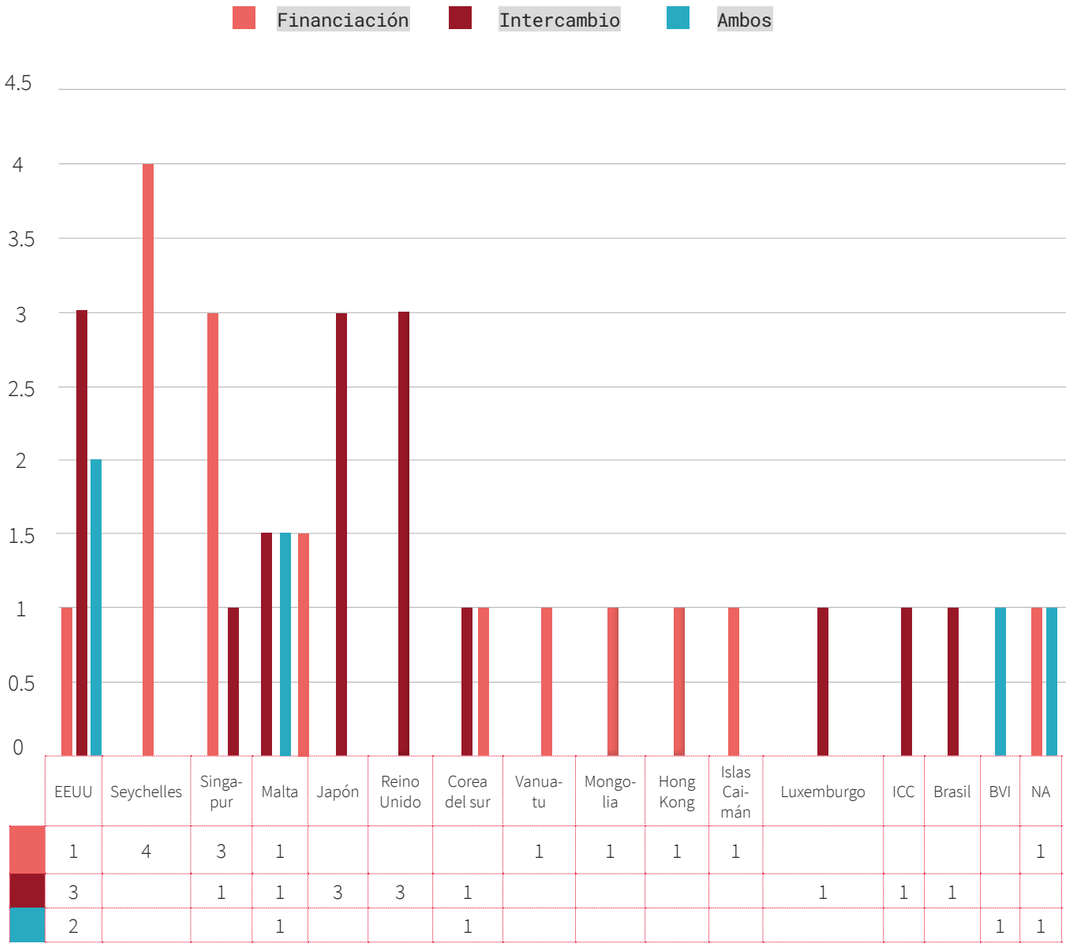


Figura 8: Distribución de las plataformas según la ley del contrato



	EEUU	Seychelles	Singapur	Malta	Japón	Reino Unido	Corea del sur	Vanuatu	Mongolia	Hong Kong	Islas Caimán	Luxemburgo	ICC	Brasil	BVI	NA
	1	4	3	1				1	1	1	1					1
	3		1	1	3	3	1					1	1	1		
	2			1			1								1	1

En primer lugar, es de precisar que no en todos los casos la jurisdicción en la cual se encuentra domiciliada la sociedad que administra la plataforma es igual a la ley que regula el contrato. Por esta razón los resultados de una y otra prueba, si bien son similares, no son iguales. Este el caso, a modo de ejemplo, de Bibox que, aunque se encuentra domiciliada en Estonia, dispone que la ley del contrato es la de Singapur. Así mismo, resulta necesario señalar que el nivel de disponibilidad de información varía entre el domicilio de la sociedad administradora y la ley del contrato. Mientras que en tan solo dos casos no se revela la ley del contrato, dicho número aumenta a seis en el caso del domicilio de la sociedad administradora de la plataforma.

3.1 Distribución por país

El país con un mayor número de plataformas incorporadas es Estados Unidos, con seis. Le siguen Seychelles, Malta, Japón y Reunido Unido con tres cada uno. Por su lado, Estonia, Singapur, Corea del Sur e Islas Vírgenes Británicas cuentan cada uno con dos plataformas. Los demás países de la muestra registran tan solo una plataforma. En el caso específico de Singapur, vale la pena mencionar que, tratándose de la ley del contrato, el número aumenta a cuatro.

Ahora bien, llama la atención que mientras que países como Estados Unidos, Singapur, Malta y Corea del Sur cuentan con plataformas que se enmarcan dentro de los dos prototipos arriba mencionados, otras jurisdicciones atraen solo uno de estos tipos de plataformas. Por un lado tenemos a Seychelles, que solo cuenta con plataformas de financiamiento, mientras que países como Japón y Reino Unido solo tienen plataformas de intercambio.

3.2 Distribución según el tipo de plataforma

Las plataformas de financiamiento se encuentran concentradas en Seychelles y Singapur, con cuatro y tres respectivamente. Otros destinos de incorporación de este tipo de plataformas son Estados Unidos, Malta, Hong Kong, Islas Caimán, entre otros. Por su lado, las plataformas de intercambio se concentran en países como Estados Unidos, Japón, Reino Unido, Corea del Sur, Luxemburgo y Brasil, entre otros. Finalmente, las plataformas que prestan ambos servicios, que son las de menor tamaño en la muestra (cuatro en total), se encuentran en jurisdicciones como Estados Unidos, Malta, Corea del Sur e Islas Vírgenes Británicas.

04

¿La regulación importa?

La jurisdicción de las plataformas difiere en razón de su funcionalidad. Mientras que las de financiamiento se localizan en jurisdicciones como Malta o Singapur, las de intercambio parecieran elegir otro tipo de mercados como Japón o el Reino Unido.

A continuación examinaremos ***cómo la regulación influye en la funcionalidad de las plataformas***. Para tal efecto, analizaremos la regulación aplicable a los activos digitales de las jurisdicciones más representativas de las plataformas aquí analizadas.

4.1 Plataformas de intercambio

4.1.1. Japón

En Japón las plataformas están reguladas por la Ley de Servicios de Pago de 2009, modificada por el Acto Número 62 de 2016, vigente a partir de abril 2017[155]. Dicha ley, adicional a los requisitos en materia de lavado de activos y protección al consumidor y algunos requisitos de funcionamiento[156], establece que las sociedades que administren las plataformas dentro de su jurisdicción deben estar registradas ante la agencia financiera local más cercana a su domicilio. Tratándose de una empresa extranjera, además de tener una oficina y un representante en Japón, debe contar con un registro similar en su domicilio de origen. Por esta vía se limita entonces la entrada de competidores extranjeros en la medida que, con excepción de Malta y algunos Estados de los Estados Unidos, no existen registros equivalentes en otras jurisdicciones.

Adicional a lo anterior, uno de los aspectos fundamentales de la regulación japonesa es el concepto de ***moneda virtual,*** que se asemeja a la definición de critptomoneda presentada en la tabla 1. La adopción de esta definición supone implícitamente la exclusión de ***tokens*** de utilidad y de ***tokens*** de valor. Adicionalmente, dicho país excluye explícitamente los activos denominados en FIAT, eliminando así la posibilidad de ***stablecoins*** dentro del marco de las monedas virtuales.

Esta definición de moneda virtual adoptada por la legislación japonesa explica con suficiencia por qué las plataformas en dicho país limitan su oferta al intercambio de FIAT por criptomonedas como ***bitcoin*** o ***litecoin***, alejando por completo la posibilidad de que plataformas de financiamiento como Binance puedan funcionar dentro de esta jurisdicción.

155. A la fecha de culminación de este documento, 31 de mayo de 2019, se ha reportado que el Parlamento Japonés ha emitido una modificación a la regulación en materia de activos digitales (Token Post, 2019), sin que se haya podido conseguir la versión en inglés de la mencionada adenda. Conforme a lo anunciado en algunos medios (ToKen Post, 2019; Biggs, 2019), una de las mayores modificaciones a esta ley es la sustitución del concepto de activo virtual por la de criptoactivo.

156. La modificación a la Ley de Servicios de Pago además establece algunos requisitos mínimos de funcionamiento como son el de mantener un récord de las transacciones realizadas en la plataforma, y mantener separados el FIAT y los activos digitales de los usuarios de los recursos propios de la Plataforma. Así mismo, establece un capital mínimo de funcionamiento cuya cifra es menor a un millón de dólares americanos. El registro puede ser revocado por la Autoridad de Servicios Financieros cuando evidencie que la sociedad administradora incumpla los requisitos del registro u otras obligaciones derivadas de la Ley de Servicios de Pago

4.1.2 Reino Unido

Las criptomonedas y las actividades relacionadas a su intercambio no son explícitamente reguladas en el Reino Unido, como sucede en la mayoría de los países actualmente[157]. En este caso, el Banco de Inglaterra ha señalado que los activos digitales no comprometen por el momento un riesgo sistémico que amenace la estabilidad financiera, por lo que su regulación en este sentido se considera innecesaria (FCA, 2018).

Por su lado, la FCA (2019) ha sido explícita en señalar que, si las actividades se limitan a facilitar intercambio de activos digitales tipo criptomonedas entre los usuarios, esta no se trata en lo absoluto de una actividad regulada, de manera que las plataforma solo se ven obligadas a cumplir requerimientos de prevención de lavado de activos. De lo aquí expuesto valga la pena destacar que la FCA solo se ha limitado a señalar la posibilidad de intercambio de criptomonedas, excluyendo otro tipo activos digitales, situación que ofrece una primera explicación de por qué las plataformas en dicha jurisdicción se limitan a actividades de intercambio.

Sumado a lo anterior, encontramos que la Financial Conduct Authority (FCA) (2018) ha reconocido que aplicaciones puntuales de los activos digitales, siempre que involucren igualmente fondos en FIAT, podrían llegar a enmarcarse dentro de las actividades reguladas por la Ley de Servicios de Pago (2017) o de la Ley de Moneda Electrónica (2011), requiriéndose por parte de los intervinientes la obtención de las licencias correspondientes. Este sería el caso, por ejemplo, de criptomonedas que son utilizadas para facilitar el funcionamiento de servicios de pago regulados (***e.g.***, transacciones internacionales) o cuando ***stablecoins*** se usan pare servir como medio de intercambio por enmarcase dentro del concepto de moneda electrónica (***e-money***). Así, plataformas como Coinbase, si bien no ofrecen pares de negociación relacionados a una ***stablecoin***, dan acceso a esta, incursionando también en el mercado de servicios de pago.

Adicionalmente, y como ha sido recurrente en varias regulaciones, la FCA ha señalado que en aquellos casos en que los activos digitales puedan ser catalogados como un instrumento financiero se deberá dar cumplimiento a la Ley de Servicios y Mercados Financieros (FCA, 2019; FCA, 2018). Así las cosas, es esperable que las plataformas de financiamiento, más ante la incertidumbre que existe al determinar si un activo digital es o no un valor, prefieran localizarse en jurisdicciones cuya legislación financiera no sea compleja, o por lo menos cuya complejidad sea inferior a la de países con una legislación robusta en materia financiera como es el caso del Reino Unido. Es razonable entonces que plataformas de financiamiento no se incorporen en países como el Reino Unido y por el contrario prefieran establecerse en jurisdicciones con una regulación financiera más flexible, como podría ser el caso de Seychelles o de Islas Vírgenes Británicas. Ahora bien, esto no pretende desconocer que plataformas de financiamiento también se encuentran radicadas en varios Estados de los Estados Unidos, motivadas por las claridades regulatorias en varios de ellos.

157. Esta es la situación típica de los países de la Unión Europea al considerar, hasta el momento, que la tecnología ***blockchain*** y sus aplicaciones, como son los activos digitales, están en una etapa prematura de desarrollo, siendo inconveniente su reglamentación (Miseviciute, 2018)

4.2 Plataformas de financiamiento

4.2.1 Malta

En julio de 2018 Malta aprobó un paquete legislativo en materia de activos digitales y DLT en el que se incluía la Ley sobre Activos Virtuales. Esta permite un amplio campo de maniobra a las plataformas que se incorporen dentro de su jurisdicción, toda vez que dentro del concepto de activo DLT (*DLT Asset*) se incluyen desde criptoactivos hasta instrumentos financieros, pasando por ***tokens*** de utilidad y moneda electrónica. Aunque la ley distingue entre las personas residentes en Malta de aquellas que no, no existen restricciones para la prestación de sus servicios a personas residentes fuera de esta de jurisdicción. En general, la regulación de la isla de Malta se considera amigable con la industria ***blockchain***, que en conjunto con una carga impositiva competitiva (5 %) ha sido capaz de atraer grandes plataformas de financiamiento como Binance y Okex.

4.2.2 Corea del Sur

En Corea del Sur la transacción de activos digitales está legalmente autorizada. A diferencia de lo que sucede con Japón, la definición de activos digitales no se limita a criptomonedas, lo que ha permitido que plataformas de financiación (***i.e.***, Huobi Korea) funcionen en su territorio. Sin embargo, esta plataforma de financiamiento, a diferencia de sus similares en otras jurisdicciones, no tiene un alcance global debido a que la Comisión de Servicios Financieros del país prohíbe a ciudadanos y sociedades extranjeras inscribirse como usuarios de las plataformas que allí operen (Katten Muchin Rosenman LLP, 2019). En adición a lo anterior, los usuarios solo se pueden registrarse con el nombre que acredite su cuenta bancaria, la cual por demás debe pertenecer al mismo banco en que la plataforma tenga sus cuentas (Law Library of Congress, 2018).

4.2.3 Estados Unidos

En EE. UU. el Financial Crime Enforcment Network (FinCen), del Departamento del Tesoro, ha establecido que las plataformas se enmarcan dentro del concepto de negocio de servicios de dinero (*Money Services Business*) en los términos de la Ley de Secreto Bancario (*Bank Secrecy Act*), al considerar que estas proveen servicios de transmisión de moneda o de otros activos sustitutos de moneda (Girasa, 2018) y, por ende, deberán registrarse ante dicha agencia. Valga la pena señalar que la referencia que hace FinCen al término "servicios de transferencia moneda" no distingue entre monedas de curso legal y monedas virtuales, como las criptomonedas (Girasa, 2018). La principal consecuencia de lo aplicación de la ley aquí mencionada es que la plataforma implemente y opere un programa de prevención de lavado de activos y prevención del terrorismo.

Adicional al registro ante la FinCen, a nivel federal, Estados como Alabama, California, Connecticut, Georgia, Idaho, Nevada, Nueva York, Carolina del Norte, Texas y Vermont han emitido regulaciones específicas en materia de activos digitales, donde se exigen licencias estatales para la operación y funcionamiento de las plataformas. En este punto resulta importante anotar que, de las seis plataformas de la muestra localizadas en los Estados Unidos, Poloniex es la única que se encuentra incorporada en un Estado que no cuenta con una regulación expresa en la materia (***i.e.***, Massachusetts), como también es la única que no recibe depósitos de FIAT, lo que evidencia la causalidad directa entre la posibilidad de recibir FIAT y la necesidad de una autorización expresa por parte de las autoridades estatales.

4.2.4 Seychelles

Aunque de Seychelles no existe evidencia de regulación o siquiera de un pronunciamiento de alguna autoridad gubernamental en materia de activos digitales, la radicación de plataformas de financiamiento en dicha jurisdicción (***i.e.***, Huobi Global, Coineal, Okex, y Kucoin) evidencia el apetito que estas tienen de ubicarse en jurisdicciones con bajos niveles regulatorios.

Conclusiones

Aunque la idea generalizada es que los activos digitales no se encuentran regulados, lo cierto es que estos cuentan con definiciones regulatorias mayores a las inicialmente vislumbradas. Esto ocurre aun en aquellos países que no disponen de una regulación explícita en la materia al hacerse uso de normas ya existentes aplicables a los usos de los activos digitales, como es el caso del Reino Unido o Estados Unidos a nivel federal, en materia de servicios de transferencia de dinero y/o pago.

La regulación aplicable a los activos digitales, sea directa o indirecta, constituye un factor determinante en la funcionalidad que cumplen las plataformas conforme a su lugar de incorporación. El estudio evidencia que mientras que las jurisdicciones en que la definición de activo digital se ha limitado al concepto de criptomonedas generan plataformas focalizadas en el intercambio de este tipo de activos digitales por FIAT, en aquellas otras en que el concepto de activo digital se ha hecho extensivo a otros activos digítales (***i.e.***, ***token*** de valor o ***stablecoins***) se promueve la generación de plataformas útiles en el financiamiento de proyectos.

Bibliografía

Amber, P. (2018). From Zero To Crypto Billionaire In Under A Year: Meet The Founder Of Binance. [En línea]. Recuperado de: https://www.forbes.com/sites/pamelaambler/2018/02/07/changpeng-zhao-binance-exchange-crypto-cryptocurrency/#1a2a8f5c1eee. [Consultado el 31 de mayo de 2019].

Biggs, J. (2019). Japan Hardens Rules for Cryptocurrency Storage and Trading. [En línea]. Recuperado de: https://www.coindesk.com/japan-hardens-rules-for-crypto-currency-storage-and-trading. [Consultado el 31 de mayo de 2019].

Bitwise Asset Management (2019). Memorandum file No. SR-NYSEArca-2019-01. [En línea]. Recuperado de https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf. [Consultado el 9 de octubre de 2019].

Chen, L. y Lee, J. (2017). Bitcoin Tumbles as PBOC Declares Initial Coin Offerings Illegal. [En línea]. Recuperado de: https://www.bloomberg.com/news/articles/2017-09-04/china-central-bank-says-initial-coin-offerings-are-illegal. [Consultado el 31 de mayo de 2019].

Euler, T. (2018). The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens. [En línea]. Recuperado de: http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/. [Consultado el 31 de mayo de 2019].

FCA. (2018). Cryptoassets Taskforce: final report. [En línea]. Recuperado de: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf. [Consultado el 31 de mayo de 2019].

FCA. (2019). Guidance on Cryptoassets. [En línea]. Recuperado de: https://www.fca.org.uk/publication/consultation/cp19-03.pdf. [Consultado el 31 de mayo de 2019].

Girasa, R. J. (2018). Regulation of cryptocurrencies and blockchain technologies : national and international perspectives. Palgrave Macmillan (Palgrave studies in financial services technology). [En línea]. Recuperado de: https://search-ebscohost-com.ezp.lib.unimelb.edu.au/login.aspx?direct=true&db=cat00006a&AN=melb.b7190529&site=eds-live&scope=site. [Consultado el 31 de mayo de 2019].

Katten Muchin Rosenman LLP. (2019). Katten's Summary of Cryptoasset Legal and Regulatory Global News. [En línea]. Recuperado de: https://primefinancedisputes.org/files/2019-03/cryptoassets-global-news-study.pdf?45df25ae2e. [Consultado el 31 de mayo de 2019].

Law Library of Congress. (2018). Regulation of Cryptocurrency around the World. [En línea]. Recuperado de: https://www.loc.gov/law/help/cryptocurrency/world-survey.php. [Consultado el 31 de mayo de 2019].

Miseviciute, J. (2018). Blockchain and virtual currency regulation in the EU. Journal of Investment Compliance (Emerald Group), 19(3), 33-38. Doi: 10.1108/JOIC-04-2018-0026.

Ortiz, P. (2019). 13 startups in the Latin American crypto-exchange market. [En línea]. Recuperado de: https://www.contxto.com/en/argentina/latin-american-crypto-exchange-market-map/. [Consultado el 31 de mayo de 2019].

PWC. (2018). Stable Coin evolution and market trends. [En línea]. Recuperado de: https://www.pwc.com.au/pdf/stable-coin-evolution-and-market-trends.pdf. [Consultado el 31 de mayo de 2019].

Securities and Exchange Commission (SEC). (2017). Investor Bulletin: Initial Coin Offerings. [En línea]. Recuperado de: https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings. [Consultado el 31 de mayo de 2019].

Token Post. (2019). Japan's new crypto regulations move to upper house of National Diet. [En línea]. Recuperado de: https://tokenpost.com/Japans-new-crypto-regulations-move-to-upper-house-of-National-Diet-1951. [Consultado el 31 de mayo de 2019].

[[Los contratos inteligentes: (Bajo el ordenamiento jurídico colombiano y en especial, en virtud de las disposiciones de la Ley 527, son válidos y no se le negarán efectos jurídicos, validez o fuerza obligatoria a los mismos) (“El código es ley.”)]].

Daniel Villarroel

“Las personas tienden a temer lo que no conocen. Si las personas que navegaban los océanos en la época de Colón hubieran creído que el mundo es plano, no hubiéramos tenido los grandes descubrimientos del Nuevo Mundo”.

Thomas Emmer[158]

Resumen

Uno de los principales retos en los que se ha venido trabajando desde tiempo atrás en el uso de la tecnología, años antes de la expedición de la Ley 527, es la creación de contratos animados, que se ha materializado a través de los denominados contratos inteligentes. Estos han significado soluciones o avances significativos tanto en el aseguramiento de la confianza y las relaciones patrimoniales como en los problemas esenciales de la teoría contractual. Dado que estos desarrollos han sido generados principalmente por ingenieros, programadores y economistas, y aunque su denominación se ha extendido, la principal discusión ha girado en torno a su validez bajo la esfera legal y, en últimas, determinar si esos contratos se encuentran bajo el lenguaje jurídico y son válidos y ejecutables conforme las normas jurídicas.

En el presente artículo se presenta un acercamiento a la figura del contrato inteligente a través de su definición y de una descripción de sus principales características, para posteriormente formular unas consideraciones sobre las razones prácticas de estas figuras y su validez en el ordenamiento colombiano. De este modo se llega a concluir que: (i) los contratos inteligentes tienen el mismo valor jurídico y probatorio que los contratos de otras formas, y (ii) no se le negarán efectos jurídicos, validez o fuerza obligatoria a un contrato por la sola razón de que se ejecute como contrato inteligente o contenga este término.

Palabras clave: teoría contractual; relaciones transaccionales; derechos de propiedad; algoritmos; ***blockchain***; sistemas de computación; contratos algorítmicos.

158. Presentación del congresista Thomas Emmer en la audiencia a la SEC en el Congreso de los Estados Unidos de América respecto de los tokens de utilidad: https://www.youtube.com/watch?time_continue=1&v=EO3qYW9DF-A.

Abstract

One of the main challenges that has been working for a long time in the use of technology, years before the issuance of Law 527, is the creation of animated contracts, which has materialized through the so-called smart contract. These contracts have also meant significant solutions or advances in the assurance of trust and patrimonial relations as in the essential problems of contractual theory. Given that these developments have been generated mainly by engineers, programmers and economists and although their denomination has been extended, the main discussion has revolved around their validity under the legal sphere, ultimately, determine if those contracts are contracts under the language legal and if they are valid and enforceable under legal rules. In this article we present an approach to the figure of the smart contracts, through its definition and main characteristics, to later formulate some considerations on the practical reasons of these figures and their validity in the Colombian legal system, concluding that: (i) smart contracts have the same legal value as contracts of other forms and (ii) shall not be denied legal effects, validity or enforceability solely because that the contract is executed trhough a smart contract or contains this term.

Key Words:

01

Definición

Apalancados en los conceptos y las características de los contratos inteligentes derivados de la construcción teórica de dicha figura por Nick Zsabo —quien fue la persona que acuñó la denominación "contratos inteligentes" (Zsabo, 1996) — y del *White Paper* de la ***blockchain*** Ethereum[159], planteamos su definición en los siguientes términos: un contrato inteligente es una programación dirigida por eventos con estado[160], que computariza cualquier lógica o regla arbitraria y que se ejecuta sobre una ***blockchain***. Este se usa para automatizar las transacciones una vez se satisface el código concebido y desplegado, incluyendo —pero no limitado a— la custodia y el control de activos o la transferencia de estos, la creación y distribución de activos digitales y la sincronización de la información por el propio código[161].

Para efectos del presente artículo, adelantamos el análisis de los contratos inteligentes bajo el entendimiento de la figura tradicional del contrato de una manera amplia y general, indistinto de su denominación o alcance, sea que se trate como convención, contrato, acto jurídico, negocio jurídico o declaración de voluntad[162]. Así pues, se entiende que hacemos referencia de forma genérica y amplia a la disposición de intereses patrimoniales y personales por parte de los sujetos.

159. Ethereum es la segunda blockchain creada y de mayor nivel de importancia después de bitcoin. El White Paper actualizado de la Ethereum se puede consultar en el siguiente enlace: https://github.com/ethereum/wiki/wiki/White-Paper.

160. O un protocolo transaccional computarizado.

161. No existe un consenso sobre una definición única de contratos inteligentes. Para efectos de una aproximación, adicional a la definiciones técnicas de los artículos de Nick Zsabo y el White Paper de Ethereum, ténganse como referencia, desde la perspectiva jurídica, las definiciones similares de contratos inteligentes contenidas en las normas jurídicas del Estado de Arizona (de firmas, transacciones electrónicas y tecnología blockchain —signatures; electronic transactions; blockchain technology— en https://legiscan.com/AZ/text/HB2417/id/1588180) como del Estado de Tennessee (https://legiscan.com/TN/text/SB1662/2017).Ley de Arizona: "'Smart contract' means an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger".Ley de Tennessee: "'Smart contract' means an event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that:

- (A) Take custody over and instruct transfer of assets on that ledger;
- (B) Create and distribute electronic assets;
- (C) Synchronize information; or
- (D) Manage identity and user access to software applications".

162. Incluyendo las definiciones de contrato de los artículos 1495 del Código Civil y 864 del Código de Comercio

02

Principales características

A partir de esta definición del contrato inteligente, consideramos importante, aunque de forma general por las limitaciones de espacio, ahondar en sus principales características. Esto, por demás, nos permitirá un mejor entendimiento de los elementos mínimos de los contratos inteligentes y aterrizar su concepto. Las consideraciones que a continuación se exponen se sustentan principalmente en el funcionamiento de la ***blockchain*** Ethereum y del lenguaje de programación Solidity[163].

2.1 Ejecución automática

La ejecución automática es la principal característica atribuida por regla general a los contratos inteligentes. Esta automatización implica que las disposiciones de un contrato están determinadas como un evento por un lenguaje de programación, de manera que una vez se produce tal evento, se ejecuta (acciona) el código y, por ende, la disposición correspondiente.

Esta ejecución da lugar a un cambio en el estado de la máquina —o el estado de transición—. Siguiendo el *White Paper* de Ethereum (s.f.), el contrato inteligente se entiende como una caja criptográfica que contiene valor y solo es desbloqueada si se cumplen ciertas condiciones. Es por esto que suele señalarse la compra en máquinas expendedoras de bebidas como el antecedente de los contratos inteligentes, ya que una vez insertadas las monedas en la máquina se ejecuta la entrega de la bebida.

Dada la relevancia de la característica de automatización en la ejecución del contrato, así como de su adecuado entendimiento, consideramos relevante presentar unas consideraciones sobre: (i) el concepto del sistema de estado de transición y (ii) la ejecución del código.

2.1.1. El sistema del estado de transición

El protocolo de los contratos inteligentes se soporta en estados, por lo que dicho término se incluye en la definición de aquellos. Bajo la ciencia de la computación, los contratos inteligentes y ***blockchain*** se estructuran sobre la información de todas las transacciones desde el momento cero —la génesis—, y el estado, en términos generales, se entiende como una descripción del programa diseñado para recordar los eventos precedentes. Así, bajo un circuito de lógica secuencial, las salidas son una función tanto de las entradas actuales como de las pasadas.

Bajo este sistema se verifica la veracidad del estado en un momento 1, contrastando la situación y los elementos de un estado anterior (estado 0), y así sucesivamente. De modo ilustrativo podemos tomar como ejemplo el caso de las transacciones bancarias, donde el estado (S) es el balance, una transacción (tx) es iniciada pasando una

163. Solidity es un lenguaje de programación de nivel alto, orientado para la implementación de contratos inteligentes (influenciado por C++, Python y JavaScript) designado para la Ethereum Virtual Machine (EVM) con distintas características sofisticadas y complejas. De la creación de Solidity puede inferirse el desarrollo práctico logrado en la evolución de los contratos inteligentes.

suma de dinero (20) de la cuenta de Alice a la cuenta de Bob y la función del estado de transición disminuye el dinero de la cuenta de Alice en 20 e incrementa el valor de la cuenta de Bob en 20, lo que da lugar a un nuevo estado (`S'`). Si la cuenta de Alice tiene menos de 20 en el primer momento, la función del estado de transición devuelve un error.
Lo anterior se expresa computacionalmente de la siguiente manera:

```
APPLY(S,TX) -> S' or ERROR
```

De manera lógica, se parte del supuesto de que Alice no puede transferir a Bob una cantidad de dinero X si ella no tiene por lo menos dicha cantidad en su cuenta, por lo que en la transacción son posibles dos resultados: (i) error: la función del estado de transición devuelve un error —siguiendo el ejemplo, cuando Alice tiene en su cuenta menos de 20— o (ii) `S':` el sistema permite la transacción y crea un nuevo estado en la máquina (acredita los 20 en la cuenta de Bob y los debita de la cuenta de Alice), cuando Alice al iniciar la transacción tiene en su cuenta por lo menos 20[164].

Lo anterior se expresa computacionalmente de la siguiente manera:

```
APPLY({ Alice: $50, Bob: $50
},"send $20 from Alice to Bob")
= { Alice: $30, Bob: $70 }

APPLY({ Alice: $50, Bob: $50
},"send $70 from Alice to Bob")
= ERROR
```

2.1.2. El sistema de estado de transición en Bitcoin

Ahora miremos este estado de transición bajo la tecnología ***blockchain*** y su ambiente computacional. Tomando el caso de Bitcoin para entenderlo desde un punto técnico, en el sistema de estado de transición existe un estado de la propiedad de todos los ***bitcoins***, y una función de estado de transición que toma un estado y una transacción y genera un nuevo estado que es el resultado[165]. Adicionalmente, en comparación con el ejemplo anterior, en Bitcoin se agregan más herramientas para verificar tanto la existencia de la cuenta y la propiedad de esta como que el propietario es quien inició la transacción. Esto se hace a través de la generación de llaves (tanto pública como privada) por medio de criptografía de curva elíptica (ECC).

Siguiendo con el análisis de Bitcoin, el estado en este caso es la suma de todos los ***bitcoins*** (técnicamente, las salidas de transacciones no gastadas "UTXO" —***Unspent Transaction Outputs***—) que han sido minados y no gastados todavía. Cada UTXO tiene una denominación y un propietario (definido por una dirección de 20 bites que corresponde a una llave pública criptográfica)[166]. Una transacción contiene una o más entradas —cada una de las cuales contiene una referencia a un UTXO existente y una firma criptográfica generada por la llave privada asociada con la dirección del propietario— y una o más salidas —cada una de estas contiene una nueva UTXO para ser agregada al estado—.

164. Para los ejemplos usaremos las denominaciones "Alice" y "Bob", que son los caracteres comúnmente usados, entre otros campos, en la criptografía. Valga indicar que estos caracteres fueron creados por Ron Rivest, Adi Shamir y Leonard Adlemany en la publicación del artículo "A method for obtaining digital signatures and public-key cryptosystems". El uso de Alice y Bob debe entenderse de forma comprensiva, no refiriéndose exclusivamente a humanos, sino pudiendo tratarse de agentes genéricos tales como computadores o programas que se ejecutan en un computador. El artículo mencionado pude ser consultado en el siguiente enlace: https://dl.acm.org/citation.cfm?id=359342.

165. Usamos Bitcoin en mayúscula para referirnos al protocolo y bitcoin en minúscula respecto de las unidades en las que este se divide.

166. Técnicamente, una dirección de Bitcoin es el hash de la llave pública y no la llave pública como tal. Sin embargo, se ha extendido el uso del término "llave pública" para hacer referencia al propio hash de esta en el concepto práctico de firmas digitales.

La función del estado de transición `APPLY(S,TX) -> S'` en Bitcoin, de forma general, contiene los siguientes pasos:

1. Por cada entrada en TX:

- Si la UTXO referenciada no está en S, devuelve un error. Este paso previene transacciones enviadas por ***bitcoins*** que no existen.

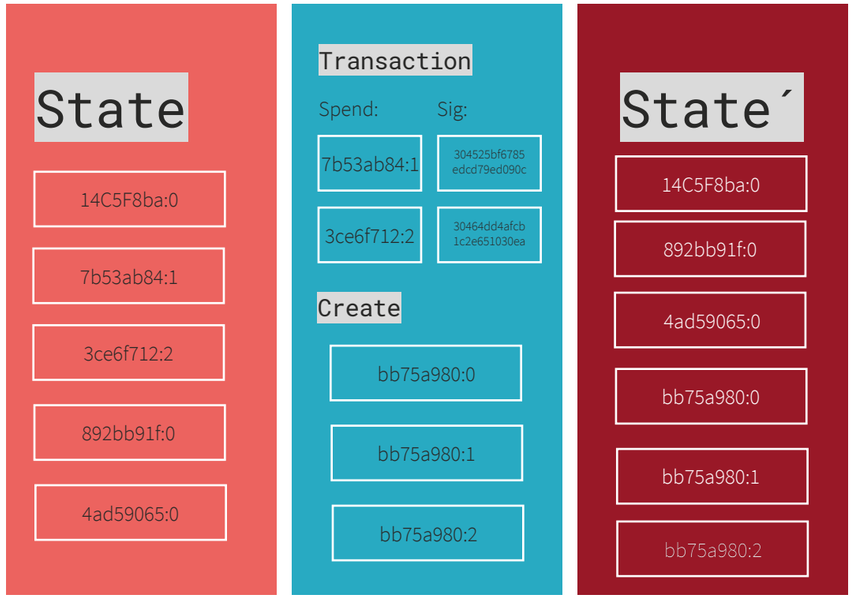
- Si la firma proveída no coincide con el propietario de la UTXO, devuelve un error. Este paso previene transacciones enviadas de ***bitcoins*** de otras personas o por quien no es el propietario[167].

2. Si la suma de la denominación de todas las entradas UTXO es menor que la suma de todas las salidas de UTXO, devuelve un error. Este paso asegura el valor de la transacción.

3. Devuelve `S'` con todas las entradas de UTXO removidas y todas las salidas de UTXO agregadas. Este paso es la creación de un nuevo estado cuando se han verificado de forma exitosa los pasos anteriores.

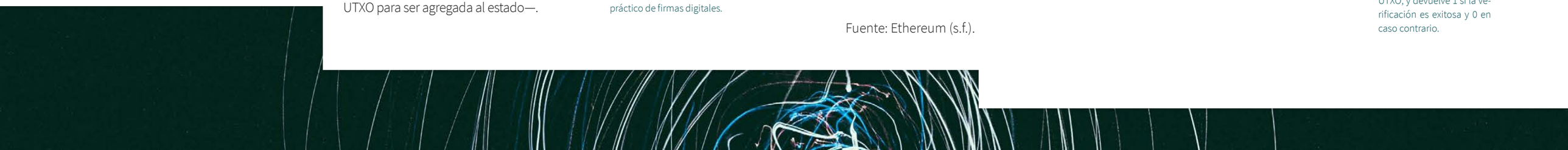
En la ***blockchain*** de Bitcoin se puede visualizar el estado de transición como la función donde se despliegan todas las transacciones en la base distribuida y descentralizada tal como se observa en la figura 2.

Figura 1



Fuente: Ethereum (s.f.).

167. Para garantizar la propiedad, el mecanismo de propiedad de la llave pública es implementado vía ***script***. El ***script*** toma una firma de curva elíptica como entrada, la verifica contra la transacción y la dirección propietaria de los UTXO, y devuelve 1 si la verificación es exitosa y 0 en caso contrario.



2.2.3. El sistema de estado de transición en los contratos inteligentes

Siguiendo el análisis y tomando el caso de la ***blockchain*** de Ethereum, el estado es compuesto por objetos denominados cuentas, cada una de las cuales tiene igualmente una dirección de 20 bites y donde el estado de transición corresponde a transferencias de valor e información entre ellas[168]. Bajo Ethereum existen dos tipos de cuenta: (1) cuentas de propiedad externa que son controladas por llaves privadas y (2) cuentas de contrato que son controladas por el propio código del contrato. En una cuenta de contrato, cada vez que se recibe un mensaje se activa su código, lo que permite leer y escribir en su almacenamiento interno, enviar otro tipo de mensajes o crear nuevos contratos si es requerido.

Los contratos inteligentes funcionan bajo la arquitectura de Bitcoin señalada, pero con dos componentes adicionales: (i) se agregan datos a la transacción que no son exclusivamente valor, y (ii) una dirección puede ser un contrato en sí mismo, controlada por el propio código. En esa medida, los contratos son usados para codificar funciones de estados de transición arbitrarios, permitiendo no solo la transferencia de valor como en los casos anteriores, sino muchas otras lógicas a través de la escritura de estas en líneas de código.

Siguiendo con los ejemplos, ya no solo podemos codificar que Alice transfiera 20 a Bob, una vez se verifica y valida que ella tiene por lo menos 20 en su cuenta, es propietaria de la cuenta y con su firma fue la que inició la transacción, sino que podemos codificar que Alice transfiera 20 a Bob el día Y o cuando ella reciba el activo Z o infinidad de supuestos. Así, una vez acaecido el supuesto correspondiente, que está insertado en una dirección ***blockchain*** a través de un lenguaje de programación, se satisface el ***script***, con lo que este mismo código ejecuta automáticamente el contrato (transfiere a Bob los 20), sin intervención humana alguna.

Teniendo en cuenta las consideraciones anteriores, podemos determinar que los contratos inteligentes son agentes autónomos que se despliegan dentro de una ***blockchain*** y que ejecutan su propio código si se cumplen todas las reglas por las cuales fueron concebidos. Generalmente, estas reglas derivan en una transacción donde se tiene un control directo sobre el balance actual de los activos digitales (***ether*** en el caso de Ethereum) y el almacenamiento de sus variables internas, a las cuales se les puede mantener total trazabilidad a lo largo del tiempo.

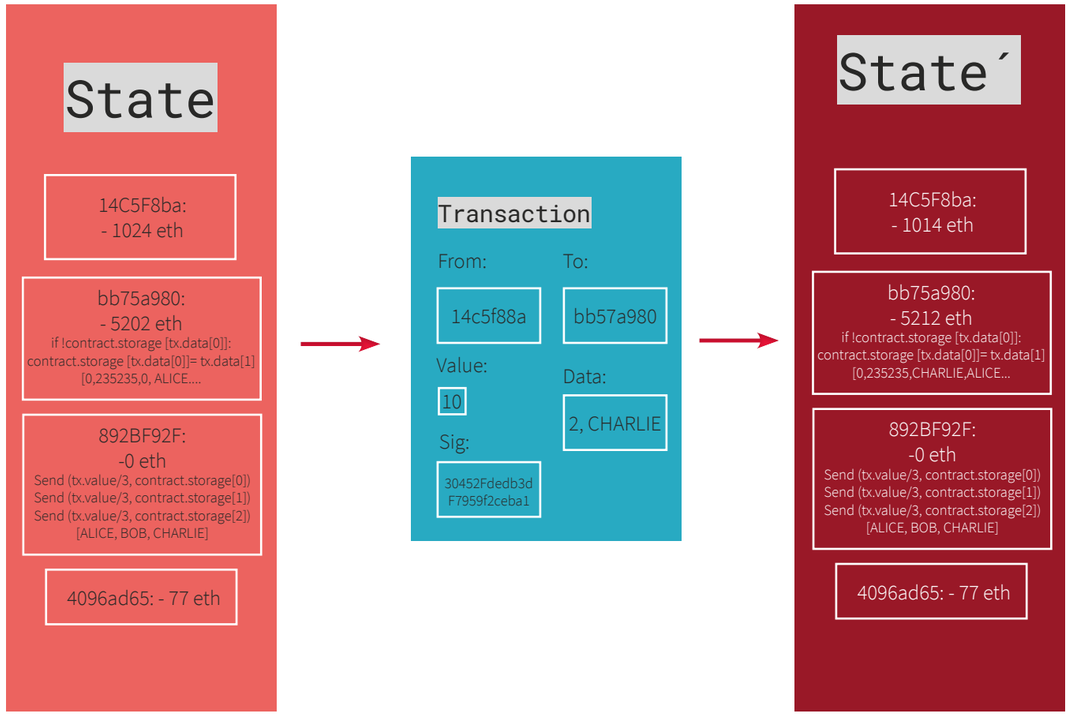
Valga indicar que cada transacción tiene un costo, que para el caso de Ethereum corresponde al ***gas***, que es el resultado de los bites que se usan en la transacción —en términos generales, el poder computacional—. Tomando en cuenta la anterior anotación, es necesario precisar que cuando se da una instrucción y por ende se ejecuta el código del contrato, este último se ejecuta hasta que se complete o hasta que no sea posible seguir ejecutándose por falta de ***gas***.

Técnicamente, es posible la ejecución de forma infinita de una regla o condición en un contrato inteligente pero, dado el costo de la transacción, lo adecuado es limitar las condiciones de los contratos al punto específico de que estas lleguen a cumplirse de manera satisfactoria. Si el valor transferido falla por falta de dinero o la ejecución del código se queda sin ***gas***, se revierten todos los cambios de los estados de transición salvo el pago de la comisión.

Así mismo, debe señalarse que es posible crear contratos inteligentes bajo otras ***blockchains***, sin dejar de mencionar la propia disposición de intereses —acto jurídico— que se configura con la transferencia de valor en la ***blockchain*** de Bitcoin (unidades de ***bitcoin*** transferidas de Alice a Bob), lo que depende, en principio, del conjunto de computación que soporte el lenguaje de ***script*** de la correspondiente ***blockchain***. Así, por ejemplo, en la ***blockchain*** de Bitcoin, las UTXO señaladas pueden ser propiedad no solo de una llave pública, sino de un ***script*** expresado en un lenguaje de programación simple basado en cualquier ***stack*** de desarrollo. Bajo este supuesto, una transacción bajo el protocolo UTXO debe proveer información que satisfaga el ***script*** concebido y desplegado.

La función del estado de transición —o estado de la máquina— de un contrato inteligente sencillo bajo la ***blockchain*** Ethereum se puede visualizar en la figura 2.

Figura 2



Fuente: Ethereum (s.f.).

168. Una cuenta de Ethereum contiene el ***nonce*** para asegurar que cada transacción es procesada solo una vez, el balance de ***ether***, el código del contrato y el almacenamiento.

2.2.4. La ejecución del código

El código de los contratos inteligentes (que varía de acuerdo con la ***blockchain*** usada y, por ende, con el correspondiente lenguaje de programación, que en el caso de Ethereum consiste en un lenguaje basado en un ***stack*** orientado a objetos) está conformado por una serie de bites, cada uno de los cuales representa una operación. En general, la ejecución del código es un loop infinito[169] que consiste en ir incrementando el contador del programa de a una unidad a la vez (la cual empieza en cero), hasta que al final el código es ejecutado satisfactoriamente o una instrucción de stop o return es detectada.

En caso de no ser ejecutado satisfactoriamente, se da un error y, por ende, se arroja una instrucción de throw. En esa medida, siguiendo el modelo del código de la máquina de Ethereum, su modelo de ejecución y estado computacional completo puede entenderse por el tuple[170] (estado del bloque, transacción, mensaje, código, memoria, stack, pc y gas). El estado del bloque es el estado global que contiene todas las cuentas, los balances y el almacenamiento y cada instrucción tiene su propia definición en términos de cómo afecta el tuple.

De conformidad con lo señalado, podemos concluir que (i) tanto la ejecución del código como el bloque están sujetos a una validación algorítmica. De esto puede desprenderse que, técnicamente, el término más apropiado podría ser el de "contratos algorítmicos" más que el de "contratos inteligentes". Por otro lado, (ii) el despliegue de unas reglas de negocio ejecutadas en lenguaje computacional y controladas por el propio código permiten afirmar de forma altisonante, y siguiendo el principio establecido en el artículo 1602 del Código Civil —incorporado por demás en la mayoría de los ordenamientos jurídicos—, que el código es ley —Code is Law—.

2.2. El lenguaje de programación

El lenguaje de programación para expresar las reglas o lógica de negocio, en el caso de Ethereum, es Turing completo. Es decir, se trata de una máquina virtual Turing completo construida sobre una ***blockchain*** (***Ethereum Virtual Machine*** —EVM—), bajo el entendido de que el código usado para construir el contrato inteligente puede codificar, al menos teóricamente, cualquier regla o transacción que puede ser matemáticamente definida, incluso los ***loops*** infinitos[171]. Esto, nuevamente de manera muy resumida, permite a cualquier persona codificar cualquier lógica o regla de negocio arbitraria.

Así mismo, es importante señalar, frente a la ejecución del código en términos del hardware físico, que tal proceso para el contrato es parte de la definición de la función del estado de transición, que a su vez es parte del algoritmo de validación del bloque. Por lo tanto, si por ejemplo una transacción es agregada en el bloque A, la ejecución del código generada por esa transacción será ejecutada por todos los nodos que descarguen y validen el bloque A, ahora y en el futuro.

169. Existen otros mecanismos para garantizar la consistencia respecto de iniciar aquello que se puede ejecutar, tales como el costo del ***gas*** —el poder y costo computacional requerido para llevar a cabo una operación—.

170. Un tuple, en términos generales, se entiende como un tipo de datos que representa a las tuplas, que a su vez son un único valor que agrupa varios valores. http://progra.usm.cl/apunte/materia/tuplas.html.

171. No es necesario un lenguaje específico, tomando Solidity, que es el lenguaje de Ethereum solo como referencia, aunque cabe señalar que existen distintos lenguajes de programación en distintas ***blockchains***.

2.3. Blockchain

En la definición de contratos inteligentes señalada, se indicó como elemento que el contrato —o la expresión de este en programa computacional— se ejecuta en una ***blockchain***. Ahora, si bien el concepto de contratos inteligentes fue creado por Nick Szabo en 1996, estos solo pudieron hacerse realidad a través de una tecnología que surgió mucho después, a finales de la primera década de este siglo. Incluso, el fundamento de estos contratos comparte gran parte de las características de esta tecnología (firmas digitales —según el concepto computacional y no jurídico de la Ley 527 y los decretos reglamentarios[172]—, criptografía, distribución y descentralización), hasta tal punto que una de las unidades en las que se divide el ***ether***, el activo de la ***blockchain*** de Ethereum, lleva su nombre. En definitiva, lo cierto es que nuestro alcance y la definición de contratos inteligentes se delimitan sobre esta tecnología.

Después de hacer realidad el dinero programable a través de Bitcoin, que permite la interacción económica en internet, los contratos inteligentes son, a la fecha, la aplicación más interesante y disruptiva del ecosistema tecnológico. Bitcoin, cuyo ***White Paper*** se publicó el 31 de octubre de 2008, es el surgimiento, la génesis de ***blockchain***, y es el medio a través del cual se crea una red persona a persona —***peer-to-peer*** (P2P)— que permite llevar y mantener un registro público, único y común de manera totalmente distribuida, donde se almacenan todas las transacciones (entendidas como unidades de información) que son diseminadas por toda la red.

Dicho registro público o libro contable es generado y almacenado también de manera distribuida, de modo que todos los participantes estén de acuerdo en su contenido sin la intervención de autoridades centrales o terceros de confianza. Esto es lo que se denomina ***blockchain*** —cadena de bloques—, en la medida en que las transacciones de la red se van agrupando en bloques, que a su vez se van encadenando y enlazando de manera secuencial (cada bloque contiene información del bloque anterior). Con el paso del tiempo, nuevos bloques son creados y añadidos a la cadena existente, y así este registro público contiene todas las transacciones anteriores[173] desde la transacción cero, información que puede ser verificada y conocida por todas las personas participantes de la red.

Teóricamente, este encadenamiento requiere modificar todas las transacciones y bloques anteriores para modificar un solo dato de una transacción. Por lo tanto, la cadena de bloques es un registro que solo permite aumentar la información. De este modo, el conjunto de transacciones aceptadas como válidas por la red son aquellas contenidas en cada uno de los bloques que pertenecen a la cadena, por lo que, con el tiempo, se dificulta cada vez

172. Acá no interviene una entidad de certificación.

173. Otras ***blockchains*** distintas de Bitcoin funcionan bajo otra arquitectura y no contienen ni guardan la historia completa en cada bloque, haciendo uso de distintas estructuras del ***Merkle Tree***; por ejemplo, almacenando una sola vez los datos y usando indicadores de estos, tales como ***hashes*** de ***subtrees***.

más alterar cualquier información, al contar cada vez con más bloques relacionados.

Los sistemas distribuidos han existido de tiempo atrás, pero la gran disrupción hecha realidad por ***bitcoin***, más allá de ser la primera criptomoneda criptográfica y un activo digital sin respaldo ni valor intrínseco y sin un emisor centralizado o alguien que lo controle, trascendiendo la definición de moneda, divisa y poder liberatorio ilimitado del ordenamiento jurídico, puede sintetizarse de forma general en tres puntos.

En primer lugar, el encadenamiento ***blockchain*** evita el doble gasto, es decir, permite comprobar y verificar que no se está gastando dos veces un activo o en general cualquier transacción, por cualquier persona, sin necesidad de que medie la intervención de una autoridad central o tercero de confianza. En segundo lugar, asegura los titulares de los activos a través de firmas digitales en cada transacción, dado que cada dirección de Bitcoin representa una llave pública y solo se pueden hacer transferencias a través de la llave privada asociada a esa llave pública (como se indicó, Bitcoin está sustentado en criptografía de curvas elípticas). En tercer lugar, Bitcoin es la primera solución práctica al problema de seguridad de los sistemas distribuidos conocido como el problema de los generales bizantinos: el dilema de lograr un consenso entre un conjunto de entidades con un objetivo común cuando entre ellas pueden existir traidores, es decir, entidades con objetivos opuestos que intenten dinamitar el proceso. En el caso de Bitcoin, tal consenso se da a través de ***proof-of-work*** (prueba de trabajo), lo que ha permitido en su desarrollo la creación de muchos más atributos y aplicaciones.

Estas características muy resumidas —y no exhaustivas— dan lugar al surgimiento del internet del valor, que permite por primera vez en la historia transferir directamente propiedad digital a otro usuario de la red, de manera que solo el propietario pueda hacerlo y únicamente el destinatario pueda recibirla. Esto se logra en la medida en que la transferencia es validada y reconocida por todos los participantes (nodos) de la red, de manera totalmente descentralizada y distribuida.

Blockchain toma su valor para el caso de los contratos inteligentes por tratarse de una tecnología sustentada en un consenso distribuido. En relación con la importancia y delimitación de dichos contratos a esta tecnología, debe señalarse que Nick Szabo contempló un protocolo casi 10 años antes del surgimiento de ***blockchain*** a través de la tecnología de bases de datos replicadas que mantienen un registro público, evitando ser centralizadas y permitiéndoles "sobrevivir a una guerra nuclear"[174].

En su planteamiento, Szabo analiza y reconoce la importancia de los registros escritos que han dado surgimiento a nuestro sistema actual de derechos de propiedad a través del seguimiento a la cadena de la transferencia del derecho de dominio. Sin embargo, cuestiona la vulnerabilidad de los registros escritos, los abusos a los que pueden verse sometidos —como la posibilidad de su destrucción o alteración—, la existencia de errores y fraude en la reconstrucción de registros y cómo los repositorios o registros electrónicos centralizados han sido incluso peor dado que son altamente vulnerables a su pérdida o alteración, principalmente por las personas que interactúan con ellos. Ahora bien, en la práctica no se encontraban disponibles sistemas de bases de datos replicadas, por lo que el protocolo nunca fue implementado hasta el surgimiento de Bitcoin, que hizo realidad las bases de datos distribuidas, descentralizadas, replicadas y compartidas.

Finalmente, sobre estas consideraciones generales de ***blockchain*** debe señalarse que esta tecnología, que es la infraestructura sobre la que se crea Bitcoin, cuenta con otras aplicaciones derivadas de los atributos señalados que permiten múltiples aplicaciones. Entre estas se incluyen el uso de activos digitales para representar instrumentos financieros (***colored coins***) y la propiedad de activos físicos (***smart property***) y de bienes no fungibles como dominios ***web*** (***namecoin***). También es posible encontrar aplicaciones más complejas que involucran activos digitales directamente controlados por una pieza de código que implementa reglas arbitrarias, como en el caso de los contratos inteligentes acá analizados, o incluso organizaciones autónomas soportadas en ***blockchain*** (DAO).

174. Este protocolo puede consultarse en el siguiente enlace: https://nakamotoinstitute.org/secure-property-titles/.

03

La razón de ser de los contratos inteligentes. ¿Para qué?

Una vez descritas de forma general las características y los elementos de los contratos inteligentes, la siguiente inquietud gira en torno a la necesidad o importancia de estos, e incluso surge la pregunta apremiante de si simplemente se están acogiendo por tratarse de una nueva tecnología sin que exista un cuestionamiento o análisis alguno.

Para dar respuesta a este interrogante, haremos uso de dos aproximaciones: (i) la realidad del comercio frente al derecho contractual y (ii) las implicaciones prácticas de la ejecución de los contratos.

3.1. La realidad del comercio frente al derecho contractual

Dos supuestos fácticos deben tenerse en cuenta para el análisis de los contratos inteligentes: (1) la teoría contractual —y no solemos ser conscientes de eso— es fruto de la evolución de miles de años de comercio, gobernanza e intercambio sin ser un monopolio del derecho, donde los contratos son un fundamento de nuestro comercio y modelo económico[175], y (2) nuevas instituciones y nuevos mecanismos de formalización de las relaciones han emergido producto de una era cibernética y unas relaciones en línea que crecen de forma exponencial[176].

A través de siglos de evolución han emergido el concepto de contrato y sus principios. Estos conceptos e ideas que rodean a los contratos —tómese el ejemplo del refinamiento y extensión del derecho de dominio—, sobre los que se sustentan nuestras relaciones comerciales y nuestra economía de mercado, implicarían igualmente siglos para far lugar a nuevos desarrollos o reemplazos[177]. Sin embargo, la aparición de nuevas tecnologías, en especial aquellas denominadas como tecnologías de la Cuarta Revolución Industrial (Schwab, 2017), prometen —y en algunos caso ya hacen posible— la materialización de opciones que no eran concebibles[178].

Para el caso de los contratos, bajo la óptica de la teoría algorítmica de la información, dichas estructuras evolucionadas milenarias implicaban, por regla general, un costo prohibitivo para computarizarlas. Sin embargo, con el surgimiento de ***blockchain*** y los avances de las ciencias de la computación y de la criptografía, se han descubierto variados y nuevos algoritmos que, combinados con los mensajes de datos, hacen posible una amplia variedad de nuevos protocolos. Para el caso específico de los contratos, esto hace posible la ejecución de algoritmos como la transmisión de mensajes de forma más sofisticada, amplia y comprensiva, incluyendo reglas o lógicas de negocio arbitrarias, antes prohibitivas.

En esa medida, no solo enfrentamos un desafío tecnológico, sino que se nos presentan herramientas que pueden diseñar, ejecutar y definir de manera más precisa, eficaz y adecuada las relaciones humanas y la formalización de estas. Así, los contratos inteligentes son producto —una evolución de la teoría contractual que comprende no solo la esfera jurídica— del reconocimiento de los mejores usos de la tecnología en el comercio, utilizando protocolos e interfaces para automatizar o facilitar todas las etapas del ciclo contractual, desde su formación hasta su liquidación y eventuales controversias. De esta forma se cuenta con nuevos mecanismos para formalizar y asegurar relaciones electrónicas y para solucionar los problemas que envuelve la teoría de los contratos.

Para efectos de ilustrar lo anterior, tómese por ejemplo el caso sencillo, pero con serios efectos negativos, de los múltiples y constantes errores en la práctica derivados de la deficiencia en la redacción de los contratos[179] y la posibilidad de que los términos de un acuerdo expresado en un leguaje natural puedan ser trasladados dentro un código o codificados en un lenguaje ***script***. En la práctica, usando códigos computacionales se logran considerables ventajas en la redacción de cláusulas contractuales, y si bien un código computacional es más limitado que el lenguaje natural, el primero genera mayor certeza y claridad, restringiendo de forma valiosa y concreta las interpretaciones de una cláusula.

Así mismo, y siguiendo este ejemplo de la redacción, adviértase cómo a través de los contratos inteligentes podemos estandarizar las mejores prácticas que no son posibles ni en los contratos físicos

175. La teoría contractual ha sido realmente en su mayoría una construcción propia de la economía. Esto se evidencia con el hecho de que economistas (Oliver Hart y Bengt Holmström) hayan sido reconocidos con el premio Nobel por, entre otros, sus análisis del diseño de los contratos, los contratos reales, las instituciones y los contratos imperfectos, ratificando su importancia en su función más que en su naturaleza o calificación.

176. El hecho de que en nuestro país la adopción tanto de estas tecnologías como del comercio electrónico siga siendo embrionaria, principalmente por esa dependencia imaginaria a una norma que defina y autorice expresamente todas las opciones y avances del mercado, no deja de ser una barrera artificial que, sin embargo, no impedirá finalmente la inmersión de dichas tecnologías en las relaciones comerciales, cada vez más globales y electrónicas. En todo caso, el riesgo práctico que enfrentamos es que bajo un ***darwinismo tecnológico***, la falta de adopción nos impida sobrevivir o adaptarnos oportunamente a esas nuevas condiciones económicas y sociales.

177. Para la descripción histórica del derecho de dominio, propiedad y el comercio, cfr. Hayek (s.f.).

178. Importante considerar, en este análisis del derecho contractual y en general de la teoría del derecho, el planteamiento de Yuval Nahari en su libro ***21 lecciones para el siglo XXI***, según el cual las nuevas estructuras sociales y económicas, y en general nuestro modelo, estarán definidas en esta nueva era por la ciencia de la computación y la tecnología (y sus profesionales) y no por los abogados y políticos, como en épocas pasadas.

179. Cfr. Hart (2016a).

ni en la mayoría de los contratos electrónicos, como por ejemplo revisar, testear, auditar y probar un contrato antes de su redacción definitiva —producción para el caso de los contratos inteligentes— e incluso durante su ejecución[180]. No se debe dejar de mencionar que, lógicamente, todos los riesgos no son eliminados ni es una solución absoluta, y que existen varios elementos que deben mejorarse, propios de toda tecnología nueva (por ejemplo, dado que el software es escrito por humanos, puede contener ***bugs***).

Finalmente, frente a estas ventajas de los medios electrónicos en comparación con los medios físicos en el campo jurídico, resulta pertinente resaltar el reconocimiento que en esa vía hizo la Corte Constitucional al revisar la constitucionalidad de la Ley 527. Al respecto se manifestó así: *"Los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley"*[181].

3.2. Las implicaciones prácticas de la ejecución de los contratos

Bien sea que el contrato sea ejecutable de manera forzada por un Estado o por otro mecanismo, tal documento es la base de la estructura de la economía de mercado. Esta ejecución del contrato inteligente sin intervención humana previamente señalada tiene bastantes atributos y ventajas: por ejemplo, hacer el incumplimiento de un contrato bastante costoso o incluso prohibitivo y, en últimas, lograr que efectivamente los contratos se cumplan[182].

El dinero (Graeber, 2011; Davies, 1994) como los contratos (Simpsont, 1979; Horwitz, 1974) son creaciones bastante anteriores al derecho y al Estado y, lógicamente, a toda la teoría del negocio jurídico. Como con precisión lo señalaba el profesor Hinestrosa:

> *En algún momento de su devenir, cada pueblo "primitivo" debió´ inventar el "trato", es decir, el acto dispositivo de intereses, muy posiblemente para el intercambio de bienes con otro pueblo, con reconocimiento, o mejor, consciente de la firmeza y obligatoriedad de su comportamiento* (Hinestrosa, 2013)[183].

180. Confrontar, por ejemplo, mejores prácticas en la programación de contratos inteligentes (https://consensys.github.io/smart-contract-best-practices/general_philosophy/). Valga indicar que actualmente ha tomado fuerza el diseño de los contratos mediante el cual se busca que sean más comprensibles para los usuarios no jurídicos, enfocados más en diseño y experiencia de usuario (principalmente bajo metodologías ágiles y design thinking), que son valiosos en el acercamiento a todas las personas que interactúan en el tráfico mercantil pero igualmente se encuentran excluidos de la definición indicada de contratos inteligentes, que se limita a un alcance computacional.

181. Corte Constitucional. Sentencia C-662/00.

182. Para una aproximación a la ejecución forzada, aunque desde una óptica del common law, véanse Kronman (1978) y Alan Schwartz (1979). En el presente artículo no se considera la diferencia entre inejecución e incumplimiento de un contrato propia de los ordenamientos jurídicos de tradición romano germánica, que permite concluir que no toda inejecución de un contrato conlleva per se su incumplimiento. En todo caso, es importante tener en cuenta el análisis de los fenómenos de incumplimientos "justificados" bajo la imprevisión, causas imputables y demás fenómenos desde la perspectiva económica a Posner y Rosenfield (1977).

183. En este sentido también son ilustrativas las referencias al respecto de Betti (1944) a las narraciones de Heródoto y de Alvise Ca' Da Mosto (s. XV), como también las anotaciones sobre el surgimiento de la economía de cambio en Roma que hace Guarino (1981, p. 668 y ss.).

En el análisis práctico de los contratos y su función frente a las relaciones patrimoniales y personales, uno de los principales desafíos surge sobre la confianza —o mejor, la desconfianza— en la disposición de intereses, bien sean personales o patrimoniales, de forma concomitante con su formación. *"Confianza-desconfianza, fides, crédito, son conceptos y actitudes que están en la raíz del tráfico jurídico. Si no hay un mínimo de confianza, no es posible imaginar trato alguno cuya ejecución no sea simultánea con su celebración (absolutamente real)"* (Hinestrosa, 2013).

Por lo anterior, la inventiva de los seres humanos, propia de las necesidades sociales, económicas y del mercado, más que de construcciones teóricas o académicas de otras esferas, ha girado en torno a la creación de medios para asegurar o facilitar los contratos que no eran absolutamente reales. Estos, igualmente necesarios e indispensables en el comercio, pasan por múltiples mecanismos, bien sean compulsivos, persuasivos o sancionatorios, como la ***compositio*** a través de un rehén, la amenaza de ***vindicta*** del grupo ante el incumplimiento, la configuración del incumplimiento como un delito, el castigo de los poderes infernales ***(damnatio)***, hasta mecanismos actuales reactivos propios del poder coercitivo del Estado. Se trata de recursos para asegurar la seriedad y certeza de la voluntad declarada por el contratante con el propósito de garantizar la creencia en la palabra empeñada, tales como ***serio et deliberato animo***, a través de distintos rituales o solemnidades (***i.e., gesta per aes et libram, in jure cessio, mancipatio, sponsio, stipulatio***).

Al final, de forma constante e incesante, se han concebido mecanismos y figuras de confianza y aseguramiento para que los privados puedan impulsar su actividad económica y disponer de sus intereses, lo que se materializa en esta evolución en la figura del contrato inteligente. Por lo demás, son instrumentos que no funcionan bajo el mecanismo reactivo usual de nuestro sistema, sino bajo un mecanismo preventivo, entre otras, porque pueden ser auditados y verificados durante su ejecución.

Lo anterior nos permite señalar, como elemental e inherente a los contratos, no solo la necesidad de proteger los intereses de los particulares, sino la misma necesidad de impedir hasta donde sea posible la inejecución de los contratos para permitir el desenvolvimiento del comercio y de las relaciones. Por lo demás, el cumplimiento de los contratos está configurado como un principio jurídico supremo en nuestro ordenamiento: *"El principio jurídico supremo del cual emana todo el derecho de las obligaciones convencionales señala que la finalidad económico-social del contrato lleva implícita el cumplimiento de las estipulaciones en él pactadas. Los contratos se celebran para cumplirse y, por ello, son ley para las partes".* Este postulado se encuentra establecido en el artículo 1602 del Código Civil, a cuyo tenor *"todo contrato legalmente celebrado es una ley para los contratantes, y no puede ser invalidado sino por su consentimiento mutuo o por causas legales"*. En un sentido similar, el artículo 864 del Código de Comercio define el contrato como un *"acuerdo de dos o más partes para constituir, regular o extinguir entre ellas una relación jurídica patrimonial"*[184].

Debe indicarse que la generación de confianza es otro de los atributos disruptivos de los contratos inteligentes, componente que es parte esencial de la filosofía de ***blockchain***, hasta tal punto que algunos señalan que la verdadera innovación de esta tecnología es la confianza[185]. Esto se observa toda vez que dicha confianza estaría depositada en algo que nadie controla —sin intermediarios o entes centralizados— pero que es inmutable, verificable y conocido por cualquiera, sin ser duplicado, alterado ni falseado, con una historia digital común.

Adicionalmente, los contratos inteligentes abren la puerta para lograr soluciones a distintas problemáticas de la teoría contractual, más allá de la eficiencia y eficacia en la formación y ejecución. Así, por ejemplo, estos contratos y la propia programación pueden configurarse en la solución de la problemática de los derechos de control residual o derechos de decisión de los contratos incompletos planteada por Oliver Hart a través de una asignación eficiente de estos en la máquina. Así mismo, los contratos inteligentes se configuran en una posibilidad de eliminar o mitigar el problema de ***hold-up*** igualmente planteado por Hart, o incluso como respuesta ante la existencia de incumplimientos estratégicos (incumplimientos deliberados que resultan más beneficiosos para una parte)[186].

184. CSJ, Sala de Casación Civil, M. P. Ariel Salazar Ramírez, SC11287-2016, Radicación N.º 11001-31-03-007-2007-00606-01 del 17 de agosto de 2016.

185. Werbach (2018) analiza el desafío para el derecho de ***blockchain*** como una relación y necesidad mutua entre el derecho y ***blockchain.***

186. Para el comportamiento de incumplimientos estratégicos, cfr. Benmelech (2009) y Benmelech y Bergman (2008).

04

La validez y los efectos de los contratos inteligentes bajo el ordenamiento jurídico colombiano

Se ha generado en varias latitudes una discusión —consideramos su razón por tratarse de una creación por fuera del derecho— sobre la validez de los contratos inteligentes bajo las normas jurídicas. Esto ha llevado incluso a que ciertos ordenamientos reconozcan de forma expresa la validez a los contratos inteligentes. Así, por ejemplo, se han expedido las normas jurídicas en los Estados de Arizona y Tennessee[187] previamente señaladas, las cuales han sido fuertemente criticadas en ciertos espacios por considerase innecesarias y tautológicas, en las que se establece que los contratos inteligentes pueden existir en el comercio y que a un contrato relacionado con una transacción no se le negarán efectos legales, validez o fuerza obligatoria por el hecho de que sea ejecutado a través de un contrato inteligente[188].

Sin perjuicio de los cuestionamientos que genera la necesidad —obsesión— del estudio jurídico de clasificar o reconocer bajo una taxonomía existente cualquier fenómeno para que con base en dicha clasificación pueda brindársele un reconocimiento jurídico[189], de conformidad con la Ley 527 —comprendiendo está dinámica de las evoluciones sociales y económicas, que son el motor del derecho— y siendo suficiente el principio de equivalencia funcional, podemos concluir que a los contratos inteligentes debemos darles la misma validez y valor probatorio de la que gozan los contratos por medios físicos o tradicionales. La sencilla razón de esto es que el contrato o negocio jurídico sigue siendo el mismo, independiente del lenguaje en que se exprese o el medio que se use o su funcionamiento. De manera que, como tal, el contrato inteligente habrá de regirse de conformidad con las normas aplicables al correspondiente negocio jurídico.

Aunque la figura del contrato inteligente va más allá de los contratos electrónicos, al menos frente a la percepción práctica que tenemos de estos[190], es relevante indicar que estos últimos existían y eran válidos previo a la expedición de la Ley 527, norma que vino a darles

187. https://legiscan.com/AZ/text/HB2417/id/1588180 y https://legiscan.com/TN/text/SB1662/2017 respectivamente. Valga indicar que varios Estados de los Estados Unidos han expedido normas de iniciativa blockchain que contienen disposiciones de aplicaciones de la tecnología blockchain, como firmas y registros.

188. *No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract is executed through a smart contract.*

189. *"En verdad, las categorías no son sino el fruto de una elaboración imponente de generaciones, en gran parte anónima, de una tradición más que milenaria que tiene sus raíces en el estudio del derecho romano, tal como vino siendo entendido por varias generaciones de juristas que se fueron sucediendo hasta llegar a nosotros"* (Betti, 1942).

190. Técnicamente, sería más preciso indicar que los contratos inteligentes son una especie de los contratos electrónicos, entendiendo estos de forma amplia como cualquier contrato por medios no físicos. En todo caso, valga mencionar que los contratos inteligentes son funcionales, a diferencia de las demás formas, que son inanimadas o estáticas, sin que sea fundamental que se cuente con inteligencia artificial, al tiempo que las condiciones y estipulaciones del contrato especificadas de forma digital —lenguaje de programación— son ejecutadas por el protocolo, es decir, sin necesidad de intervención humana. Podemos señalar tres diferencias generales entre los demás contratos electrónicos y los contratos inteligentes: (i) estos últimos están insertados por lo menos en un programa computacional para ejecutar ciertas tareas, (ii) el contrato es un agente autónomo y (iii) las formas de contratación electrónica usan por regla general protocolos asincrónicos, mientras que los pasos de los contratos inteligentes, todos, son normalmente sincrónicos.

certeza probatoria y jurídica a los mensajes de datos bajo cualquier perspectiva. Piénsese, solo como ejemplo, en los contratos formados a través de una llamada telefónica, que eran —y son— válidos y existían antes de la expedición de dicha regulación. Señálese igualmente la búsqueda de muchos años por expresar los contratos en un lenguaje computacional, que tiene como referente los contratos ricardianos, igualmente concebidos previos a la expedición de la Ley 527 y utilizados en distintas áreas prácticas. Adicionalmente, existen otros contratos electrónicos muy comunes en nuestro tráfico mercantil, que son de alguna manera los precursores de los contratos inteligentes (en especial aquellos que usan funciones o medidas de encriptación y firmas digitales), tales como las terminales POS (*point of sale*), los EDI usados para las transacciones entre empresas, SWIFT y otros mecanismos de transferencia y compensación de pagos entre bancos y el uso de terminales de los parqueaderos públicos, e igualmente existentes y válidos antes de la Ley 527. Todos estos ejemplos no solo existen en el comercio, sino que son válidos jurídicamente y generan plenos efectos, por lo que no se encuentra algún fundamento fáctico o jurídico para darles un tratamiento distinto a los contratos inteligentes frente a los tradicionales.

La Ley 527 es, entonces, una ley de carácter probatorio que permite aplicar las mismas consecuencias jurídicas que ostentan los medios físicos o tradicionales a la utilización de medios electrónicos.

Adicionalmente, no existe prohibición que impida expresar las disposiciones de un contrato en términos de datos o para que las relaciones estén representadas en mensajes de datos. Así, tómese el caso de la oferta y la aceptación como elementos de la formación del contrato: para el caso de los contratos inteligentes, por ejemplo, la oferta puede ser insertada y comunicada en la ***blockchain***, y cualquier miembro de esta puede aceptarla a través de la firma de la transacción con su llave privada o mediante un acto inequívoco como el depósito de un activo digital en un contrato inteligente, medios de oferta y aceptación que son válidos en Colombia.

Incluso, no obstante no ser necesario argumento adicional, existen otros elementos de la validez y efectos de los contratos inteligentes en nuestro ordenamiento que podemos señalar: (i) el propio artículo 14 de la Ley 527 señala, frente a la formación y validez de los contratos, disposiciones aplicables a los contratos inteligentes acá descritos, en la medida en que (a) en la formación de los contratos, tanto la oferta como la aceptación pueden ser expresados en un mensaje de datos y (b) no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos[191]; (ii) de conformidad con el literal a) del artículo 2 de la Ley 527, no existe limitación al medio que puede usarse para los mensaje de datos[192], y (iii) de acuerdo con el artículo 15 de la Ley 527, en las relaciones entre el iniciador y el destinatario de un mensaje de datos no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

Valga señalar, en especial frente a la programación y diseño de los contratos inteligentes, que, tal como lo permite el artículo 4 de la Ley 527, las partes pueden acordar las reglas contenidas en el capítulo III, parte I, que toman relevancia para los aspectos propios de estos contratos.

De conformidad con lo anterior, bajo los principios de equivalencia funcional y neutralidad funcional equiparables a todas las figuras, incluyendo pero sin limitarse a los contratos, y siguiendo la redacción de los artículos 5, 14 y 15 de la Ley 527 bajo nuestro ordenamiento jurídico: (i) los contratos inteligentes tienen el mismo valor jurídico y probatorio que los contratos de otras formas y (ii) no se les negarán efectos jurídicos, validez o fuerza obligatoria por la sola razón de que se ejecuten como contrato inteligente o contengan este término.

191. *Artículo 14. Formación y validez de los contratos. En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos".*

192. *"Artículo 2. Definiciones. Para los efectos de la presente ley se entenderá por:*

a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax".

Adicionalmente, aplicando el principio de autonomía privada o libertad contractual que irradia nuestro ordenamiento jurídico del derecho privado, se contempla la libertad para las partes de escoger la forma de expresión de sus relaciones como los mecanismos de funcionamiento de estas (Hinestrosa, 1999). Esto refuerza la validez del contrato inteligente, independiente de su forma de mensaje de datos o su funcionamiento.

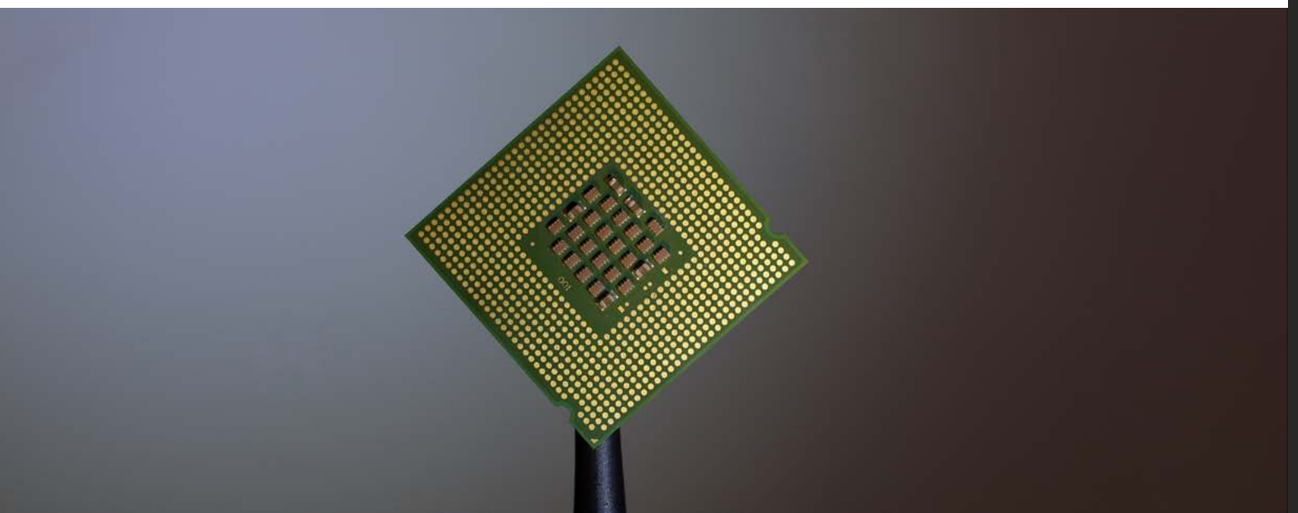
Debe señalarse que los contratos inteligentes, y en general las relaciones comerciales automatizadas o ejecutadas bajo nuevas tecnologías, presentan ciertos desafíos. Algunos de ellos son: bajo ciertas situaciones, determinar cuál es la ley aplicable a ellos y qué elementos deben tomarse para determinar el lugar u otros aspectos de los supuestos de aplicación espacial; las implicaciones de la autoridad de algoritmos; el uso de algoritmos computarizados para negociar contratos; la intervención de agentes electrónicos autónomos en la creación y operación de contratos[193]; la representación de identidad a través de medios no tradicionales; la ***tokenización*** de los derechos que recaen sobre activos físicos; el uso de activos digitales como medio de pago; atipicidad para ciertas relaciones[194]; la resolución de conflictos, y múltiples más[195].

Todos estos desafíos vienen siendo enfrentados por la propia tecnología. Igualmente, consideramos que podemos y debemos aplicarles los principios y reglas existentes de nuestro ordenamiento, que contienen un marco suficiente para su validez, efectos y fuerza obligatoria, y que no por sus eventuales problemas o diferencias en la aplicación práctica de figuras tradicionales pueden dar lugar a afectar la validez del contrato inteligente.

193. Sin dejar de indicar que los contratos inteligentes pueden alterar en el futuro la estructura de los derechos y obligaciones y que en la práctica código autónomos pueden operar independiente del sistema legal, posibilidades que tampoco les restan validez.

194. Considérese igualmente el desafío de nuevos mecanismos de funcionamiento en organizaciones como el caso de DAO. Para un acercamiento a estas nuevas formas, consultar el ***White Paper*** de DAO en el siguiente enlace: https://download.slock.it/public/DAO/WhitePaper.pdf.

195. Los análisis concretos de estas figuras exceden al presente artículo, pero consideramos pertinente al menos mencionarlas y señalar su uso en el comercio. Aunque parezca algo remoto, actualmente vemos cómo las empresas usan algoritmos computacionales en la formación de contratos, y piénsese por ejemplo en los casos más usados —pero no los únicos— para las operaciones de compra y venta de mercados financieros electrónicos y para la fijación del precio en el comercio en línea.



Conclusión

La figura de los contratos inteligentes es producto de la contribución de diversos campos como la computación, la economía, la criptografía, la teoría juegos y el derecho, y aunque se sustenta en todos los avances construidos por siglos en la teoría contractual y nuestro modelo de libre mercado, y por ende no se construye desde cero, sí rompe paradigmas vigentes por siglos de nuestra teoría contractual. Con todo, los contratos inteligentes no implican que todo lo anterior es negativo o malo, sino que de alguna manera es limitado y es posible ampliarlo, contribuyendo en la solución de los principales problemas de la teoría contractual.

En todo caso, esta nueva figura se encuentra cobijada bajo el ordenamiento jurídico colombiano, contando con plena validez, efectos y fuerza obligatoria, tal y como sucede con los contratos en papel o de otras formas. Lógicamente, la aparición de estas nuevas figuras genera nuevos desafíos, en especial respecto a la solución de las controversias que se puedan suscitar entre las partes contractuales, en las cuales debemos hacer uso igualmente de soluciones innovadores y disruptivas que permitan su desarrollo e implementación. De esta manera evitaremos ser prisioneros de los instrumentos conocidos, entendiendo en la aproximación de dichas soluciones que, al ser el contrato en general una respuesta a las realidades del comercio —y el contrato inteligente, en especial, a la dinámica vertiginosa del comercio electrónico en las relaciones privadas—, la aproximación debe enfatizarse en su función por sobre su naturaleza y no limitarse a la esfera jurídica.

A lo anterior debe agregarse que, frente a dicha dinámica de las relaciones actuales, no pueden —ni deberían— los sujetos esperar el entendimiento o refinamiento de un sistema para su aplicación donde, nuevamente, el contrato mantiene su valor, más en su función que en su calificación.

Bibliografía

Bellia, Anthony J. Jr. (2001). Contracting with Electronic Agents. ***Emory L. J., 50***.

Benmelech, E. (2009). Asset Salability and Debt Maturity: Evidence from Nineteenth Century Railroads. ***Review of Financial Studies*** (22), 1545-1584.

Benmelech, E. y Bergman, N. (2008). Liquidation Values and the Credibility of Financial Contract Renegotiation: Evidence from U.S. Airlines. ***Quarterly Journal of Economics*** (123), 1635-1677.

Betti, E. (1942). ***Istituzioni di diritto romano***. Padova.

Betti, E. (1994). ***Teoria generale del negozio giuridico***.

Calo, Ryan (2015). Robotics and the Lessons of Cyberlaw. ***Cal. L. Rev, 103,*** 513, 532.

Cifrino, Christopher J. (2014). Virtual Property, Virtual Rights: Why Contract Law, Not Property Law, Must Be the Governing Paradigm in the Law of Virtual Worlds. ***B. C. L. Rev., 235***, 254-64.

Davies, Glyn (1994). ***A History of Money: from Ancient Times to the Present Day***. Cardiff: University of Wales Press.

Ethereum (s.f.). ***A Next-Generation Smart Contract and Decentralized Application Platform.*** [En línea]. Recuperado de: https://github.com/ethereum/wiki/wiki/White-Paper. [Consultado el 27 de junio de 2019].

Fairfield, A. T. (2014). Smart Contracts, Bitcoin Bots, and Consumer Protection. ***Washington and Lee Law Review Online, 71***(2).

Graeber, David (2011). ***Debt: The First 5.000 Years***. Brooklyn, N. Y.: Melville House.

Guarino, A. (1981). ***Diritto privato romano***. Sexta edición. Napoli.

Hart, Oliver (2016a). ***Incomplete Contracts and Control Prize Lecture***. [En línea]. Harvard University. Recuperado de: https://www.nobelprize.org/uploads/2018/06/hart-lecture.pdf. [Consultado el 27 de junio de 2019].

Hart, Oliver (2016b). ***Press release: The Prize in Economic Sciences.*** [En línea]. Recuperado de: https://www.nobelprize.org/prizes/economic-sciences/2016/press-release/. [Consultado el 27 de junio de 2019].

Hayek, F. A. (s.f.). ***La fatal arrogancia: los errores del socialismo***. Unión Editorial.

Hinestrosa, Fernando (1999). Autonomía Privada y Tipicidad Contractual. Conferencia pronunciada en el Seminario sobre el Contrato, Universidad Católica de Valparaíso, 24 a 26 de mayo de 1999.

Hinestrosa, Fernando (2013). Autonomía Privada y Tipicidad Contractual. ***In memoriam***. ***Revista de Derecho Privado*** (24), 3-13.

Horwitz, Morton J. (1974). The Historical Foundations of Modern Contract Law. ***Harvard Law Review, 87***(5), 917-956. The Harvard Law Review Association. https://www.jstor.org/stable/1340045.

IBM Blockchain 101 (s.f.). ***Quick-start guide for developers*** [En línea]. Recuperado de: https://developer.ibm.com/tutorials/cl-ibm-blockchain-101-quick-start-guide-for-developers-bluemix-trs/. [Consultado el de 27 de junio de 2019].

Kronman, Anthony (19878). Specific performance. ***Universidad de Chicago. Law Review, 45***(2), 351-382.

Nakamoto, Satoshi (2016). ***Bicoin: a peer to peer electronic cash system. 2016.*** [En línea]. Recuperado de: https://bitcoin.org/bitcoin.pdf. [Consultado el 27 de junio de 2019].

Norton, Rose Fulbright (2016). ***Can Smart Contracts Be Legally Binding Contracts.*** [En línea]. Recuperado de: http://www.nortonrosefulbright.com/ knowledge/publications/144559/can-smart-contracts-be-legally-binding-contracts. [Consultado el 27 de junio de 2019].

Posner, Richard A. y Rosenfield, Andrew M. (1977). Impossibility and related doctrines in contract law: An economic analysis. ***Journal of Legal Studies 6***(1), 83-118.

Raskin, Max (2017). The Law and Legality of Smart Contracts. ***1 Geo. L. Tech. Rev.*** 304, 309-22.

Rivest, R. L., Shamir, A. y Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. ***Communications of the ACM, 21***(2), 120-126. New York: ACM New York. Recuperado de: https://dl.acm.org/citation.cfm?id=359342. [Consultado el 27 de junio de 2019].

Schmidt, Klaus (2017). Contributions of Oliver Hart and Bengt Holmstrom to Contract Theory. ***M. J. of Economics, 119***(3), 489-511. Doi: 10.1111/sjoe.12245.

Scholz, L. (2017). Algorithmic Contracts. ***20 Stan. Tech. L. Rev., 128***.

Schwab, K. (2017). ***The Fourth Industrial Revolution***. Foro Económico Mundial.

Schwartz, Alan (1979). The case for specific performance. ***Yale Law Journal, 89***(2), 271-306.

Sec. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Securities Act Release N.º 81207 (July 25, 2017). [En línea]. Recuperado de: https://www.sec.gov/litigation/investreport/34-81207.pdf. [Consultado el 27 de junio de 2019].

Simpsont, A. W. B. (1979). The Horwitz Thesis and the History of Contracts. The University of Chicago Law Review Volumen, 46(3).

Sklaroff, Jeremy M. (2017). Comment, Smart Contracts and the Cost of Inflexibility. 166 U. Pa. L. Rev., 263, 286-291.

Sokol, Phyllis K. (1995). From EDI to Electronic Commerce: a business initiative. New York: McGraw-Hill.

Surden, Harry (2012). Computable Contracts. U.C. Davis L. Rev., 46, 629-656.

Surden, Harry (2014). Machine Learning and Law. 89 Wash. L. Rev., 89, 87-88.

Szabo, Nick (1995). Smart Contracts Glossary. [En línea]. Recuperado de: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_glossary.html. [Consultado el 27 de junio de 2019].

Szabo, Nick (1996). Introduction to Algorithmic Information Theory. [En línea]. Recuperado de: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/kolmogorov.html. [Consultado el 27 de junio de 2019].

Szabo, Nick (1998). Secure Property Titles with Owner Authority. [En línea]. Recuperado de: https://nakamotoinstitute.org/secure-property-titles/. [Consultado el 27 de junio de 2019].

Werbach, K. (2018). The Blockchain and the New Architecture of Trust. Mit Press.

Werbach, K. y Cornell N. (2017). Contracts Ex Machina. Duke L.J., 67, 313, 328-34.

Wormser, Maurice (1916). The True Conception of Unilateral Contracts. Yale L. J., 26, 136.

Yadav, Yesha (2015). How Algorithmic Trading Undermines Efficiency in Capital Markets. Vand. L. Rev., 68, 1607, 1612-14.

Yadav, Yesha (2016). The Failure of Liability in Modern Markets. Va. L. Rev., 102, 1031-1036.

DESAFÍOS EN LA NEGOCIACIÓN DE LA FACTURA ELECTRÓNICA DE VENTA EN COLOMBIA

Challenges in trading e-invoices in Colombia

David Díaz

Resumen

Este capítulo tiene como objeto presentar un panorama general de lo que ha sido el proceso de implementación de factura electrónica como título valor en Colombia. Para ello, parte del análisis del entorno normativo que ha sido determinando para tal fin, al tiempo que revisa los esfuerzos realizados por las distintas autoridades gubernamentales y el Legislador para definir el ecosistema de facturación electrónica, sus participantes y funcionamiento.
El escrito también propone soluciones basadas en tecnología que harían del registro de facturas electrónicas un sistema de control fiscal, con grandes alcances de orden mercantil.

Palabras clave: factura electrónica; título valor; negociación; desmaterialización; literalidad; autonomía; DIAN; registro.

Abstract

This chapter aims to introduce a general overview of the implementation of the e-invoice as trading security, in Colombia. It begins with the analysis of the regulatory framework adopted to that end, as well as it considers the efforts put by the public authorities and legislators to shape the e-invoice ecosystem, its stakeholders and functionalities.
This paper also includes some technology-based propositions, that could make the public registry of e-invoices, a taxation control system with further mercantile implications.

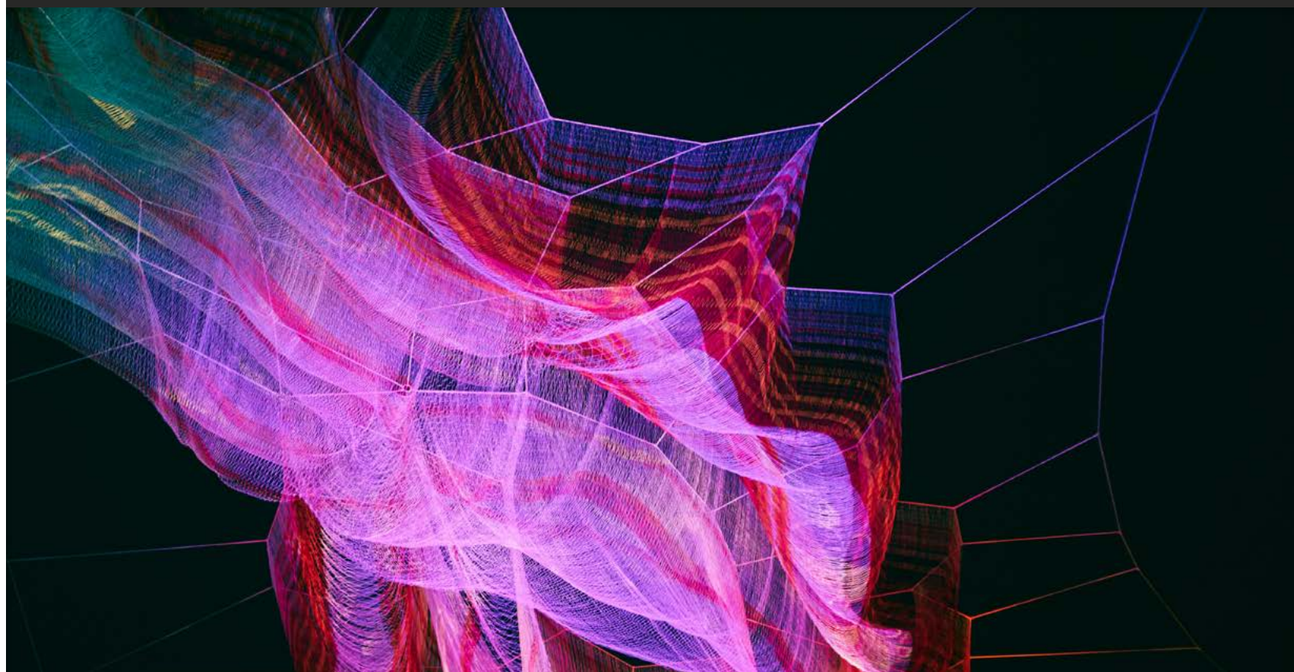
Key words: e-invoice; trading security; trading; dematerialization; literalness; autonomy; DIAN; registry.

Introducción

La estructuración del ecosistema para la negociación de la factura electrónica de venta (título valor) no ha sido una tarea fácil. El proceso de reglamentación de su operatividad, así como de los distintos actores involucrados, ha sufrido por la falta de voluntad política por parte de los Gobiernos que han ocupado el poder desde el año 2008, así como de la incomprensión de los alcances de dicho título valor y de lo que representa en términos de crecimiento empresarial para Colombia.

El presente capítulo, como bien lo sugiere su título, revisará el camino que han recorrido tanto el Legislador como las autoridades del sector central involucradas, así como los retos que se advierte tendrán que enfrentar y superar las entidades llamadas a liderar la puesta en funcionamiento del mecanismo electrónico para la negociación de la factura electrónica de venta.

En primer lugar, abordaremos brevemente los antecedentes legislativos que determinaron la existencia de la factura electrónica; en seguida, revisaremos a la luz de la Ley 527 de 1999 los requisitos para que una factura electrónica sea considerada título valor y, por último, bajo el contexto normativo vigente serán analizados los retos a los que se enfrentará la DIAN como el administrador del repositorio de facturas electrónicas.



01

¿Qué es la factura electrónica de venta?

Para responder esta pregunta hay que entender que la factura electrónica de venta tiene dos vertientes normativas que la configuran. Al igual que en la factura física, existe un conjunto normativo tributario que le da origen y un contexto regulatorio comercial que le otorga su calidad de título valor.

A efectos ilustrativos, la factura electrónica es un archivo de datos cuyo contenido es producido, transmitido y resguardado usando herramientas informáticas que comprenden tanto hardware como software. Este archivo existe únicamente en medios electrónicos, siendo un documento desmaterializado que cumple, en todas las situaciones y para todos los efectos, con el mismo objetivo que tiene una factura de papel.

Su finalidad desde el punto de vista tributario consiste en registrar las operaciones comerciales de un comerciante de forma electrónica, observando los principios establecidos en la Ley 527 de 1999 (***v.gr.***, autenticidad, integridad, disponibilidad y no repudio, equivalencia funcional, etc.), a través de la fijación de un estándar para la generación y custodia del archivo.

Para el caso de la factura electrónica en Colombia, la DIAN ha establecido que se trata de un archivo ***Extensible Markup Language*** (XML, por sus siglas en inglés), que consiste en ***"[…] un archivo de texto especial compuesto por un determinado número de etiquetas en estructura de árbol"*** (Boulanger, 2015, p. 21). Este permite disociar los datos de su presentación, convirtiéndose en una alternativa eficaz respecto del lenguaje de codificación HTML, pues sirve también para entornos más complejos como el que representan el comercio electrónico, las transacciones, la mensajería digital, entre otros (Boulanger, 2015).

Además, dicho archivo se caracteriza porque no existen diferencias entre originales o copias, ya que son idénticas, por lo cual se requiere garantizar su trazabilidad y custodia para prevenir fraudes. Otro rasgo distintivo de esta clase de archivos está dado por la autoridad tributaria, pues esta ha definido previamente un conjunto de reglas y procesos que permiten verificar que la estructura de datos XML documenta adecuada y suficientemente una transacción.

De esta manera, la factura electrónica, de acuerdo con el estándar establecido, deberá incorporar todos los requisitos consignados en el Estatuto Tributario[196] a efectos de cumplir con las obligaciones de reporte fiscal a cargo de los comerciantes. Por su parte, en lo que concierne a los requisitos mercantiles de la factura electrónica, esta deberá observar todos y cada uno de los requerimientos establecidos en el Código de Comercio a partir del artículo 772 y siguientes para que sea título valor.

196. Artículos 616-1, 511, 615, 617, 618, 684-2 del Estatuto Tributario, en el Decreto 2242 de 2015, recopilado en el 1625 de 2016.

02

Antecedentes legislativos

La factura electrónica de venta es el primer título valor desmaterializado expresamente reglamentado por el Legislador colombiano. Su historia se remonta a la Ley 223 de 1995, en el marco de la cual una breve mención fue incorporada al adicionar el artículo 616-1 al Estatuto Tributario. Posteriormente, el artículo 26 de la Ley 962 de 2005 estableció que la expedición, aceptación y archivo de las facturas podría hacerse por vía electrónica, siempre y cuando la tecnología que fuera implementada para tales fines cumpliera con todos los requisitos legales aplicables y garantizara la autenticidad e integridad. Esto aplica desde su expedición y durante el término de su conservación, en línea con los principios establecidos en la Ley 527 de 1999.

Posteriormente, la Ley 1231 de 2008, ***"Por la cual se unifica la factura como título valor como mecanismo de financiación para el micro, pequeño y mediano empresario*** […]", incorporó en el parágrafo de su artículo 1 la obligación de reglamentar la puesta en circulación de la factura electrónica como título valor a cargo del Gobierno Nacional.

Más allá de la mención a la factura electrónica, resaltamos los efectos comerciales de la Ley 1231 de 2008 en el empresariado nacional, especialmente en la base empresarial, pues su propósito principal fue el de revestir a las facturas comerciales de las características de los títulos valores (***v.gr.***, autonomía, legitimación, incorporación, literalidad y carácter documentario), a efectos de convertirlas en una herramienta para acceso a capital de trabajo por parte de los micro, pequeños y medianos empresarios colombianos[197] (mipymes). Estas propiedades son predicables también de las facturas electrónicas. Las facturas comerciales, después de la expedición de la Ley 1231 de 2008, serían denominadas "facturas de venta", cambio que revisaremos a fondo más adelante dado que es uno de los requisitos normativos para que una factura, tanto física como electrónica, tenga las calidades de título valor.

Así las cosas, la referida norma entregó a los empresarios nacionales tres herramientas; la primera es atinente a facultar a los comerciantes (emisor) para librar títulos valores (factura de venta) en el marco de sus relaciones comerciales, los cuales son aceptados por el librado (pagador) para que puedan ser negociados sin restricción alguna[198] siguiendo su ley de circulación; la segunda está relacionada con la documentación de las transacciones comerciales en un título valor que facilitaría la ejecución judicial del crédito que en dichos documentos se incorpora; y la tercera persigue la masificación de las operaciones de emisión y negociación de facturas de venta de manera rápida, a través de la expedición y transmisión de la propiedad sobre facturas electrónicas.

De lo anterior dan cuenta las consideraciones expuestas por el Congreso de la República en el marco de las discusiones del Proyecto de Ley 151 de 2007 que derivaron

197. De esto da cuenta la Gaceta del Congreso N.° 477 de 2007, en la que consta el trámite del Proyecto de Ley N.o 151 de 2007, que posteriormente se convertiría en la Ley 1231 de 2008.

198. De acuerdo con el artículo 779 del Código de Comercio, se aplicarán a las facturas de venta las normas relativas a la letra de cambio.

en la promulgación de la Ley 1231 de 2008, dentro de las cuales quedó consignado el espíritu que el Legislador quiso imprimir a la regulación de la factura de venta:

[…] La teoría de los títulos valores aplicable en el país ha seguido inmodificable en los términos establecidos en 1971, y en esa lista taxativa de títulos valores se echan de menos las facturas comerciales, pese a que estas han sido tradicionalmente los instrumentos legales de soporte de transacciones de bienes y de servicios y que su expedición es una obligación clara para todos los comerciantes. Se exceptúan únicamente las facturas cambiarias de compraventa de mercancías y de transporte, respecto de las cuales el Código de Comercio exige unos requisitos especiales, que resultan adicionales a los exigidos por la norma general de facturas para efectos tributarios.

Así, pese a que las facturas comerciales son el instrumento generalizado de comprobación y soporte de las actividades comerciales convenidas y de las formas de pago de las mismas, no tienen la naturaleza de títulos valores a pesar de tener un contenido crediticio y, por tanto, no gozan de las ventajas de estos, entre otras, de servir de título ejecutivo para su cobro. […]

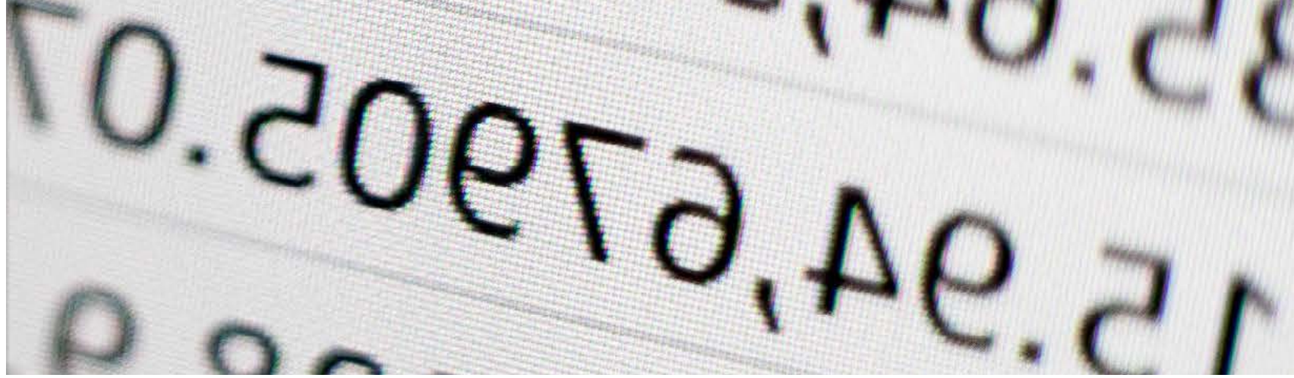
[…] Si bien entre nosotros existe, al lado de los títulos valores, la institución de la cesión de créditos, esta no es apropiada para la clase de negocios y la rapidez que el mundo de hoy exige respecto de las transacciones comerciales. Dados los formalismos con que la ley ha revestido esta figura, tampoco resulta apropiada para negociar facturas, una operación que se debe caracterizar por la rapidez y la seguridad en las transacciones. En efecto, uno de los trámites que hacen nugatoria la cesión es el consignado en el artículo 1960 del Código Civil, según el cual "La cesión no produce efecto contra el deudor ni contra terceros, mientras no ha sido notificada por el cesionario al deudor o aceptada por este". De ahí la necesidad de acudir a otras instituciones jurídicas que brinden mayor seguridad y rapidez en la circulación de los créditos.

En este sentido, la Doctrina ha dicho que la disciplina de los títulos de crédito está precedida de una idea conductora: superar las reglas que dirigen la circulación de los créditos según el instituto de la cesión, elevando la función del documento (título) del crédito a vehículo de su circulación.

Se propone, entonces, que las facturas sean títulos de contenido crediticio, enmarcándose así en la teoría general de los títulos valores, y cuyas características generales están contenidas en la definición que de los mismos consigna el artículo 619 del Código de Comercio, así: "Son documentos necesarios para legitimar el ejercicio del derecho literal y autónomo que en ellos se incorpora"[199].

Vale la pena mencionar que en el marco de las operaciones mercantiles, dentro de las cuales son expedidas las facturas de venta, es costumbre que el pagador cuente con holgadas condiciones para el pago. Estas pueden ir así desde 30 hasta 180 días calendario e incluso más tiempo. Esto impacta de manera negativa la caja de las empresas prestadoras de servicios o vendedoras de bienes (proveedores), pues solamente percibirán la contraprestación una vez vencidos los términos anteriormente anotados, lo que ocasiona que el proveedor tenga que contemplar mecanismos

199. Gaceta del Congreso de la República N.° 477 de 2007, publicada el 27 de septiembre de 2007.



que le permitan un pronto acceso al capital que se encuentra atrapado dentro de unas condiciones de pago prestablecidas.

Para superar dichas dificultades, el Legislador analizó las limitaciones inherentes a la inexistencia de una factura como título valor, pues el acceso a capital de trabajo por parte de las mipymes era cada vez más difícil dado que lo usual en esa época era estructurar el acceso a recursos líquidos mediante la cesión de derechos económicos, figura plagada de lentitud y formalismo. Originalmente, esta fue creada con un carácter principalmente civil, más que comercial, en el marco de la cual las mipymes no controlan la negociación de sus cuentas por cobrar, pues en este caso el pagador de las operaciones puede optar por no otorgar las garantías propias (pagarés en blanco con carta de instrucciones) de este tipo de operaciones que le den al adquirente de dichos derechos económicos la tranquilidad para cobrar judicialmente sus acreencias.

Igualmente, el Legislador buscó superar las trabas propias de los mecanismos tradicionales para acceder a recursos líquidos tales como el crédito, pues estos tampoco eran —ni son hoy en día— los idóneos para mipymes. Tal inconveniencia se debe a que el análisis de riesgo de las entidades financieras incumbentes inicia por estudiar los estados financieros de micro, pequeños y medianos comerciantes que pueden tener un gran flujo de recursos durante el ejercicio, pero que al cierre del año fiscal no se reflejan en sus balances de manera positiva dadas las formas de pago anteriormente anotadas, o por otra parte pueden solicitar garantías que las mipymes, por su tamaño, no pueden otorgar.

Así las cosas, el Congreso de la República, con la expedición de la Ley 1231 de 2008, tuvo como objetivo dar seguridad y eficiencia en la circulación de las facturas como título valor, pues consideró el auge que a nivel internacional había tomado el contrato por el cual se regulan algunas operaciones de compra de cartera al descuento conocido como ***factoring***. Para el caso de Colombia, este encontraba dificultades en su crecimiento e implementación dado que el marco regulatorio no prescribía la factura como título valor.

Aunque la Ley 1231 de 2008 ha sido reglamentada varias veces desde su expedición[200] para asuntos que distan de la factura electrónica, fue solamente hasta la entrada en vigencia de la Ley 1753 de 2015 que le fueron conferidas facultades reglamentarias al Ministerio de Comercio Industria y Turismo

200. Decreto 2669 de 2012, Decreto 2242 de 2015 y Decreto 1349 de 2016.

(MinCIT) para que profiriera el marco normativo aplicable al entonces denominado Registro de Facturas Electrónicas (Refel)[201]. Este repositorio serviría para permitir la negociabilidad de las facturas electrónicas consideradas como título valor.

Desde el punto de vista tributario, como ya lo mencionamos, fue la Ley 223 de 1995 la que en primer lugar contempló la posibilidad de implementar la factura electrónica, en ese tiempo como documento equivalente. Sin embargo, fue con la expedición del Decreto 2242 de 2015, que hace parte del Decreto Único Reglamentario en materia tributaria (Decreto 1625 de 2016), que se definieron las condiciones de expedición e interoperabilidad de la factura electrónica con fines de masificación y control fiscal.

Las normas sobre facturación electrónica deben ser observadas por personas naturales y jurídicas que de acuerdo con el Estatuto Tributario tienen la obligación de facturar y: (i) sean seleccionadas por la DIAN para tal efecto, o (ii) tengan la obligación de facturar y decidan voluntariamente expedir factura electrónica, o (iii) no están obligadas a facturar y opten por expedir dicho tipo de factura.

De acuerdo con lo establecido en el numeral primero del artículo 1.6.1.4.1.2. del Decreto 1625 de 2016, la factura electrónica es el soporte de negocios jurídicos tales como operaciones de venta de bienes y/o prestación de servicios. Para efectos fiscales, esta queda consignada en sistemas computacionales y/o soluciones informáticas que cumplen con los requisitos de expedición, recibo, aceptación, rechazo y conservación establecidos en el mencionado decreto, que en observancia de los principios establecidos en la Ley 527 de 1999 garantizan su autenticidad, integridad y disponibilidad desde el tiempo de su expedición y durante todo el término de conservación.

A partir del Decreto 2242 de 2015 quedaron establecidas las características de orden técnico y tecnológico que deberían observar tanto los emisores como los proveedores tecnológicos que tienen a su cargo suministrar el software necesario para la emisión, remisión, aceptación y conexión al repositorio de facturas electrónicas. En cuanto al modelo de facturación electrónica que está en proceso de implementación en Colombia, la DIAN ha observado de cerca el modelo chileno, pues su estructura es de orden sincrónico[202], lo cual permite la emisión de la factura electrónica y su posterior remisión en tiempo real a la autoridad tributaria.

En este punto consideramos pertinente precisar cuáles son los actuales integrantes del ecosistema de facturación electrónica, pues la normativa tributaria ha definido los más importantes a estos efectos. Para describir los actores, empezaremos por orden de participación en la cadena de emisión de facturas electrónicas:

Emisor:

es la persona natural o jurídica obligada, de acuerdo con el Estatuto Tributario y los actos administrativos de la DIAN, a emitir factura electrónica por la venta de bienes y/o prestación de servicios. El emisor deberá contratar a un proveedor tecnológico, usar la solución tecnológica gratuita que proveerá la DIAN para emitir facturas electrónicas o implementar su software propio[203].

Proveedores tecnológicos:

regulados por la DIAN mediante Resolución 019 de 2016, tendrán un papel fundamental pues serán las entidades privadas de orden técnico que median en el proceso de creación de la factura electrónica. Prestan el servicio de emisión de facturas al emisor, además de la directa conectividad a la DIAN para remitir toda la información necesaria sobre las facturas electrónicas.

Dentro de las variadas funciones que deberán desempeñar destacan las siguientes: (i) velar por el cumplimiento de los requisitos normativos establecidos para las facturas de venta, tanto en materia tributaria como mercantil; (ii) garantizar la autenticidad, integridad y disponibilidad de las facturas electrónicas; (iii) conectarse al repositorio de facturas electrónicas, que administrará la DIAN, para permitir su negociación.

Estas empresas cobrarán una tarifa por la expedición de las facturas electrónicas. Sin embargo para las mipymes, al igual que en Chile, existirá un sistema de facturación gratuito que suministrará la DIAN para que factores como el costo o la implementación técnica de un mecanismo de facturación electrónica no sean una limitante a la hora de expedirlas.

DIAN:

para el caso del ecosistema de generación de facturas electrónicas, la autoridad en materia fiscal fungirá como el ente receptor y centralizador de información, principalmente de orden tributario. Esta también conocerá de primera mano la información generada en el marco de los hábitos comerciales de los emisores con sus pagadores (aceptantes). Además, la DIAN desempeñará tres funciones claves que van más allá de su labor de fiscalización: (i) validar las facturas electrónicas de venta, lo cual será un requisito de forma para que estas sean consideradas como título valor; (ii) administrar el registro de facturas electrónicas que detenten la calidad de título valor, asegurando su funcionalidad y operatividad; y (iii) llevar la trazabilidad de la negociación de las facturas electrónicas como título valor, permitiendo su endoso (en propiedad, en procuración, en garantía, con responsabilidad, sin responsabilidad, etc.)[204].

201. Artículo 9 de la Ley 1753 de 2015: *"Registro de Facturas Electrónicas. Créase el Registro de Facturas Electrónicas, el cual será administrado por el Ministerio de Comercio, Industria y Turismo. Este registro incluirá las facturas electrónicas que sean consideradas como título valor que circulen en el territorio nacional y permitirá la consulta de información de las mismas. Igualmente permitirá hacer la trazabilidad de dichas facturas electrónicas, bajo los estándares necesarios para el control del lavado de activos y garantizará el cumplimiento de los principios de unicidad, autenticidad, integridad y no repudio de la factura electrónica. El Gobierno nacional reglamentará la puesta en funcionamiento del registro único. Parágrafo 1°. El Ministerio de Comercio, Industria y Turismo podrá contratar con terceros la administración de este registro. El Ministerio de Comercio, Industria y Turismo mediante resolución establecerá las condiciones y requisitos que deberá cumplir el contratista. Parágrafo 2°. Los costos de administración de este registro se financiarán con una contraprestación a favor del administrador y a cargo de quien consulte la información, de quien solicite el registro de la transferencia, y de quien solicite la expedición de certificados sobre la existencia del título y su titularidad para efectos de la ejecución de las facturas electrónicas, entre otros, que será determinada por el Ministerio de Comercio, Industria y Turismo, tomando como referencia los costos de administración e inversión necesarios para la puesta en operación, mantenimiento y continuidad del servicio. El monto de esta contraprestación será actualizado anualmente".*

202. Ley 1819 del 2016.

203. En este caso el software debe ser habilitado por la DIAN.

204. Parágrafo 5 del artículo 616-1 del Estatuto Tributario: *"La plataforma de factura electrónica de la Dirección de Impuestos y Aduanas Nacionales-DIAN incluirá el registro de las facturas electrónicas consideradas como título valor que circulen en el territorio nacional y permitirá su consulta y trazabilidad. Las entidades autorizadas para realizar actividades de factoraje tendrán que desarrollar y adaptar sus sistemas tecnológicos a aquellos de la Dirección de Impuestos y Aduanas Nacionales-DIAN. El Gobierno Nacional reglamentará la circulación de las facturas electrónicas".*

Sistemas de negociación o intermediario:

los sistemas de negociación o intermediarios serán aquellas entidades, con carácter mercantil o financiero, que estarán llamadas a darle liquidez al ecosistema de facturas electrónicas permitiéndoles a las empresas acceder a capital de trabajo mediante la venta de sus facturas electrónicas, que para todos los efectos son activos que hacen parte de su patrimonio. Estas entidades funcionan hoy como proveedores de servicios de *factoring* o *confirming*.

Su labor será netamente comercial, pues deberán aproximarse a los emisores para que, en el marco de la libre competencia, puedan ofrecer las mejores tasas a los facturadores contra la adquisición al descuento de sus facturas. Sin embargo, el factor diferenciador de estos sistemas no solo estará representado en el costo de financiación que ofrezcan, pues su valor agregado deberá enfocarse en los productos conexos que, dentro de sus capacidades, puedan poner al servicio de los facturadores electrónicos (*v.gr.*, soluciones a problemas operativos, disminución de error humano, automatización vía API, velocidad en la transacción y en el desembolso de recursos, cobertura en zonas con acceso limitado a internet, etc.).

Con las anteriores referencias culminamos una vista general a la regulación del sistema de facturación electrónica y su conformación operativa en Colombia. En los acápites subsiguientes revisaremos con mayor precisión las características que tenía el Refel, su funcionalidad, la razón por la cual hoy en día no existe y su sustitución por el registro de facturas que administrará la DIAN.

03

La factura electrónica como título valor y la Ley 527 de 1999

Inicialmente, la factura de venta deberá cumplir con los requisitos generales establecidos para la existencia de cualquier título valor. Estos son los consignados en el artículo 621 del Código de Comercio, los cuales corresponden a: (i) la mención del derecho que en el título se incorpora y (ii) la firma de quien lo crea.

En cuanto a los requisitos específicos, el artículo 772 y siguientes del Código de Comercio señalan un conjunto de características que deben cumplirse de manera integral para que las facturas de venta sean consideradas como título valor. Dentro de ellas encontramos la denominación expresa de *"factura de venta"*, rasgo al que se le suman aquellos incluidos en el artículo 617 del Estatuto Tributario. Bajo dicho contexto regulatorio, esos mismos requisitos deberán ser cumplidos por la factura electrónica para que cuente con la calidad de título valor.

Al respecto, la Superintendencia de Sociedades, mediante Oficio 220-010483 del 22 de febrero de 2019, analizó los siguientes requisitos especiales, consignados en el Código de Comercio, frente a las disposiciones establecidas en el Decreto 1349 de 2015:

a. Fecha de vencimiento: las facturas electrónicas, de acuerdo con el numeral 3 del artículo 2.2.2.53.12 del Decreto 1349 de 2016, indicarán el valor y la fecha de vencimiento o de pago de la factura electrónica de venta, dejando así constancia de que se trata de un documento que incorpora un derecho de carácter crediticio sujeto a un plazo determinado.

b. Fecha de recibo de la factura: el artículo 2.2.2.53.5 del precitado decreto establece que *"El emisor entregará o pondrá a disposición del adquirente/pagador la factura electrónica en el formato electrónico de generación, de conformidad con lo dispuesto en el artículo 3º del Decreto 2242 de 2015"*. Sin duda, la reglamentación con la que hoy cuenta la factura electrónica incorpora un mecanismo para que pueda quedar constancia de que la factura fue recibida en debida forma por parte del girado.

c. En el caso de la factura electrónica, la DIAN prevé que el acuse de recibo de la factura sea surtido una vez dicha autoridad haya validado la factura, para lo cual operará: (i) la emisión y transmisión de la factura del vendedor a la DIAN; (ii) la validación de la factura por la DIAN; y (iii) la entrega al adquirente, momento a partir del cual empezarán a correr los tres días hábiles establecidos en el artículo 773 del Código de Comercio a efectos de que la factura sea aceptada tácitamente.

d. El emisor, vendedor o prestador del servicio deberá dejar constancia en el original de la factura del estado de pago del precio: esta característica se cumple con una conjunción de los artículos 2.2.2.53.1, 2.2.2.53.2, 2.2.2.53.10, 2.2.2.53.11 y 2.2.2.53.12, dentro de los cuales se instrumentalizó el registro al que serán llevadas por el emisor las facturas electrónicas. En este sistema serán consignados todos los eventos ocurridos con dichos títulos valores, tales como su pago parcial o total, su transferencia de propiedad a través del endoso electrónico, las instrucciones de pago al legítimo tenedor (que deberán ser consultadas por el pagador en el registro de facturas al vencimiento de este), y finalmente permitirá expedir los certificados de información y los títulos que permitan el cobro judicial de las facturas electrónicas, que contendrá el estado de pago de la respectiva factura.

a. Aceptación de la factura: esta es desarrollada por el artículo 2.2.2.53.5, en el marco del cual se habilita la aceptación expresa por medios electrónicos, emitida por el adquirente del bien o beneficiario del servicio. La aceptación tácita operará con sujeción a los criterios establecidos en el Código de Comercio; sin embargo, las facturas que surtan este proceso serán incorporadas al registro con una manifestación del emisor, realizada bajo la gravedad de juramento, en la cual dejarán constancia de que la factura fue aceptada tácitamente.

En caso de que el adquirente/pagador no tenga la capacidad de recibir factura electrónica y por tanto no pueda aceptarla expresa o tácitamente de forma electrónica, esta no podrá circular como título valor, mientras que su representación gráfica carece de cualquier valor para su negociación.

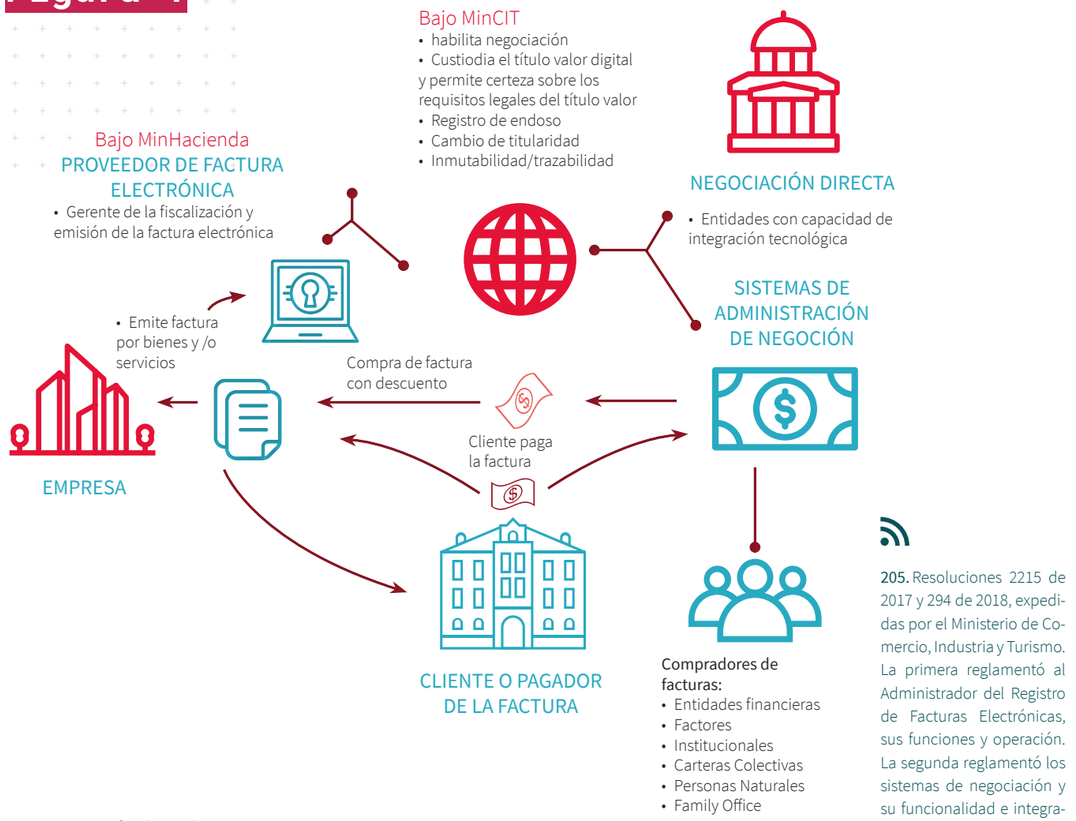
04

La factura electrónica de venta y su negociación

4.1. El Registro Electrónico de Factura Electrónica (Refel)

El Refel estaba sujeto a una extensa regulación expedida por el MinCIT[205], dentro de la cual se contaban resoluciones por las cuales fueron establecidos los criterios operativos y tecnológicos de los terceros que harían parte del ecosistema de negociación de facturación electrónica como título valor. El sistema, de acuerdo con la concepción del precitado Ministerio, estaba conformado por actores e integraciones reflejados en la figura 1.

Figura 1



Fuente: Mesfix (2018).

205. Resoluciones 2215 de 2017 y 294 de 2018, expedidas por el Ministerio de Comercio, Industria y Turismo. La primera reglamentó al Administrador del Registro de Facturas Electrónicas, sus funciones y operación. La segunda reglamentó los sistemas de negociación y su funcionalidad e integración con el Refel.

No obstante, y en un giro inesperado, el Legislador colombiano sustrajo la competencia del MinCIT para administrar el Refel mediante el parágrafo 5 del artículo 16 de la Ley 1943 de 2018, cuyo tenor literal reza:

La plataforma de factura electrónica de la Dirección de Impuestos y Aduanas Nacionales (DIAN) incluirá el registro de las facturas electrónicas consideradas como título valor que circulen en el territorio nacional y permitirá su consulta y trazabilidad. Las entidades autorizadas para realizar actividades de factoraje tendrán que desarrollar y adaptar sus sistemas tecnológicos a aquellos de la Dirección de Impuestos y Aduanas Nacionales (DIAN). El Gobierno nacional reglamentará la circulación de las facturas electrónicas.

Dicha ley, también conocida como "Ley de Financiamiento", derogó expresamente el artículo 9 de la Ley 1753 de 2015, en el cual constaba el mandato legal que tenía el MinCIT.

De esto se intuye que la falta de gestión por parte de tal Ministerio, quien por más de tres años estuvo a la cabeza de poner en marca el Refel, pudo haber motivado esta decisión del Congreso de la República, sumada a la voluntad del Gobierno Nacional en dicho sentido, dado el fallido intento de licitación pública N.º 01 de 2018 que puso en marcha el MinCIT a inicios del año 2018.

Podría calificarse como afortunada la transición del MinCIT a la DIAN si se consideran los siguientes problemas que tenía el Refel en sus prepliegos de licitación:

a. Se trataba de un esquema centralizado, adjudicado por concesión a un privado, quien tendría que incurrir con la implementación tecnológica del Refel, contra la recepción de una remuneración. Un esquema como este era llamativo ya que, a pesar de los retos que imponía la implementación del registro, estos no serían asumidos por la entidad pública. Sin embargo, este no limitaba que intereses privados fijaran los criterios de acceso a capital de trabajo para los empresarios nacionales.

b. El Registro Único de Proponentes (RUP) solicitaba que los participantes contaran con la capacidad de prestar servicios financieros y servicios basados en tecnologías de la información, de lo cual se advertía que solamente algunos proponentes colombianos cumplían con los segmentos económicos buscados en la licitación.

c. Se hacía referencia a *"[…] las mejores prácticas y las más recientes tecnologías aplicables"*; sin embargo, en los estudios previos no fue considerada la infraestructura propuesta para que el registro estuviera basado en tecnología ***blockchain***, la cual cumpliría con todos los requisitos de oportunidad, seguridad, eficacia y eficiencia.

d. No fue considerado que el valor de las transacciones y los costos generados a cada uno de los intervinientes podrían ser cercanos a cero si se daba la implementación de ***blockchain*** en la administración del Refel. Un Refel basado en tal tecnología resultaría en un sistema más costo-eficiente, de mayor y mejor acceso para los emisores de facturas electrónicas que quisieran negociar dichos títulos valores.

e. En este mismo sentido, el Refel se hacía prohibitivo si las tarifas no comprendían la necesidad de un acceso generalizado, pues solo aquellos que pudieran pagar la inscripción anual que estaba prevista estarían facultados para ingresar al registro, ya sea como emisores, sistemas de negociación, tenedores legítimos, etc. Esto se habría convertido en un desincentivo para la implementación del ***factoring*** como mecanismo de acceso a capital de trabajo de las mipymes, yendo en contravía de los preceptos establecidos en la Ley 1231 de 2008 y demás que han regulado el ***factoring*** como mecanismo de formalización de empresa.

f. La visión que se tenía del Refel en los pliegos era de mediano plazo, pues el sistema que proponía implementar el MinCIT estaba basado en una estructura centralizada que al cabo de cinco años iba a ser obsoleta. Esto dejaba en entredicho la aplicación de principios de la contratación, tales como el de planeación, pues hubiera podido afirmarse en ese entonces que existían mejores formas de poner en marcha dicho proyecto, haciendo de este un sistema a prueba de obsolescencia tecnológica en el corto y mediano plazo.

g. No comprendía una visión de política de datos abiertos, en el marco de la cual se les permitiera a los usuarios administrar la información que sobre ellos se recopilara en cualquier base de datos.

h. No establecía de manera adecuada un plan de continuidad en caso de toma del registro por parte del Gobierno Nacional. En consecuencia, no se garantizaba la operación del sistema durante un periodo de interinidad.

i. No contemplaba la coexistencia de múltiples endosatarios que al mismo tiempo pudieran adquirir la(s) facturas(s) en una operación de compraventa.

j. El literal A del ordinal IV del Anexo Técnico, atinente a seguridad, establecía que la plataforma debía incluir mecanismos y herramientas de protección frente a ataques electrónicos como ***hacking***, denegación del servicio o introducción de software malicioso. Todo lo anterior se podía cumplir implementando el sistema basado en ***blockchain***.

Las anteriores eran solo algunas de las dificultades que presentaba la estructura operativa del Refel. Sin embargo, estas fueron conjuradas en el momento en el que la licitación fue suspendida indefinidamente, después de tres meses de revisión por parte del MinCIT y un sinnúmero de comentarios que pusieron en evidencia las debilidades del proyecto.

Es de notar que el Refel, ahora en manos de la DIAN, será simplemente un repositorio de facturas electrónicas que administrará directamente la autoridad tributaria en el marco de sus capacidades legales y reglamentarias, lo cual supone otros retos a la hora de implementar las normas atinentes a la negociación de dichos títulos valores.

4.2. Efectos de no contar con regulación del Refel

Como indicamos en el anterior acápite, la Ley de Financiamiento derogó expresamente el artículo que facultaba al MinCIT para administrar el Refel, transfiriendo dicha tarea a la DIAN. No obstante, existen algunas dificultades que se desprenden de este hecho, relacionadas principalmente con los actos administrativos expedidos por el MinCIT que sirvieron para regular tanto al Refel como a los sistemas de negociación.
En este punto cabe preguntarse:

a. Sobre los decretos y resoluciones expedidos en el marco de la capacidad legal que ostentaba el MinCIT, ¿opera el fenómeno del decaimiento de los actos administrativos[206] por el desaparecimiento del fundamento legal del ordenamiento jurídico? Una aproximación muy rápida a esta pregunta nos permite intuir que sí. Sin embargo, esta discusión amerita un análisis extenso para conocer los efectos de dicho fenómeno frente al actual esquema que tendrá la negociación de facturas electrónicas en nuestro país.

b. ¿Estará llamada la DIAN a emitir actos administrativos para regular los sistemas de negociación? De ser esto así, estaría excediendo sus facultades legales y reglamentarias.

c. ¿Generó la Ley de Financiamiento un vacío en la normativa colombiana de factura electrónica en relación con su negociación? De ser afirmativa la respuesta, implicaría que los sistemas de negociación y/o intermediarios no tendrían la reglamentación para tomar parte en la negociación de dichos títulos valores, lo cual limitaría el desarrollo de un mercado de facturas electrónicas que tenga la suficiente profundidad como para generar un impacto positivo en la base empresarial colombiana.

Además, si el ecosistema no cuenta desde su inicio con los mecanismos de fondeo, podría retrasar la implementación de la factura electrónica como mecanismo de control fiscal, dado el daño económico que podría causársele a los facturadores electrónicos por no poder acceder a fuentes alternativas de capital de trabajo que no impacten su capacidad de endeudamiento.

4.3. Transferencia de competencia en la administración del registro a la DIAN

En lo que atañe a las facultades de la DIAN frente a la implementación del repositorio de facturas electrónicas con fines de negociación, llama la atención que el Legislador haya delegado esa tarea a una unidad administrativa especial como la DIAN, cuyo propósito principal es servirle al Ministerio de Hacienda y Crédito Público como órgano técnico y especializado en

la administración de los impuestos de renta y complementarios, de timbre nacional y sobre las ventas; los derechos de aduana y los demás impuestos internos del orden nacional cuya competencia no esté asignada a otras entidades del Estado, bien se trate de impuestos internos o al comercio exterior; así como la dirección y administración de la gestión aduanera, incluyendo la aprehensión, decomiso o declaración en abandono a favor de la Nación de mercancías y su administración y disposición[207].

En este contexto, inquieta que las mismas limitaciones reglamentarias de la DIAN se conviertan en una barrera para que las facturas electrónicas no puedan contar con todos los criterios que hacen de ellas un título valor (su carácter negociable y su libre circulación) y un activo de las empresas. Esta preocupación cobra más fuerza una vez verificados los decretos reglamentarios que delimitan las funciones de la DIAN[208], pues dentro de dicho cuerpo normativo no hay evidencia de que ese organismo pueda realizar actividades de administración del mencionado registro, cuya funcionalidad, en gran parte, es de orden mercantil, onerosa y transaccional, lo cual está desligado de una finalidad de vigilancia fiscal y/o de recaudo tributario.

En esta medida, la Ley de Financiamiento desconoció la naturaleza de la DIAN al asignarle funciones que exceden las previstas en su ley de funcionamiento tales como: (i) custodiar títulos valores (facturas electrónicas); (ii) registrar la negociación de dichos títulos valores a través de endosos electrónicos; y (iii) llevar la trazabilidad de pagos y demás actividades relacionadas, sobre las cuales es claro que la DIAN no tiene experiencia de orden técnico y/o administrativo.

206. Ley 1437 de 2011. Código de Procedimiento Administrativo y de lo Contencioso Administrativo:

"Artículo 91. *Pérdida de ejecutoriedad del acto administrativo. Salvo norma expresa en contrario, los actos administrativos en firme serán obligatorios mientras no hayan sido anulados por la Jurisdicción de lo Contencioso Administrativo. Perderán obligatoriedad y, por lo tanto, no podrán ser ejecutados en los siguientes casos:*

1. Cuando sean suspendidos provisionalmente sus efectos por la Jurisdicción de lo Contencioso Administrativo.

2. Cuando desaparezcan sus fundamentos de hecho o de derecho.

3. Cuando al cabo de cinco (5) años de estar en firme, la autoridad no ha realizado los actos que le correspondan para ejecutarlos.

4. Cuando se cumpla la condición resolutoria a que se encuentre sometido el acto.

5. Cuando pierdan vigencia" [negrilla fuera del texto].

207. Artículo 1 del Decreto 1292 de 2015.

208. Decreto 1071 de 26 de junio de 1999, Decreto 3626 de 10 de octubre de 2005, Decreto 4048 del 22 de octubre de 2008, Decreto 1321 del 26 de abril de 2011 y Decreto 1292 del 17 de julio de 2015

4.4. Negociación de facturas electrónicas de venta desde la DIAN

De acuerdo con la legislación vigente, a continuación presentaremos el esquema que intuimos implementará la DIAN para permitir la negociación de facturas electrónicas que cuenten con los requisitos legales para ser título valor.

4.4.1. El repositorio o depósito

Se tratará de un registro centralizado, administrado directamente por la DIAN. Solo en este aspecto ya dista bastante del modelo que pretendía implementar el MinCIT, pues no mediará concesión alguna para su puesta en funcionamiento. El depósito se encargará de:

a. Permitir la conexión de aquellos proveedores tecnológicos que han sido autorizados antes por la DIAN para operar, quienes luego se vincularán contractualmente con los emisores (comerciantes). Los comerciantes que no puedan contratar a un proveedor tecnológico podrán usar el software gratuito de facturación electrónica que entregará la DIAN a los emisores que lo requieran.

b. Llevar el control sobre la emisión de facturas electrónicas de acuerdo con las resoluciones de autorización que expida a los comerciantes, mediante el procedimiento de validación previa que realizará la DIAN y la firma digital del emisor. Esta se convierte en una funcionalidad muy importante a efectos de evitar riesgo moral en la emisión de facturas, el cual sucede con las facturas de papel en una eventual doble negociación. De esta forma se garantiza la unicidad en la existencia de facturas, la trazabilidad de su negociación y que sus legítimos tenedores podrán ejercer sus derechos sin que medie riesgo de fraude.

c. Servir como mecanismo para consignar los eventos de acuse de recibo y la aceptación tácita o expresa de las facturas electrónicas. Este es uno de los pilares de su funcionamiento, pues dichos elementos configuran legalmente los requisitos para convertir la factura electrónica en un título valor.

d. Dejar constancia de todos los eventos de negociación de las facturas electrónicas, incorporando los endosos.

e. Servir como vitrina virtual para que los emisores interesados puedan ofrecer sus facturas electrónicas de venta-título valor a los sistemas de negociación. En este caso puede suceder que el emisor cuente con una negociación previa con un sistema de negociación, procediendo la negociación directa, o que el emisor no tenga un acuerdo previo con un sistema de negociación, en cuyo caso los sistemas de este tipo deberán realizar una labor comercial para ofrecer sus servicios.

f. Emitir los certificados necesarios a favor de los legítimos tenedores de las facturas electrónicas a efectos de permitir su ejecución judicial.

4.4.2. Su funcionamiento

Las siguientes deberían ser las instancias que tendrán que surtirse durante el procedimiento de emisión y negociación de facturas electrónicas-título valor:

a. El emisor vende mercaderías y/o presta un servicio al adquirente (pagador).

b. El emisor, haciendo uso de su proveedor tecnológico o de la solución gratuita de la DIAN, crea la factura electrónica de venta y la transmite a dicha entidad.

c. La DIAN valida que la factura electrónica de venta contenga todos los requisitos legales, entre ellos que corresponda a la autorización de facturación que tenga el emisor.

d. Una vez validada la factura, el emisor la remite al adquirente (pagador), quien la recibirá a través de su proveedor tecnológico, la solución gratuita de la DIAN o un software propio debidamente habilitado por esta.

e. Entregada la factura al adquirente, inicia el término de tres días hábiles para que opere la aceptación tácita.

f. Cuando el adquirente (pagador) emite el acuse de recibo, este es enviado tanto al emisor como a la DIAN. En este momento se configuran los requisitos para que dicha factura sea título valor.

g. Cuando el adquirente (pagador) no emite el acuse de recibo y transcurren los tres días hábiles, el emisor notificará a la DIAN este hecho, dejando constancia de que operó la aceptación tácita. Esta constancia se entenderá emitida bajo la gravedad de juramento.

Cumplido el anterior procedimiento, se entenderá originada factura electrónica de venta, con todas las características de título valor. Reiteramos que se tratará de un documento desmaterializado, cuyo formato es XML, que cuenta con un código único de factura electrónica (CUFE). Eventualmente, podrá contar con un sistema de verificación consistente en un código de barras o QR que permitirá constatar su validez y estará representada gráficamente en un archivo PDF.

4.4.3.Interacción en la negociación

a. El emisor notificará su intención de venta a la DIAN a través del proveedor tecnológico, la solución gratuita o el software propio.

b. La DIAN incorporará dicha intención el registro para que los sistemas de negociación y/o intermediarios del mercado puedan conocer la factura electrónica de venta que se pretende negociar.

a. En caso de existir una negociación previa entre un emisor y un sistema de negociación (intermediario), el emisor podrá informar al registro de la existencia de un mandato para que dicho sistema de negociación, en virtud de las condicionas pactadas vía contractual, bloquee la factura y adquiera el título.

b. Si, por el contrario, no existe una negociación previa con el emisor, la factura electrónica de venta será publicada en el registro para que los sistemas de negociación presenten ofertas para su adquisición.

c. Una vez negociada la factura electrónica, los sistemas de negociación podrán informar el cambio de propiedad a la DIAN, lo cual confirma la autoridad tributaria al sistema de negociación, y procede a notificar al pagador sobre la transferencia del título. El registro incorporará los datos de pago del nuevo legítimo tenedor, así como la información de la operación de compraventa del título.

d. Al vencimiento de la factura, el pagador debe dar noticia del pago al registro. Posteriormente, la DIAN notificará al sistema de negociación, y este emitirá la confirmación de pago. Esta notificación generaría la inhabilitación de la negociación del título por haberse extinguido la obligación de pago. En caso de que el pagador haya remitido la notificación de pago sin que medie confirmación por parte del legítimo tenedor, el título valor no podrá circular más.

05

Propuestas de interconectividad y funcionalidad del registro de facturas electrónicas

En este acápite relacionaremos algunas características con las que creemos que el registro podría convertirse en un habilitador en la negociación de facturas, promoviendo el crecimiento de las empresas, la formalización de estas y la inclusión financiera, yendo más allá de garantizar la idoneidad de un activo por negociar como lo es la factura de venta.

5.1. Continuidad en la facturación y prevención de bloqueo de negociación por factores técnicos de los proveedores tecnológicos (PT)

El registro debería contemplar que los emisores de facturas puedan contar con más de un proveedor tecnológico, con el fin de habilitarlos para que hagan el cambio de proveedor en cuanto se vean limitados por la usabilidad de uno de ellos. Además, permitiría que en caso de que alguno de los proveedores presente fallos se garantice la continuidad en la expedición de facturas electrónicas con un proveedor que sirva de respaldo.

Por su parte, la solución gratuita de facturación que ponga al servicio la DIAN debería tener toda la conectividad e integración para la emisión de facturas electrónicas y su posterior negociación. Esto les permitiría a las mipymes que no tienen recursos para costear un PT privado contar con un software integral.

En caso de bloqueo en la negociación de facturas por parte del PT (ya sea por su voluntad o por capacidad técnica), consideramos pertinente que los sistemas de negociación también tengan facultades para obrar en calidad de mandatarios de los emisores. De tal modo estos, en nombre y representación de los emisores, podrían realizar operaciones de transferencia de facturas a través de endosos que quedarán registrados en el repositorio de facturas electrónicas.

5.2. Protección a libre competencia por bloqueo de negociación de facturas electrónicas con supervisión de la SIC

Consideramos de la mayor importancia que, a través de sistemas como el repositorio de facturas electrónicas, empiecen a consolidarse sinergias entre las entidades públicas (a nivel intersectorial). El propósito de esto sería hacer más eficiente la protección al empresariado nacional frente a prácticas como el bloqueo en la negociación de facturas.

El repositorio de facturas electrónicas es el mecanismo idóneo para combatir este tipo de comportamientos. La prohibición de obstruir la circulación de facturas se encuentra establecida en el artículo 778 del Código de Comercio, norma que faculta a la Superintendencia de Industria y Comercio para que investigue y castigue a aquellas entidades que limiten la negociación de facturas en Colombia, pues esto es considerado como una práctica restrictiva de la libre competencia.

En el caso de la Superintendencia de Industria y Comercio, si la DIAN le provee una interfaz de consulta permanente sobre las transacciones del registro, las solicitudes de negociación y la eventual negativa de los pagadores frente a la negociación, por cualquier motivo, estaría generando una interacción entre autoridades administrativas que resultaría eficiente para prevenir, investigar y castigar dichos comportamientos, desincentivando el bloqueo de facturas electrónicas.

5.3. Apertura de Application Programming Interface (API)

Actualmente, el registro no prevé el suministro de información a los participantes del mercado de facturas electrónicas. A nivel global, la tendencia es democratizar el acceso a información de este tipo, a efectos de potenciar que jugadores basados en financiación alternativa, apalancados en la tecnología, faciliten el acceso a capital de trabajo a mipymes de forma rápida y económica.

No contar con esta funcionalidad podría jugar en contra de la profundización del mercado y el crecimiento en el uso del *factoring* y de la financiación alternativa como mecanismo de acceso a capital de trabajo de las mipymes. Así se perdería entonces la oportunidad de acelerar el desarrollo económico del país a través de la Cuarta Revolución Industrial.

Una iniciativa similar ya está en funcionamiento en Ecuador, donde haciendo uso de

la trazabilidad de la FE se identificó y analizó valor agregado y la composición de mercado, el porcentaje de bienes y servicios de fuente nacional en los encadenamientos productivos para una serie de sectores de la economía, complementando con otras fuentes información. Este tipo de estudio tiene dos aplicaciones relevantes en el conocimiento de la cadena de valor. La primera para apoyar el diseño de políticas públicas identificando los nodos de producción nacional y las industrias de mayor encadenamiento y, la segunda, para mejorar el impacto de la inversión pública y los incentivos fiscales orientándolos a aquellas actividades con mayor componente nacional y efecto multiplicador. En definitiva, esta aplicación otorga a la AT un papel en el proceso de regulación y competencia, además, de mejorar las políticas hacendarias tradicionales sobre el diseño de la inversión pública y los incentivos fiscales (Barreix y Zambrano, 2018).

Frente a lo anterior, y en consideración al contexto internacional donde múltiples economías están profundizando la inclusión financiera y el acceso a capital de la base empresarial, apoyados en la apertura de información de los registros de facturación electrónica, debe tenerse en cuenta que la DIAN podría desempeñar un papel preponderante en la democratización del acceso a información haciendo que el mercado se nutra de data estructurada en un marco de equidad. Esto ayudaría a superar barreras de mercado como las que impone la información asimétrica, lo cual para algunos jugadores del mercado representa una ventaja competitiva.

La apertura de esta información a todos los sistemas de negociación, actores de financiación alternativa y tradicional, permite la disminución en costos y acelera la implementación de eficiencias para facilitar el acceso a capital de trabajo a mipymes pues: (i) disminuye el riesgo moral que existe en el marco de la vinculación por la falta de certeza sobre la documentación objeto de estudio; (ii) la DIAN brindaría información confiable en materia de hábitos de pago de los facturadores electrónicos y sus clientes, previa autorización; (iii) permite la creación de un sistema de trazabilidad de recursos, robusteciendo así los sistemas de prevención de lavado de activos y financiación del terrorismo; (iv) permite evaluar con más criterio el riesgo en operaciones de *factoring*, *confirming* y cualquier otro mecanismo que propenda al financiamiento de capital de trabajo, lo cual repercutiría necesariamente en la fijación de una tasa de interés acorde con el riesgo real que representa un emisor.

5.4. Aplicación de regulación comercial y sinergias intersectoriales

Entendemos que actualmente la DIAN está estructurando el registro de facturas electrónicas dentro del marco de sus facultades legales y reglamentarias. Sin embargo, esto no se puede convertir en un obstáculo para que el registro de facturas electrónicas sea implementado sin observar de manera estricta la regulación comercial en materia de facturas electrónicas de venta, pues dichos títulos valores son fundamentales para el acceso al capital de trabajo de las mipymes en Colombia. Cualquier afectación a la calidad de título valor de las facturas electrónicas puede tener amplias repercusiones en el crecimiento del empresariado nacional, en la profundización del *factoring* y en el financiamiento alternativo como herramienta de acceso a capital de trabajo, la formalización de empresa, la competitividad del país, la inclusión financiera e inclusive el recaudo tributario.

5.5. Proceso ejecutivo con facturas electrónicas

Aunque es un paso que va más allá de la estructuración del sistema de registro y negociación de facturas electrónicas, una parte fundamental en la circulación de dichos títulos valores es su ejecución. En este sentido, una eventual reforma al Código General del Proceso podría comprender un modelo de proceso ejecutivo para facturas electrónicas que sea mucho más expedito.

Lo anterior cobra sentido si consideramos que, dentro de una ejecución regular en la que se aportan el título y los soportes que legitiman al tenedor, la participación del demandado es casi nula hasta la emisión del mandamiento de pago. Así el demandante, en el caso de la factura electrónica, tendría un documento que incorpora un derecho a su favor, el cual ha sido verificado por una autoridad administrativa como la DIAN, la cual vela porque este cumpla con los requisitos legales para que sea título valor.

En dicha medida, prevemos que el proceso ejecutivo, al menos hasta la emisión del mandamiento de pago, podría surtirse de manera electrónica hasta el momento en el que el deudor deba ser notificado, instancia en la que un juez de la República estaría llamado a intervenir para garantizar el derecho a controvertir el auto que ordena pagar las sumas ejecutadas.

Sobre esta propuesta hay que hacer un llamado a la prudencia y al estudio de sus efectos positivos y negativos. Sin embargo, no hay que dejar de lado que la innovación y la tecnología deben permear en la mayor medida posible nuestra sociedad y sus instituciones, en pro de establecer mecanismos que nos hagan más competitivos frente a otros países.

Conclusión

A lo largo de este capítulo revisamos los antecedentes normativos de la factura electrónica de venta. Esto con la finalidad de demostrar que la puesta en marcha del registro de facturas electrónicas requiere de un trabajo mancomunado de distintas entidades del orden central, tales como la DIAN, el Ministerio de Comercio, Industria y Turismo y la Superintendencia de Industria y Comercio.

Sin embargo, la necesidad de contar con la factura electrónica en el menor tiempo posible como mecanismo de control tributario ha hecho que se le reste importancia a ella como título valor, pues se advierte que la DIAN podría no contemplar el impacto económico que tendría en el país una implementación que no considere la totalidad de los elementos mercantiles de dicho documento digital.

Sin duda, desde que este proyecto empezó con fuerza desde el año 2008, no ha quedado evidencia de que las autoridades llamadas a liderar la puesta en marcha del registro del que hemos hablado hayan integrado mesas de trabajo interdisciplinares que les permitan dilucidar la importancia que tiene este sistema para la base empresarial colombiana, que por falta de acceso a productos de crédito tradicionales encuentra en la negociación de sus facturas la salida para continuar desarrollando sus actividades mercantiles, generando empleo, incrementando el recaudo de impuestos y aportando al PIB de Colombia.

También analizamos el contexto operativo del registro de facturas. Al respecto presentamos el esquema centralizado de administración del registro, el cual propugna porque la competencia entre sistemas de negociación e intermediarios sea la que le dé dinámica al mercado. Resaltamos esta característica, pues le dará valor agregado a la negociación de facturas, diferenciándose del modelo que pretendía implementar el MinCIT.

El artículo culminó con algunas sugerencias para que el registro sea revolucionario. Estas ideas propenden a sacar el máximo provecho de la información que generará el registro, la cual se convertiría en un habilitador de negocios sin par en la región y que haría muy atractivo al mercado de facturas en Colombia para empresarios nacionales e internacionales, máxime si se tiene en cuenta que es uno de los activos más sanos a nivel internacional para invertir. En esta medida, contaríamos con un mercado diferenciado y con tal profundidad que la base empresarial colombiana tendría los recursos necesarios para crecer.

Bibliografía

Barreix, A. y Zambrano, R. (2018). **Factura electrónica en América Latina**. Monografía del BID 595. Banco Interamericano de Desarrollo.

Boulanger, T. (2015). XML Práctico: Bases esenciales, conceptos y casos prácticos. Segunda edición. Eni Ediciones.

Mesfix. (2018). Las facturas electrónicas no podrán ser negociadas para financiación de mipymes. [En línea]. Recuperado de: https://mesfix.com/blog/2018/10/03/facturas-electronicas-no-podran-ser-negociadas/. [Consultado el 18 de mayo de 2019].

Mol-Gómez-Vázquez, A., Hernández-Cánovas, G. y Koëter-Kant, J. (2016). Legal and Institutional Determinants of Factoring in SMEs: Empirical Analysis across 25 European Countries. Journal Of Small Business Management, 56(2), 312-329. Doi: 10.1111/jsbm.12260.

Soufani, K. (2001). The Role of Factoring in Financing UK SMEs: A Supply Side Analysis. Journal of Small Business and Enterprise Development, 8(1), 37-46.

Jurisprudencia

Artículo 779 del Código de Comercio.

Artículos 616-1, 511, 615, 617, 618 y 684-2 del Estatuto Tributario.

Ley 1437 de 2011, Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Ley 223 de 1995.

Ley 962 de 2005.

Ley 527 de 1999.

Ley 1231 de 2008.

Ley 1753 de 2015.

Ley 1819 del 2016.

Decreto 2242 de 2015, recopilado en el 1625 de 2016.

Decreto 2669 de 2012.

Decreto 1349 de 2016.

Decreto 1071 de 26 de junio de 1999.

Decreto 3626 de 10 de octubre de 2005.

Decreto 4048 del 22 de octubre de 2008.

Decreto 1321 del 26 de abril de 2011.

Decreto 1292 del 17 de julio de 2015.

Resoluciones 2215 de 2017 y 294 de 2018, expedidas por el Ministerio de Comercio, Industria y Turismo.

Resolución 001 del 5 de enero de 2018, proferida por la DIAN.

Resolución 0294 de 2018 del Ministerio de Comercio, Industria y Turismo.

Resolución 2215 de 2017 del Ministerio de Comercio, Industria y Turismo.

Oficio 220-010483 del 22 de febrero de 2019, de la Superintendencia de Sociedades.

Gaceta del Congreso N.° 477 de 2007, publicada el 27 de septiembre de 2007.

Proyecto de Ley N.o 151 de 2007.

RETOS DEL USO DE DRONES EN EL COMERCIO ELECTRÓNICO

Germán Realpe Delgado[209]

Resumen

El sueño del hombre siempre ha sido volar, tocar las nubes y poder ver el mundo desde las alturas. Existen una gran cantidad de poemas y frases relacionadas con volar, los cuales transmiten la sensación de que el hombre pueda levantarse del suelo. Este anhelo de volar como un pájaro se remonta a los orígenes de la humanidad, y varios siglos después, con los hermanos Wright, el hombre pudo alcanzar las nubes por medio de la aviación. Sin embargo, hace unos años los drones se tomaron el mundo para mostrar que el vuelo puede experimentarse por otros medios.

Los drones han empezado a su vez a convertirse en los mejores aliados para el comercio electrónico y los servicios asociados a este. El presente artículo muestra la historia, los retos y la evolución de estos artefactos y su relación con el comercio electrónico, al tiempo que analiza cómo en la actualidad el mensaje de datos, introducido por la Ley 527 de 1999, empieza a fusionarse con el uso de drones, robots y tecnología.

El uso de tecnología como la de los drones implica muchos retos, entre ellos la regulación, el uso en el comercio electrónico, la privacidad y seguridad de la información, y la necesidad de controlar, por parte de cada Estado, su espacio aéreo.

El presente análisis se basa en distintas fuentes como lo son artículos, páginas *web* de tecnología, noticias publicadas en medios de comunicación, libros y la experiencia del autor en seguridad de la información y en el uso de drones.

Palabras claves: dron; uso de drones en el comercio electrónico; ***hacking*** drones; ***drone delivery***; ***drone ecommerce.***

209. Abogado de la Universidad Santo Tomás, especialista en Derecho Comercial de la Universidad Javeriana, especialista en Derecho Informático de la Universidad Externado de Colombia, y de la Universidad Complutense de Madrid. Consultor en seguridad de la información técnica en OSINT (búsqueda de información de fuentes públicas). Auditor interno en la norma ISO 27001 de Seguridad de la Información. Ha asesorado y participado en proyectos de tecnología y seguridad informática en distintas empresas del sector privado y entidades públicas como el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), CAR, entre muchas otras. Autor de proyectos de ley, entre ellos el borrador de decreto que reglamenta la Ley 1437 de 2011. Como apoyo aportó en la redacción del Decreto 2609 de 2012, en lo referente a documento electrónico, y resoluciones como la 2518 de 2015, respecto a activos de información en la Corporación Autónoma Regional de Cundinamarca (CAR). Reconocido por SAP México como uno de los colombianos que más conocen de ***cloud computing***.

Abstract

Man's dream has always been to fly, touch the clouds and be able to see the world from above. There are a lot of poems and phrases related to flying, which convey the feeling that man can rise from the ground. This longing to fly like a bird dates back to the origins of mankind, and several centuries later, with the Wright brothers, man was able to reach the clouds through aviation. However, a few years ago the drones took the world to show that the flight can be experienced by other means. The drones have also begun to become the best allies for electronic commerce and the services associated with it.

This article shows the history, challenges and evolution of these artifacts and their relationship with electronic commerce, while analyzing how the data message, introduced by Law 527 of 1999, begins to merge with the use of drones, robots and technology.
The use of technology such as drones involves many challenges, including regulation, use in electronic commerce, privacy and information security, and the need to control, by each State, its airspace. This analysis is based on different sources such as articles, technology web pages, news published in the media, books and the author's experience in information security and the use of drones.

01

De la mitología a la tecnología

Según la mitología griega, Ícaro, llevado por sus ganas de escapar de una isla, fabricó con su padre unas alas de madera y de cera que lo llevaron a la libertad. Sin embargo, una vez voló a demasiada altura sus alas se derritieron, por lo que él cayó al mar y murió. Esta historia refleja cómo volar siempre ha sido el sueño de los hombres: tocar las nubes se vuelve una expresión de imponencia, de fortaleza, la cual la tienen muchos héroes en sus historietas. Y esto, que era un mito, cobró realidad con los hermanos Wright, quienes durante varios años construyeron el primer aeroplano del mundo, el cual tocó el cielo el 17 de diciembre de 1903. Luego de este logro, la aviación cambiaría la forma de transportación de los hombres, hasta tal punto que hoy podemos estar en cualquier lugar en pocas horas.

La evolución de la aviación para muchos ha sido lenta, pero con muchas ventajas. De hecho, en la actualidad ya se está pensando en viajar a otros planetas y se están considerando medios de transporte alternativos. Por ejemplo, Elon Musk viene desarrollando el proyecto Hiperloop, también conocido como transporte de alta velocidad ya que puede alcanzar velocidades superiores a los 1.200 kilómetros por hora (Xataka, 2018). El mismo Musk también viene trabajando en su empresa Space X con miras a hacer viajes al espacio, cuyo primer paso fue enviar el pasado 8 de febrero de 2018 un cohete a Marte (BBC Mundo, 2018).

En lo relacionado con drones, son muchas las fuentes que muestran la historia de los primeros instrumentos de este tipo, pero sin lugar a duda tiene mucha importancia el aporte de Elmer Ambrose Sperry, conocido por desarrollar una plataforma de aeronaves sin piloto con un dispositivo para lanzar torpedos con una catapulta. Luego, en guerras como la de Vietnam se empezaron a utilizar aviones no tripulados para la vigilancia aérea. Posteriormente, durante los años 80 se consolidó la tecnología UAV como algo tecnológicamente fiable y que potencialmente ya podía rendir más que un avión tripulado, como puso de manifiesto el enfrentamiento hombre-máquina entre el piloto de la unidad de élite Top Gun, John Smith, y su F-4 Phantom contra un avión no tripulado (Víctor Delgado, s.f.).

Para hablar de drones debemos también hablar de robots, ya que el dron no es otra cosa que un robot con sensores que puede prestarse para muchas aplicaciones (Wikipedia, s.f.). En otras palabras, un dron es un sistema de información, una computadora con la capacidad y el propósito de movimiento, que en general es capaz de desarrollar múltiples tareas de manera flexible según su programación.

En el año 2000 empezaron a tomar fuerzas los drones caseros, los cuales se podían comprar en tiendas de tecnología. A nivel personal, en el Consumer Electronics Show realizado en el 2010 en Las Vegas, causó un gran impacto la presentación del Parrot AR Drone, el cual contaba con un sistema operativo Linux, cámaras y sensores, y se podía controlar desde aplicaciones móviles.

En la misma línea se encuentra la trayectoria de Frank Wang, quien empezó estudiando ingeniera electrónica para luego pasar a quedar en un tercer puesto en una competencia de robótica denominada Robocon Asia Pacífico (Carbajal, 2017). Años más tarde, Wang fundaría la empresa DJI, la cual empezó en el 2006 con 20 empleados y en la actualidad es la más fuerte en diseño y construcción de drones, con oficinas en Estados Unidos, Alemania, Holanda, China, entre otros países (Xataka, 2015). Lo interesante de este caso particular es que ha venido creando todo un ecosistema con temas de software, hardware, fotografía y se ha convertido en líder indiscutible en el mercado de drones, donde tiene equipos para sectores como agricultura, cine, seguridad, infraestructuras, vigilancia, construcción, etc.[210]

Para el entretenimiento existen también los drones de carreras. Estos son controlados por medio de gafas FPV (***First Person View***), transmiten una cámara en tiempo real y pueden alcanzar velocidades superiores a los 200 kilómetros por hora. De hecho, esta clase de drones están empezando a trascender el campo del entretenimiento para ser usados con fines ambientales, cinematográficos y de vigilancia.

Otra aplicación de los drones es la deportiva. Así, en la actualidad se cuenta con diversos pilotos profesionales y una liga denominada The Drone Racing League, fundada por Nicholas Horbaczewski en 2015, que cuenta con pruebas realizadas en distintos países a nivel mundial y otorga premios por más de un millón de dólares[211]. El potencial de estas carreras a nivel internacional apunta a que las ventas de estos drones alcancen los 16 millones de unidades en el año 2020.

Otra categoría de drones es la denominada ***Remotely Piloted Aircraft*** (RPA), que son los drones que se usan para fines militares y estatales. Según la clasificación de la Organización Internacional de Aviación Civil (OACI), que considera estos instrumentos como ***Unmanned Aerial System*** (sistema aéreo no tripulado) (UAS), estaríamos hablando entonces de ***Remotely Piloted Aircraft System*** (sistema aéreo tripulado por control remoto) (RPAS). Dentro del ámbito tecnológico, podemos encontrar los drones para servicios, los cuales son utilizados a nivel empresarial, y los drones caseros, empleados para temas de entretenimiento, ***hobbie*** o fotografía.

Se debe resaltar que los drones todavía no tienen cabida en la aviación comercial, y la misma OACI se encuentra en distintas discusiones respecto a la integración de esta tecnología a la aviación tradicional. En esa medida, es claro que el tema de riesgo y la forma de compartir el espacio aéreo tendrán regulaciones o directrices en unos pocos años.

En conclusión, con los drones el hombre está conquistando su sueño de tocar las nubes, a la par que se sirve de ellos para proveer distintos servicios, con todo lo que esto implica para el ámbito empresarial y el uso personal.

210. Productos de la empresa DJI disponibles en https://www.dji.com/products/industrial.

211. ***Web*** de la empresa de drones de carreras disponible en https://thedroneracingleague.com.

02

Drones y robots en el comercio electrónico

La entrega de paquetes con drones puede parecer algo de película, pero sin duda será el cambio más importante que pueda tener el comercio electrónico. Entre las empresas que vienen haciendo distintos pilotos en ese sentido se encuentra Amazon, la cual tiene un servicio denominado Amazon Prime Air[212], destinado a realizar entregas con paquetes de peso máximo de dos kilos y a una distancia máxima de 25 kilómetros. En esa misma línea avanzan otras empresas no tan grandes, como Cambridge Consultants, la cual tiene un dron mensajero denominado DelivAir, el cual se enfocará en entregas inmediatas de mercancías de poco peso (Cambridge Consultants, 2017). Asimismo, la empresa china Jd.com obtuvo una licencia de operación en Indonesia y está realizando varias pruebas que tienen como finalidad utilizar aviones no tripulados para entregar en un futuro el 85 % de sus pedidos en el mismo día de la orden o al día siguiente (Russell, 2019).

Por otra parte, ya existen varias empresas que vienen trabajando en la entrega de domicilios o ***delivery*** con el uso de robots. En ese sentido debe mencionarse la empresa Kiwi, liderada por el colombiano Felipe Chávez, la cual empezó como una ***startup*** y en la actualidad es la que más domicilios ha hecho con robots a nivel mundial. Sus kiwibots son pequeñas máquinas con seis cámaras, sensores e inteligencia artificial que utilizan una tecnología llamada ***computer vision***, la cual les permite reconocer los objetos que se encuentran en el camino, desde árboles, carros y semáforos hasta personas (Bustamante, 2017). Se trata, pues, de un sistema colaborativo entre humanos y robots, en donde muchos de los ingenieros y programadores son colombianos (Cortés, 2018).

212. Servicio de Amazon Prime disponible en https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011.

Kiwi empezó entregando domicilios en la universidad de Berkeley en California, pero su servicio se ha extendido a varios campus universitarios de Estados Unidos. La empresa también cuenta con oficinas en Bogotá y en Medellín, y parte de su flota de robots se está desarrollando en Shenzhen, China. Estos kiwibots son una solución para bajar tiempos y costos en países como Estados Unidos, donde el costo de un domicilio o de un ***delivery*** en el marco del comercio electrónico es en promedio de nueve a once dólares. Una curiosidad de esta iniciativa es que empezó haciendo entregas de domicilios solicitadas por la aplicación WhatsApp con un simple mensaje de datos al que le daban todo el valor probatorio en el momento de sustentar su negocio, y ha evolucionado al transporte de mercancías con el uso de robots.

El común denominador de estos proyectos es tiempo, agilidad y costos, algo que se ve reflejado con el uso de drones o robots. La regulación en este campo es algo que todavía genera algunas dudas en varios países, pero queda claro que se puede superar ya que la innovación es algo que no se puede frenar.

Otras empresas en Colombia de mensajería tradicional se encuentran realizando proyectos de innovación con el uso de drones. En definitiva, los proyectos de comercio electrónico son una necesidad de las empresas de transporte de mercancía, y en ese sentido las alianzas con empresas de servicio de drones pueden ser útiles para ampliar en pocos años su alcance mediante esta tecnología.

Empresas como el BPO colombiano Millenium vienen trabajando en proyectos de esta clase. Ejemplo de ello es el desarrollo de un robot con nombre Thalon, enfocado al sector hotelero (EFE, 2019). La empresa, que se dedica a temas de servicios, cuenta con un área de innovación y de datos no estructurados en donde los drones y el software son parte fundamental de sus nuevos productos. Son iniciativas que ya se están ejecutando; se podría decir, entonces, que el único reto son los cambios en la regulación en un contexto donde los drones entran a compartir espacio con la aviación tradicional. Por ejemplo, es importante analizar la manera de enfrentar los riesgos de operación.

Podemos decir que Colombia es pionera en el uso de drones para el comercio electrónico y que está siendo un referente a nivel mundial tanto por sus empresas como por la capacidad de innovación de sus profesionales en disciplinas como aeronáutica, desarrollo de software, programación e innovación.

03

Del mensaje de datos al uso de drones

La Ley 527 de 1999 es sin lugar a duda el cambio más importante en Colombia para el comercio electrónico. Esta representa la introducción y adaptación de la ley modelo sobre comercio electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (Uncitral, por su sigla en inglés), y en esa medida ha dado los conceptos fundamentales en Colombia para la incorporación de todo tipo de tecnologías con validez técnica y jurídica por medio del concepto del mensaje de datos.

El mensaje de datos es definido en la ley mencionada como la ***"información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax"***[213]. Así pues queda planteado el campo para la aplicación de todo tipo de tecnologías y se constituye la entrada para la utilización de mensaje de datos en varios aspectos de la vida humana, ya que es el que sirve para expresar en la actualidad el consentimiento en el uso de redes sociales y de correos electrónicos en plataformas como Uber, Rappi, Airbnb, entre otras. A esto se le debe sumar la validez probatoria de tales mensajes, la cual de forma legal es señalada en los artículos 6 y 10 de la Ley 527 de 1999.

La misma ley se refiere al equivalente funcional así: ***"cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que este contiene es accesible para su posterior consulta"***[214]. En otras palabras, este equivalente es la mejor expresión del uso de tecnología equivalente al papel en todo tipo de transacciones del ser humano.

Los dos conceptos mencionados —mensaje de datos y equivalente funcional—, sin quererlo, han contribuido en 20 años al desarrollo de todo tipo de tecnologías. Es el caso de softwares, hardware, drones, sistemas de información, inteligencia artificial, sistemas expertos, soluciones de ***big data***, aplicaciones móviles, entre otras.

Siguiendo con la Ley 527 de 1999, el comercio electrónico abarca ***"las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar"***[215]. Esta interpretación ha llevado a evolucionar el comercio electrónico a la incorporación de software y hardware para las operaciones de venta, compra y logística de todo tipo de bienes muebles.

En últimas, la flexibilidad y estabilidad del comercio electrónico se debe en parte a la evolución del mensaje de datos en su máxima expresión. De manera que el tema no es jurídico; es tecnológico: su evolución

213. Artículo 2, Definiciones, de la Ley 527 de 1999, "por la cual se define y reglamenta el acceso y uso del mensaje de datos, del comercio electrónico".

214. Artículo 6 de la Ley 527 de 1999, "por la cual se define y reglamenta el acceso y uso del mensaje de datos, del comercio electrónico".

215. Artículo 2, Definiciones, de la Ley 527 de 1999, "por la cual se define y reglamenta el acceso y uso del mensaje de datos, del comercio electrónico".

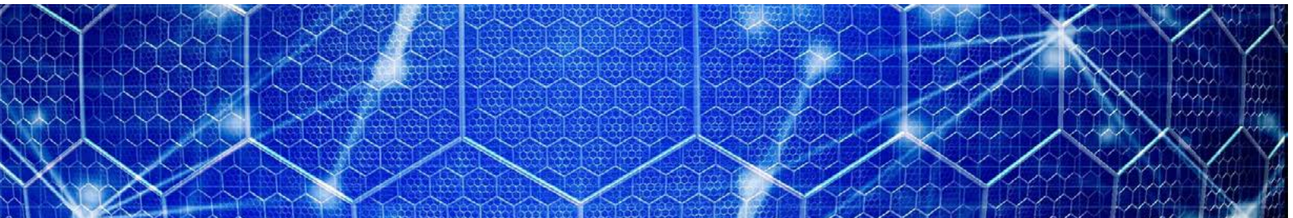
se debe a la transformación digital, a la necesidad de la sociedad actual de contar con información y productos de forma rápida. También tiene su parte el cambio cultural que implican los llamados ***millennials.*** La autora Lee Caraher, en su libro ***Millennials en la oficina***, muestra cómo las generaciones actuales no siguen reglas y su proceso de evolución hace que la industria se desarrolle mucho más rápido. La autora también muestra cómo la comunicación ha cambiado, lo que hace que las plataformas de comunicación evolucionen año tras año.

La Ley 527 de 1999 cumple 20 años, algo que en el mundo jurídico no significa muchos cambios. De hecho, si revisamos su esencia normativa, esta no ha tenido modificaciones y son más las normas que la citan que las que la cambian. Es el caso de normas como la Ley 1437 de 2011, o las de gestión documental que incorporan la esencia de la Ley 527 de 1999 en la definición de documento electrónico y del principio de equivalente funcional (***i.e.***, Decreto 2609 de 2012 del Archivo general de la Nación). Para servicios de gobierno electrónico pasa lo mismo: la referencia a la Ley 527 es casi obligatoria en distintas normas y políticas de gobierno digital, como es el caso del Decreto 1008 del 14 de junio de 2018.

Ahora bien, todo lo contrario pasa con el manejo de la información y la tecnología, el cual ha llevado a diversos cambios tecnológicos. Ya en la primera parte de este escrito hablamos de cómo el hombre ha enviado un cohete a Marte y señalamos que, en 20 años posteriores a la Ley 527, ya estamos en un mundo de automatización de muchas actividades humanas. Tal avance se refleja en algunos de los ejemplos que pone la Ley 527 de 1999: si bien se refiere a la información que es enviada por medios como telegrama, télex, telefax, ahora en 2019 muchos de estos medios prácticamente no existen, y la información es enviada por mecanismos como WhatsApp, Telegram, Instagram, Facebook, entre otros.

El mundo actual hace que la forma como se envía información sea distinta que la de hace unos años. En ese contexto, el papel de robots, softwares, hardware y drones es fundamental, ya que ofrecen dos aspectos vitales que se están trasladando a todos los sectores y mercados laborales: la inmediatez y la automatización de tareas complejas. Es así como la robótica y el uso de drones han llegado a reducir los costos de producción y han aumentado la eficiencia de las empresas. Un estudio de la Universidad de Oxford de 2017 incluso señala que muchos profesionales están en riesgo con la automatización, sobre todo aquellos relacionados con trasporte y logística. De todas maneras, la originalidad y la inteligencia social no son tan sencillas de automatizar (BBC Mundo, 2017).

Podemos señalar entonces que los conceptos de mensaje de datos y equivalente funcional han tenido una evolución o, mejor aún, una revolución debido a la tecnología, lo que hace que nos encontremos en un momento de plena transformación digital.



04

Regulación de los drones

Las posibilidades de los drones son innumerables: aplican para cualquier industria y actividad. De este modo, a nivel mundial existe una gran cantidad de empresas que se encuentran ofreciendo distintos servicios empresariales con el uso de drones. Tales servicios pueden ir desde la toma de una foto con un dron para un evento hasta usos industriales, ambientales, de vigilancia o de comercio electrónico.

El auge de la venta de drones, así como de empresas que ofrecen servicios, llevó a la necesidad de regular con normativa locales el uso de esta tecnología. Particularmente, como se mencionó, se debe abordar el riesgo que implica el hecho de que los drones empiecen a compartir espacio aéreo con la aviación comercial. Con esto en mente, la OACI se encuentra realizando diversos estudios para buscar la forma de que los drones puedan compartir el cielo con la aviación tradicional. Cabe considerar al respecto que, debido al tamaño y a sus condiciones operacionales, las aeronaves y los prototipos no tripulados no se ajustan a las definiciones correspondientes a las aeronaves normales que figuran en el Convenio sobre Aviación Civil Internacional (Convenio de Chicago), por lo que la OACI viene analizando la mejor forma de dar pautas para que puedan coexistir los drones y el tránsito aéreo.

En principio hay que recordar el término adecuado para referirse a los drones de acuerdo a lo señalado por la OACI, cuya clasificación de UAS (***Unmanned Aerial System***, sistema aéreo no tripulado) convierte el RPA en RPAS (***Remotely Piloted Aircraft System***).

Para dar pautas, la OACI hace una serie de reuniones en donde participan los distintos países. La última se llevó a cabo en septiembre de 2018, en el marco del Tercer Simposio Mundial de Sistemas de Aeronaves Pilotadas a Distancia (RPAS) y también del Segundo Simposio OACI sobre la Industria de Sistemas de Aeronaves no Tripuladas (OACI, 2018). Las preocupaciones pueden señalarse en los siguientes puntos:

* Gestión del tránsito entre UAS.
* Seguridad en las operaciones.
* Privacidad de los ciudadanos.
* Uso de espacio aéreo compartido.
* Operación de drones en ultramar.
* Regulación a baja altitud.
* Licencias y permisos de operación.

La respuesta de la industria a nivel mundial frente a estas inquietudes es que los entes de control regulen y controlen la operación con drones. Para esto cada país ha venido desarrollando normativas locales, las cuales en muchos casos ya se encuentran en su segunda y tercera versión desde su expedición. Esto pasa por ejemplo en España y Colombia, los cuales ya tienen segundas versiones sobre su normativa de drones, denominados legalmente como UAS.

En el caso de España, en el año 2018 entró en vigencia el Real Decreto 1036 de 2017, el cual modificó el Decreto 552/2014 del 27 de junio de 2014. Esta nueva regulación amplía los permisos de vuelo, concediendo la posibilidad de volar en un espacio aéreo controlado y de hacer vuelos nocturnos, o de impulsar nuevas actividades urbanas como la limpieza de rascacielos, la inspección de fisuras o daños arquitectónicos de monumentos emblemáticos, el control aéreo del tráfico, la vigilancia de costas, entre otras (EFE, 2018).

En el caso de Colombia, la normativa relacionada con drones es competencia de la Aeronáutica Civil como autoridad aeronáutica en Colombia. La primera regulación en el tema fue la Circular Reglamentaria 5100-082-002 de 2015[2016], conocida como la Circular 002, que incorporó a la normatividad requisitos generales de operación con drones o RPAS. Así, este documento impone la obligación de registrar el dron y solicitar el permiso para la operación ante la Aerocivil. La circular, que en un principio aplicaba para actividades diferentes a las de recreación y deporte y fue la primera regulación del uso de drones en Colombia, tuvo un cambio importante en lo que respecta al registro y permiso de operación, así como en cuanto a la necesidad de que los pilotos tengan una formación certificada por academias autorizadas ante la aeronáutica.

Luego del incremento de operaciones, y dada la necesidad de los cambios normativos en el mes de diciembre de 2018, se expidió la Resolución 04201 del 27 de diciembre de 2018, la cual es el marco normativo que aplica para Colombia. Esta nueva norma tiene como diferenciador que ya no es una circular, sino que aplica un apéndice para la norma RAC 91 de los reglamentos aeronáuticos de Colombia denominado “Operación de sistemas de aeronaves no tripuladas UAS”. Dentro de su aplicabilidad se excluyen el uso de aeromodelos o globos cautivos, las operaciones realizadas por las fuerzas militares o de política dentro de sus funciones y el empleo de drones en espacios cubiertos.

De la norma se debe destacar que la operación de los drones es clasificada, de acuerdo a su riesgo operacional, en clase A y clase B o regulada. En el primer caso no se requiere autorización dado que no representa un riesgo, caso contrario a lo que pasa con las operaciones de la clase B o regulada, en donde se encuentran UAS con peso superior a 25 kg y de hasta 150 kg que sí requieren siempre autorización de la UAEAC (Unidad Administrativa Especial de la Aeronáutica Civil)[217].

La norma también incluye una categoría pensada para servicios de transporte o sobrevuelos internacionales, denominada clase C: drones con peso superior a los 150 kg. Al respecto, la resolución es clara en resaltar que todavía no se autoriza su operación en el espacio aéreo colombiano, aun cuando esta pudiera ser de bajo riesgo, aunque se deja abierta una posibilidad a que la Aeronáutica emita permisos especiales a entidades públicas y privadas debidamente reconocidas o autorizadas con fines exclusivos de investigación científica, innovación y desarrollo.

En últimas, esta nueva norma es un cambio importante para el uso de drones en Colombia, en donde para temas regulatorios son llamados UAS. En primer lugar, tenemos una tipificación por peso y por operación. Así mismo, tenemos una clase A, la cual permite realizar operación sin necesidad de autorización, aunque bajo la limitante de que no puede llevarse a cabo sobre público, conglomeraciones o edificios. Tampoco se permiten el transporte de objetos o la fumigación con estos UAS, ni las tareas de búsqueda, entre otras. El propietario de un UAS de esta clase debe estar inscrito con datos como nombre, correo electrónico, datos de contacto y marca y modelo del dron con el cual realice su operación.

Para las operaciones de drones clase B se necesita autorización de la aeronáutica y el cumplimiento de varios requisitos de operación, entre ellos la inscripción como explotador y operador de UAS de clase B. Así mismo se exige permiso previo, como tener una póliza de responsabilidad civil. En el caso del piloto del dron, debe ser mayor de 18 años y demostrar que aprobó el curso teórico certificado, por un centro de instrucción aeronáutica, o escuela autorizada por la Aeronáutica Civil[218].

En cuanto a comercio electrónico o transporte internacional, la norma, como se dijo, deja la puerta abierta, pero todo condicionado a las recomendaciones de la OACI y sus anexos técnicos de la aviación civil internacional. Aun así, la norma, en el numeral 4.2, de requisitos de operación de UAS de clase C, hace la salvedad de que la Aeronáutica Civil podrá autorizar su operación con carácter experimental, para lo cual será posible designar áreas especiales del espacio aéreo[219].

En conclusión, podemos ver que la normativa en Colombia cuenta con unas condiciones especiales para la operación de drones, y que desde el año 2018 se contemplan tres tipos de clases por operación y riesgo, entre ellas una para temas de comercio electrónico o mensajería (clase C), que todavía se encuentra en un carácter experimental y solo se puede aplicar para proyectos de investigación e innovación. De igual forma, es claro que el ente regulador está a la espera de las recomendaciones de la OACI, así como del desarrollo paulatino de los drones a nivel mundial.

216. Circular reglamentaria 5100-082-002 de 2015, de la Aeronáutica Civil.

217. Resolución 04201 del 27 de diciembre de 2018, de la Unidad Administrativa Especial de la Aeronáutica Civil.

218. Resolución 04201 del 27 de diciembre de 2018, de la unidad administrativa especial de la Aeronáutica Civil, numeral 3.7, requisitos para operadores de UAS de clase B.

219. Resolución 04201 del 27 de diciembre de 2018, de la unidad administrativa especial de la Aeronáutica Civil, numeral 4.2, requisitos para operadores de UAS de clase C.

05

Privacidad y seguridad de la información

Algunas de las preocupaciones en el uso de drones o UAS es lo referente a la privacidad de los ciudadanos, así como a la seguridad de la información, ya que estos instrumentos tienen sensores y potentes cámaras de video que les permiten capturar información y datos personales, en cuyo uso se deben respetar la integridad, la confidencialidad y la disponibilidad. Además, dicha información, que es generada y enviada por mensaje de datos, es transmitida por los drones tanto a las empresas fabricantes como a los distintos operadores.

La seguridad de la información de los drones se encuentra relacionada con las redes wifi, los sistemas de posicionamiento, el uso de software y hardware, la utilización de sensores, GPS, privacidad de fotografías y videos, grabaciones en infraestructuras críticas y registro de los drones en las páginas de los fabricantes. Por lo demás, la protección de datos personales y la seguridad de esta información también se extienden al uso mismo de drones. En el caso de datos personales se debe tener en cuenta la regulación de cada país, y se resalta la necesidad del consentimiento en el uso de drones, sobre todo en los casos que se capturen datos personales y sensibles (Martínez y Peláez, 2015).

En países como Argentina se pueden encontrar normas especiales sobre drones y privacidad. Es el caso de la Disposición 20/2015 del 27 de mayo de 2015 de la Dirección Nacional de Protección de Datos Personales, norma que señala la necesidad de proteger la privacidad del usuario en el la recolección de datos personales con el uso de drones. Así mismo se establece el requisito de inscribirse en el registro nacional de bases de datos de la Dirección Nacional de Bases de Datos Personales, esto es, las bases de datos recabadas con el uso de drones. La norma, además, deja en claro que esto no aplica para drones con fines recreativos y que no tienen la finalidad de capturar datos personales de terceros[220].

En el caso colombiano, los principios consagrados en el artículo 4 de la Ley 1581 de 2012, sobre tratamiento de datos personales, también aplican al uso de drones, estos son, el principio de finalidad, el de libertad, el de seguridad y el de confidencialidad. En el país también existe un instrumento que se puede relacionar con el uso de drones, y es la cartilla de protección de datos personales en sistemas de videovigilancia SV, la cual aplica a personas y empresas que utilizan sistemas de vigilancia por medio de cámaras, videocámaras, análogas o digitales, cámaras IP, minicámaras, y en general cualquier medio por el cual se realicen tratamiento de imágenes (Superintendencia de Industria y Comercio, s.f.). La cartilla resalta la necesidad del encargado y responsable del tratamiento de datos personales de garantizar la protección de los derechos de los titulares de información respecto de la recolección, almacenamiento, uso y disposición de sus datos personales, en este caso de su imagen.

Es fundamental, de acuerdo con la Ley 1581 de 2012, el Decreto 1377 de 2013[221] y las normas que la complementan, respetar la obligación de autorización, la finalidad de los sistemas de vigilancia y los procedimientos operacionales, así como establecer medidas de seguridad técnicas y humanas para la seguridad de los datos. Además, la delegatura de protección de datos de la Superintendencia de Industria y Comercio ha señalado que, cuando se implementa alguna técnica para la extracción de elementos particulares del rostro en una fotografía o video, estos se pueden clasificar como datos biométricos y por tanto sensibles[222]. Esto sucede en muchos casos con el software que tienen algunos drones, lo que significa que en algunos casos podríamos encontrarnos frente al manejo de datos biométricos y sensibles.

Dentro de las recomendaciones que trae la mencionada guía de la Superintendencia de Industria y Comercio, se encuentra la de cifrar los datos personales y mantenerlos solo por el tiempo que sea necesario de acuerdo con la finalidad especifica. Así mismo se resaltan algunas sugerencias que pueden aplicar para el uso de drones, como hacer una evaluación de impacto con los sistemas de vigilancia respecto de la intimidad de las personas. En esa misma línea, se propone diseñar políticas y protocolos para la atención de peticiones, consultas y reclamos presentados por los titulares en el manejo de datos.

En lo relativo a la seguridad de la información, es preciso tener en cuenta que, al incorporar el dron un sistema de información, este lleva a todo tipo de riesgos y vulnerabilidades. Los fallos pueden presentarse tanto en el dron como en el software que lo controla. Es así como ya se utiliza el término "*hacking* drones" en los distintos grupos de seguridad de la información, proyectos, *papers* o drones que incorporan temas de *hacking* y seguridad.

Por ejemplo, en el año 2018 investigadores de la firma de seguridad Chek Point descubrieron un fallo en la plataforma de drones DJI, la cual es usada para controlar los drones del fabricante. Según el informe de la firma de ciberseguridad y de acuerdo con el Bug Bounty Program de DJI, ciberatacantes podrían haber obtenido acceso a la cuenta de un usuario a través de una vulnerabilidad en el proceso de identificación en el foro de DJI, una comunidad ***online*** patrocinada por la marca para debatir sobre sus productos. Los usuarios de DJI que habían sincronizado sus registros de vuelo, así como fotos y vídeos en los servidores de la nube de DJI, y los usuarios corporativos de DJI que usaron el software DJI FlightHub, que incluye una cámara en vivo, audio y vista de mapa, podrían haberse visto afectados por la vulnerabilidad (Europapress, 2018).

En Colombia es claro que en el uso de drones se pueden cometer los delitos informáticos señalados en la Ley 1273 de 2009. Es el caso de violación de datos personales, daño informático y acceso abusivo a sistema informático.

220. Disposición 20/2015 del 27 de mayo de 2015, sobre uso de datos con drones, disponible en http://www.jus.gob.ar/media/2898655/disp_2015_20.pdf.

221. Decreto 1377 de 2013, artículos 14 y 15. El Decreto 1377 de 2013, está recogido en el artículo 2.2.2.25 del Decreto Único Reglamentario 1704 de 2015.

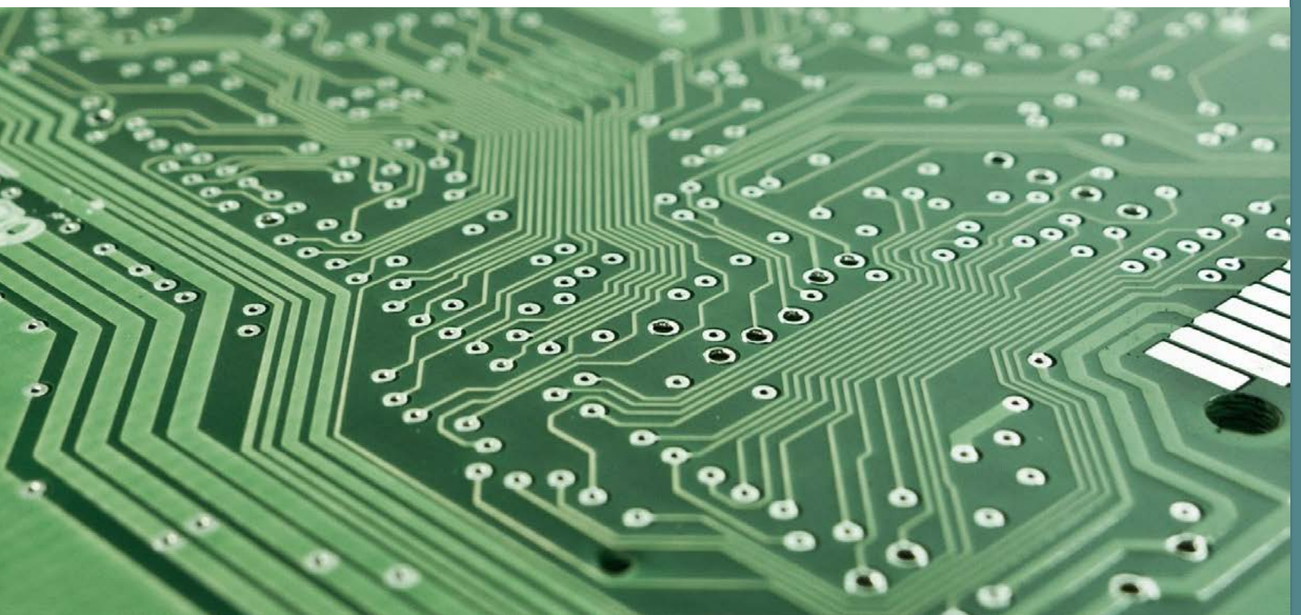
222. Superintendencia de Industria y Comercio, concepto con radicación 18-1712591, disponible en http://www.sic.gov.co/sites/default/files/normatividad/082018/Rad-180171259TratamientoDatosSensibles.pdf.

Existen muchas investigaciones donde profesionales de seguridad han ***hackeado*** drones con fines investigativos y académicos. En particular, en el evento de ***hackers*** Black Hat Asia 2016 el investigador Nils Rodday presentó y publicó su investigación titulada ***Hacking a Professional Drone***, en la cual muestra el proceso para ***hackear*** y tomar el control de un dron, teniendo en cuenta que estos elementos utilizan protocolos de comunicación como wifi y sistemas operativos que pueden tener vulnerabilidades (Rodday, s.f.).

Recomiendo el libro ***Un dron indetectable***, del español David Meléndez, presentado en una ponencia en Black Hat Usa 2018 en donde mostró su proyecto denominado Interceptor, el cual convierte un dron pequeño en una herramienta indetectable en software. El ingeniero explicó que ***"el dron funciona con wifi en su modo normal. Pero no crea una red como los demás drones, o como la red de nuestras casas, sino que los datos viajan a través de los mensajes que los routers usan para anunciar su propia red"*** (Cid, 2018).

El ingeniero también es autor del libro ***Hacking con drones***, de la editorial Oxword, donde se muestra una visión desde el aspecto tecnológico y técnico del mundo de los drones. Además de tratar los aspectos de software, algoritmos, control automático, hardware, sensores, electrónica y potencia, se hace referencia a la telemetría, las comunicaciones y la seguridad —tanto física como lógica— de los drones. El libro deja claro que todo software y hardware puede ser vulnerable y que los retos de los profesionales de seguridad es entender y mitigar los riesgos con el uso de drones.

De manera pues que la privacidad y la seguridad de la información desafían el uso de drones. Son retos frente a los cuales trabajan firmas de seguridad, entidades estatales, agencias de protección de datos y profesionales de la seguridad con miras a hacer esta tecnología más segura y dar pautas y recomendaciones en el uso y gestión de drones a nivel personal y empresarial.



Conclusiones

El límite ya no es el cielo. Si Ícaro o los hermanos Wright conocieran los drones, estarían sorprendidos; el dron y los robots son el símbolo de una nueva generación donde todo es posible. La transformación digital en los últimos años ha llevado a diversos cambios y hemos pasado de una tercera ola, anunciada por Alvin Toffler (1980), a una ola de automatización de diversos procesos. Desde una perspectiva normativa, a los 20 años de la Ley 527 de 1999, es claro el cambio importante introducido por esta norma, cuyas definiciones de comercio electrónico, sistemas de información, mensaje de datos, firma electrónica y firma digital han tenido su máxima expresión con el desarrollo de la tecnología.

Tuve la oportunidad de participar para el Gobierno colombiano en dos de los proyectos de regulación de iniciativas cero papel, así como en la redacción de varias normas sobre el uso de tecnología en relación con la Ley 527 de 1999, entre ellas el Decreto 2609 de 2012 del Archivo General de la Nación, en donde incorporamos a los tipos de información el uso de tecnologías en la nube en su artículo número 2[223]. Una de las conclusiones en todos estos proyectos es que el desarrollo tecnológico es imparable y que instrumentos como la Ley 527 de 1999 o de comercio electrónico todavía se siguen aplicando, ya que dan validez jurídica y probatoria al uso de mensaje de datos a distintas actividades del ser humano.

La Ley 527 de 1999 es un instrumento perfecto ya que hace una unión entre la tecnología y el componente del equivalente funcional por medio del mensaje de datos, el cual se encuentra en todo tipo de sistemas de información que funcionan en la actualidad. La tecnología va mucho más rápido que el derecho y la regulación; por lo tanto, el aporte de normas como la Ley 527 es muy grande ya que se adelantan al tiempo en temas de innovación, definición y transformación digital.

Nuestro consentimiento es expresado por mensaje de datos, desde el momento en que nos levantamos y enviamos un mensaje por WhatsApp o una red social hasta el simple proceso de pedir un vehículo por la aplicación Uber. Nuestro mundo actual funciona con mensajes de datos, y en muchos casos les damos fortaleza técnica con el uso de firmas digitales y electrónicas. La firma electrónica también toma un papel especial con su introducción con el Decreto 2364 de 2012[224], ya que métodos como códigos, contraseñas, datos biométricos o claves criptográficas, que permiten identificar a una persona, son utilizados de forma simple por todo tipo de tecnologías, entre ellas los robots y los drones o UAS. Tal como se desarrolló en el artículo, son varios los retos del comercio electrónico; entre ellos se encuentran la regulación, la privacidad, la seguridad, el uso de drones, la ocupación del espacio aéreo por los drones y su interacción con la aviación civil, así como todo lo que implica la automatización desde el nivel técnico y jurídico.

Hace unos años la regulación no daba cabida a tener drones en los cielos con propósitos empresariales. Sin embargo,

223. Decreto 2609 de 2012, en donde se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

224. Decreto 2364 de 2012, por el cual se impulsa la firma electrónica en Colombia y reglamenta el artículo 7 de la Ley 527 de 1999.

en la actualidad las nuevas normas están dejando opciones para los proyectos de investigación que en pocos años serán empresas o servicios de entidades públicas y privadas. En el 2019 incluso ya entró en operación la nueva norma colombiana de la Aeronáutica Civil, Resolución 04201 de diciembre 27 de 2018 de la Aeronáutica Civil, sobre el uso de drones o UAS, que deja la puerta abierta en su categoría C para que en algún momento se autorice el uso de esta tecnología para el transporte o comercio electrónico en Colombia, algo que hace unos años era imposible de conceder para las autoridades aeronáuticas. De cualquier forma, en las categorías A y B de la norma muchas empresas tienen la posibilidad de hacer pruebas y desarrollar proyectos de investigación con el uso de drones.

Para el transcurso del 2019 la empresa española DroneXservices ya tiene autorizado un permiso para trabajos específicos de inspección de infraestructuras, topografía y otros con RPAS en áreas en las que hasta hoy no era posible, como aquellas ciudades en las que hay un aeropuerto (Sorribas, 2019). Esto la convierte en la primera empresa en España en tener una autorización de este tipo.

Mientras tanto, en Colombia, varias empresas con las cuales trabajo ya vienen desarrollando proyectos de comercio electrónico y drones, y estoy seguro de que en poco tiempo estarán ofreciendo servicios a nivel empresarial. En el caso de la automatización y uso de robots para el comercio electrónico, ***startups*** colombianas como Kiwi, que empezaron con el uso de mensaje de datos, han evolucionado al uso de robots, con operación en distintas ciudades de Estados Unidos[225], lo que deja claro que estamos en una revolución del comercio electrónico, que inició con la concepción y aplicación de la Ley 527 de 1999, la cual cumple 20 años de introducir una trasformación digital para Colombia.

La ley modelo de Uncitral, introducida por medio de la Ley 527 de 1999, abrió las puertas para un mundo sin fronteras, para un mundo de una transformación digital sin precedentes y cuyo futuro inmediato es la innovación, la inmediación y la automatización de todos los procesos humanos. El comercio electrónico actual hace que las personas quieran el producto ideal en el momento adecuado, y que comprar un producto o realizar alguna interacción se conviertan en una experiencia. Los drones o robots crean hoy esas experiencias únicas que son requeridas por nuestras generaciones actuales, las cuales basan su economía en metodologías ***startup***, como lo muestra el libro ***Lean startup***, de Eric Ries, y que se definen en tres simples pasos: crear, medir y aprender. En unos años tu almuerzo te llegará en un dron, y para tus hijos será algo normal.

225. Según https://www.kiwicampus.com.

Bibliografía

BBC Mundo. (2017). ¿Está tu profesión en peligro de extinción? [En línea]. Recuperado de https://www.bbc.com/mundo/noticias-38930099.

BBC Mundo. (2018). A dónde se dirige el auto Tesla lanzado al espacio por SpaceX en el cohete Falcon Heavy (y por qué no durará miles de años como dijo Elon Musk). [En línea]. Recuperado de https://www.bbc.com/mundo/noticias-42981121.

Bustamante, Nicolás (2017). Conozca a Kiwi, el robot repartidor del futuro. [En línea]. Recuperado de https://www.eltiempo.com/vida/ciencia/emprendedores-colombianos-desarrollan-kiwi-robot-repartidor-de-domicilios-158040.

Cambridge Consultants. (2017). The future of drone delivery. [En línea]. Recuperado de https://www.cambridgeconsultants.com/press-releases/future-drone-delivery.

Caraher, Lee (s.f.). Millenials en la oficina. Grupo Planeta.

Carbajal, Braulio (2017). Frank Wang soñó con el cielo y se transformó en millonario. [En línea]. Recuperado de https://www.milenio.com/negocios/frank-wang-sono-cielo-transformo-millonario.

Cid, Guillermo (2018). Este joven ingeniero zaragozano ha creado un dron casero prácticamente indetectable. [En línea]. Recuperado de https://www.elconfidencial.com/tecnologia/2018-08-21/drones-indetectables-david-melendez-low-cost_1606298/.

Cortés, Helena (2018). Kiwi campus, la empresa de robots domiciliarios abrió sede en Medellín. [En línea]. Recuperado de https://www.elcolombiano.com/tecnologia/este-robot-colombiano-lleva-burritos-a-domicilio-MY9274428.

Deusto (2018). Un análisis a los riesgos del uso de drones. [En línea]. Recuperado de https://blogs.deusto.es/master-informatica/un-analisis-a-los-riesgos-del-uso-de-drones/.

EFE. (2018). Así es la nueva normativa de drones en España. [En línea]. Recuperado de https://www.20minutos.es/noticia/3229653/0/drones-nueva-normativa/.

EFE. (2019). El robot colombiano que promete revolucionar el servicio en hoteles. [En línea]. Recuperado de https://www.portafolio.co/negocios/empresas/el-robot-colombiano-que-promete-revolucionar-el-servicio-en-hoteles-529490.

Europapress (2018). Fallo de seguridad en la plataforma y la aplicación de drones DJI. [En línea]. Recuperado de https://www.eltiempo.com/tecnosfera/dispositivos/falla-de-seguridad-en-aplicaciones-de-drones-dji-291542.

Martínez, Cristina y Peláez, Juan (2015). Principales retos de ciberseguridad en drones (Parte I). [En línea]. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/ciberseguridad-drones.

Meléndez, David (s.f.). Hacking con drones. Love is in the air. Editorial Oxword.

OACI (2018). La Secretaria General de la OACI destaca las prioridades de la gestión de un espacio aéreo seguro y armonizado para las aeronaves no tripuladas y los drones. [En línea]. Recuperado de https://www.icao.int/Newsroom/Pages/ES/ICAO-Secretary-General-stresses-safe-and-harmonized-airspace-management-priorities-for-unmanned-aircraft-and-drones.aspx.

Ries, Eric (2018). El método Lean Startup. Cómo crear empresas de éxito utilizando la innovación continua. Editorial Planeta.

Rodday, Nils (s.f.). Hacking a Professional Drone. [En línea]. Recuperado de https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf.

Russell, John (2019). China's JD.com tests drone delivery in Indonesia in first overseas pilot. [En línea]. Recuperado de https://techcrunch.com/2019/01/22/jd-drone-indonesia/.

Sorribas, Borja (2019). Volar drones en espacio aéreo controlado empieza a ser una realidad en España. [En línea]. Recuperado de https://www.todrone.com/dronexservices-volar-drones-espacio-aereo-controlado-realidad-espana/.

Superintendencia de Industria y Comercio (s.f.). Guía de protección de datos personales en sistemas de videovigilancia.

Toffler, Alvin (1980). La tercera ola. Plaza & Janes Editores.

Vance, A. (2017). Elon Musk, El creador de Tesla, Paypal y SpaceX que anticipa el futuro. Colombia: Editorial Planeta.

Víctor Delgado (s.f.). Historia de los drones. [En línea]. Recuperado de http://eldrone.es/historia-de-los-drones/.

Wikipedia (s.f.). Parrot AR.Drone. [En línea]. Recuperado de https://es.wikipedia.org/wiki/Parrot_AR.Drone.

Xataka (2015). DJI, la empresa líder en drones es china y no copia a nadie. [En línea]. Recuperado de https://www.xataka.com/drones/dji-la-empresa-lider-en-drones-es-china-y-no-copia-a-nadie.

Xataka (2018). Quién es quién en el proyecto Hyperloop: cómo es y quién trabaja en el transporte futurista de Elon Musk. [En línea]. Recuperado de https://www.xataka.com/vehiculos/quien-quien-proyecto-hyperloop-como-quien-trabaja-transporte-futurista-elon-musk.

Jurisprudencia

Ley 527 del 21 de agosto de 1999, 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.

Decreto 2364 de 2012, por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999.

Decreto 1377 de 2013, artículos 14 y 15. El Decreto 1377 de 2013 está recogido en el artículo 2.2.2.25 del Decreto Único Reglamentario 1704 de 2015.

Circular reglamentaria 5100-082-002 de 2015, de la Aeronáutica Civil.

Resolución 04201 del 27 de diciembre de 2018 de la Aeronáutica Civil.

Disposición 20/2015 del 27 de mayo de 2015, norma argentina sobre uso de datos personales con el uso de drones.

Decreto 1008 del 14 de junio de 2018, por medio del cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

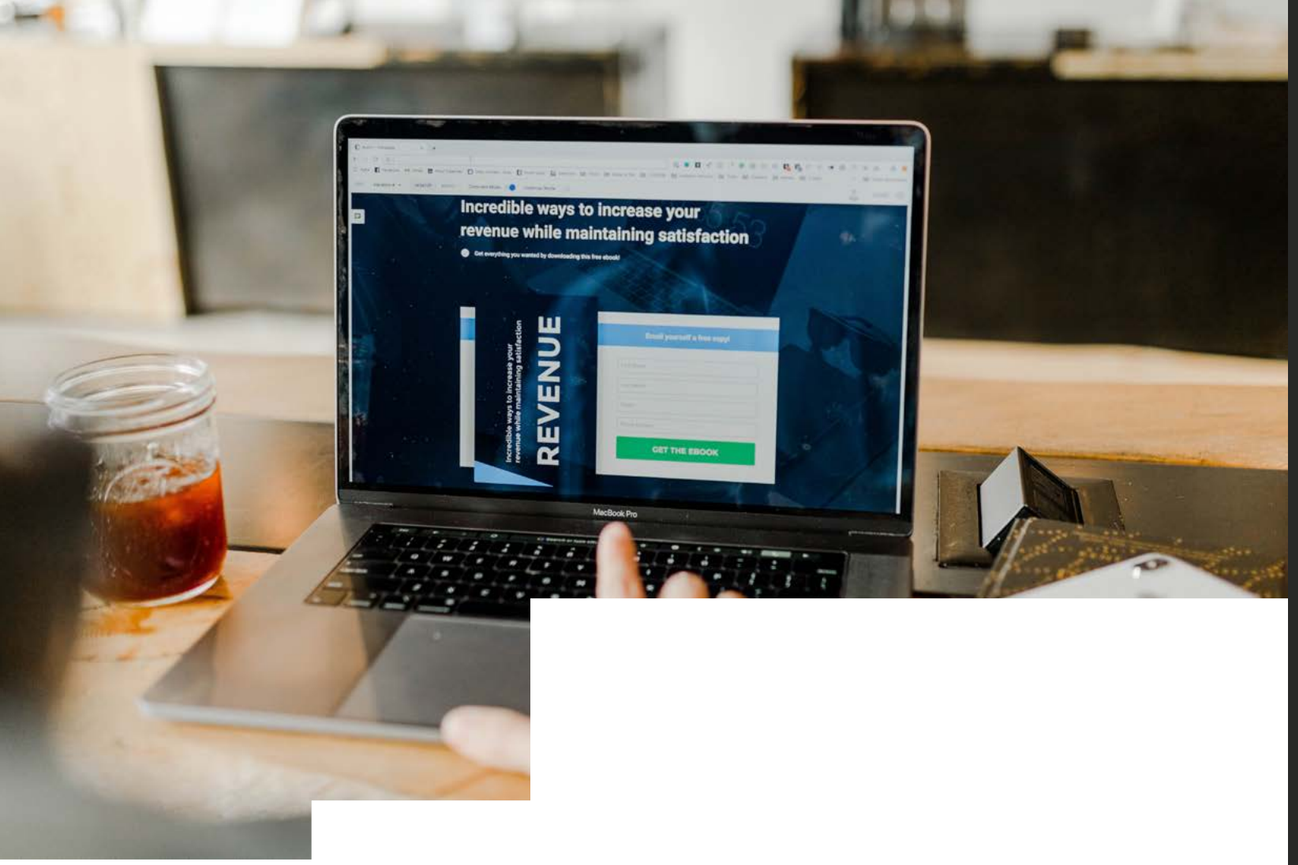
EL FUTURO DE LOS PAGOS DIGITALES

Juan Sebastián Peredo

Resumen

Los sistemas de pagos están constantemente en evolución, con modificaciones, cambios e introducciones de medios de pago e instrumentos utilizados. Todo esto repercute en los hábitos de consumo de las personas y en las formas en que estas toman la decisión de adquirir bienes y servicios y de realizar transferencias. Por lo tanto, es importante analizar la estructura actual de los sistemas de pagos y analizar los fenómenos que están ocurriendo y que podrán ocurrir en el futuro.
Dentro de los muchos fenómenos que componen la evolución de los sistemas de pagos, este capítulo busca explorar, a la luz el sistema actual, la adaptación que se ha tenido en materia de billeteras digitales/monederos electrónicos y la irrupción de los criptoactivos en el mundo de los pagos. De manera general, se evidencia, como ha sido expuesto por el Regulador colombiano, una necesidad de actualización de la normativa que rige los sistemas de pagos de manera que las entidades y los consumidores puedan verse beneficiados en tiempo y costos. Teniendo en cuenta lo anterior, este capítulo busca discutir el sistema de pagos actual en Colombia, la utilización de billeteras digitales y la influencia de los criptoactivos en los sistemas de pagos.

Palabras clave: pagos; criptoactivos; billeteras digitales.



Abstract

Payment systems are constantly evolving, with modifications, changes and introductions of payment methods and instruments. All this, with an impact on people's consumption habits and the ways in which persons acquire goods and services and transfer money. Therefore, the importance of analyzing the current structure of payment systems and analyze the phenomena occurring and that may occur in the future. Within the many phenomena that compose the evolution of payment systems, this chapter seeks to explore, at the light of the current system, the adaptation that has been made regarding digital wallets and the emergence of cryptoassets in the payments' systems. In general, it is evident, as has been stated by the Colombian regulator, a need to update the regulations governing payment systems so that entities and consumers can benefit from time and costs. Given the above, this chapter seeks to analyze the current payment system in Colombia, the use of digital wallets and the influence of cryptoassets in payment systems.

Key words: payments; cryptoassets; digital wallets.

Introducción

Los sistemas de pagos[226] en Colombia, y en general en el mundo, están constantemente en evolución. Por este motivo, hablar sobre el futuro de los pagos digitales puede resultar una misión imposible. Esta evolución es evidente en la medida en que los medios de pago y los instrumentos utilizados cambian, y esto impacta en los hábitos de consumo de las personas. Estos cambios, a diferencia de otros en el mundo financiero que parecen imperceptibles, son del todo evidentes para los consumidores por cuanto los separan del arraigo que han desarrollado con algunos medios e instrumentos de pago y los llevan a la utilización de nuevas herramientas. Para los consumidores es palpable que, donde utilizaban efectivo para realizar pagos, ahora utilizan tarjetas de crédito; donde sacaban una chequera, ahora realizan una transferencia electrónica; donde firmaban un ***voucher,*** ahora acercan un celular para leer un código QR[227]. Los medios y los instrumentos de pago han ido cambiando y, de una manera un poco menos perceptible, los sistemas de pago han tenido que ajustarse a la nueva realidad y dinamismo con el que las personas quieren realizar sus transacciones.

La evolución de los sistemas de pagos, hasta recientemente, ha estado arraigada en las instituciones financieras tradicionales, quienes han sido las llamadas a adaptarse, a proponer los nuevos instrumentos, a competir de esta manera con otras entidades. Las instituciones financieras han tenido que tomar pasos hacia la digitalización de sus productos y servicios (Unidad de Proyección Normativa y Estudios de Regulación Financiera, 2018), respondiendo a las exigencias del mercado, a la inmediatez y virtualidad que la nueva generación de clientes exige y continuará exigiendo. No ha sido tarea fácil porque, a diferencia de las empresas emergentes, las instituciones financieras tradicionales no tenían en la cabeza a la tecnología como el centro de su negocio (Buckley y Mas, 2016) y, por lo tanto, cualquier evolución en sus sistemas de pagos estaba directamente relacionada con el funcionamiento y funcionalidad de sus instrumentos existentes.

Ahora bien, lo que en algún momento se pensaba que era de la esfera única y exclusiva de las entidades financieras y del sector financiero existente y arraigado (definido por los anglosajones como ***incumbent***), es ahora capital de los desarrolladores de nuevas tecnologías y de las empresas de pagos emergentes que, sin aferrarse a ideas preconcebidas de cómo debe funcionar un sistema de pagos, han tomado la iniciativa de crear nuevos ambientes de pagos y de transaccionalidad. Esto genera que nazcan nuevos medios e instrumentos de pago y que en el centro de estos se encuentre la inmediatez[228] de las transacciones. Estas nuevas tecnologías y formas de relacionarse con los consumidores y sus necesidades han dado pie a la reforma de los sistemas de pago, al surgimiento y utilización de otros mecanismos como billeteras digitales y de nuevos instrumentos como los criptoactivos.

226. De acuerdo con el Banco de la República, *"Los sistemas de pagos son aquellos que se utilizan para realizar transacciones financieras mediante la transferencia de valor monetario. Incluyen instituciones, personas, reglas, procedimientos, estándares y tecnologías que hacen que estos intercambios sean posibles"* (Banco de la República, 2018). Según el artículo 2.17.1.1.1 del Decreto 2555 de 2010, sistema de pago *"Es un conjunto organizado de políticas, reglas, acuerdos, instrumentos de pago, entidades y componentes tecnológicos, tales como equipos, software y sistemas de comunicación, que permiten la transferencia de fondos entre los participantes, mediante la recepción, el procesamiento, la transmisión, la compensación y/o la liquidación de órdenes de transferencia y recaudo"*.

227. Quick Response.

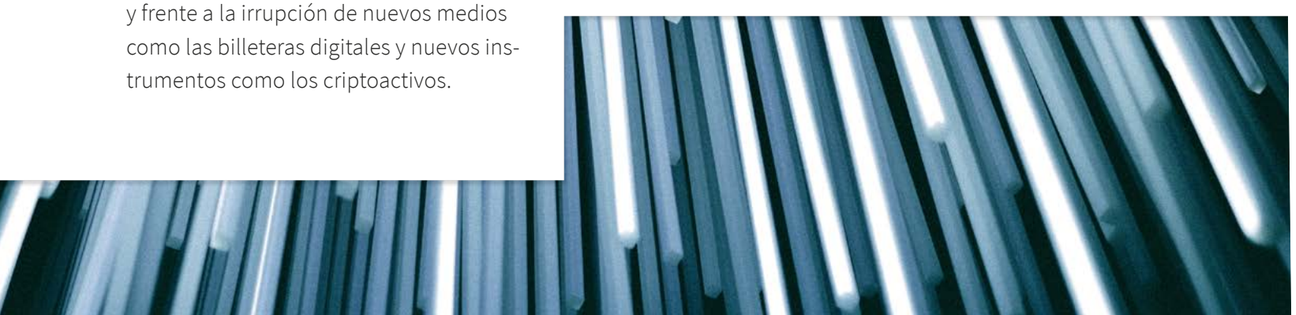
228. Inmediatez tanto en la verificación del pago como en la recepción de este.

Los reguladores alrededor del mundo, y por supuesto en Colombia, han tenido que responder al avance de la tecnología y de los sistemas de pagos. De tajo, se entiende como dado que la evolución hacia sistemas de pagos digitales genera un mayor bienestar en la población y promueve la inclusión financiera (Unidad de Proyección Normativa y Estudios de Regulación Financiera, 2018), derribando barreras por el uso del efectivo y promoviendo la bancarización de las personas. La tarea, en materia de pagos y específicamente de pagos digitales, ha pasado por crear un ambiente de interconexión e interoperabilidad que permita que los diferentes actores, medios e instrumentos de pago tengan un relacionamiento fluido, eficiente y con menores costos. La seguridad sigue siendo un asunto fundamental, pero la experiencia de usuario, la competencia y la inmediatez de las transacciones han tomado mayor relevancia.

El reto al que se enfrenta cualquier regulador que desea darles una nueva forma a los sistemas de pagos de su país pasa por crear un ambiente que permita la inclusión de nuevos actores, medios y tecnología, que preserve la seguridad para los usuarios y que incentive la incorporación de nuevos desarrollos. En el caso colombiano, sin perjuicio de un grandioso número de variables que se podrían analizar, consideramos que inicialmente se puede plantear una discusión respecto de las problemáticas y soluciones frente al sistema de pagos actualmente concebido y frente a la irrupción de nuevos medios como las billeteras digitales y nuevos instrumentos como los criptoactivos.

En todo caso, el desarrollo del sistema de pagos pasa por afrontar las dificultades actuales en términos de acceso a este por parte de nuevos actores y de interconexión entre estos actores y las entidades "incumbentes". Esto implica, como se verá más adelante, cambios regulatorios en la concepción e infraestructura del sistema de pagos. Así mismo, el desarrollo de nuevos ambientes de pagos, parcial o totalmente desvinculados del sistema de pagos existente, afronta limitaciones regulatorias y legales que han obligado a una vinculación de estos nuevos ambientes con los productos y servicios ofrecidos por las entidades financieras (no necesariamente siguiendo la práctica de otros países, pero como consecuencia de las limitaciones que se desarrollarán más adelante). Por último, la irrupción de los criptoactivos, como un nuevo instrumento para el pago de bienes y servicios y como mecanismo de transferencia tiene que tener un rol preponderante en la identificación de nuevos mecanismos alternativos a los sistemas de pago actuales.

Por esta razón, a través de este capítulo nos enfocaremos en tres asuntos que dan cuenta del presente y futuro de los pagos digitales: (i) frente al sistema de pagos actual en Colombia; (ii) en relación con la digitalización de los instrumentos en las billeteras digitales; y (iii) frente al surgimiento de nuevos instrumentos como los criptoactivos. Finalmente, llegaremos a unas conclusiones respecto de todos estos.



01

Consideraciones frente al sistema de pagos actual en Colombia

El sistema de pagos en Colombia no ha sido objeto de modificaciones sustanciales en los últimos años, desde el punto de vista jurídico. Las normas que lo regulan se han mantenido, en mayor o menor medida, iguales. Sin embargo, la irrupción de un nuevo tipo de entidades no financieras ha hecho que el sistema de pagos colombiano sufra un acomodamiento que ha permitido la multiplicación del número de comercios y personas que han accedido a los pagos digitales en Colombia. Estas entidades han tomado el nombre de pasarelas de pagos (llamadas por la Superintendencia Financiera entidades administradoras de pasarelas de pagos). Esta irrupción de nuevas entidades, en todo caso, no ha modificado el sistema de pagos como legalmente se encuentra concebido y simplemente ha incorporado un actor que permite la vinculación de un mayor número de usuarios en el sistema de pagos como actualmente existe, apalancándose en las normas que rigen actualmente los sistemas de pagos.

Para efectos de poder dar unos comentarios respecto del futuro del sistema de pagos "incumbente" en Colombia, es necesario, así sea de manera sumaria, explicar cómo funciona y qué actores intervienen.

En la normativa colombiana se encuentra planteada una diferenciación de los roles que cada entidad desarrolla en el sistema de pagos colombiano. Esta definición en los roles es, de alguna manera, estricta y por tal razón la visión reciente del Regulador de realizar una modificación frente a ella. De manera general, podemos decir que en Colombia existen entidades emisoras, entidades adquirentes y entidades que se encargan de la compensación y liquidación de las operaciones.

A manera de ejemplo, y con el fin de escenificar la ruta de un pago en Colombia, podemos utilizar el pago de una operación de comercio electrónico, en la cual un consumidor le paga a un comercio por bienes que adquirió en la página ***web*** del comercio (en esta primera parte del ejemplo no utilizaremos pasarelas de pago). Para que el comercio acepte el pago a través de su página ***web***, será necesario que cuente con un establecimiento de crédito adquirente que, de manera general, actuará como el banco que recaudará los montos que le sean pagados al comercio. Por ser una transacción electrónica, esta relación se generará a través de una cámara de compensación automatizada[229] (en el caso de Colombia, la institución que se encargaría de esta operación en particular sería ACH Colombia[230]). En este sentido, el comercio estará vinculado a su entidad adquirente y al sistema de compensación y liquidación.

Una vez iniciada la operación, la red dirigirá al consumidor a la página ***web*** del establecimiento de crédito (o SEDPE[231]) emisor (es

229. Las cámaras de compensación automatizada reciben su nombre de la traducción de ***Automated Clearing House*** (ACH). Por su parte, las cámaras de compensación automatizadas son *"un sistema de compensación electrónico en el cual las órdenes de pago son intercambiadas entre instituciones financieras, principalmente a través de medios magnéticos o redes de telecomunicaciones, y son administradas por un centro de procesamiento de datos".*

230. ACH Colombia S.A., sociedad administradora de sistema de pago de bajo valor.

231. Sociedades especializadas en depósitos electrónicos.

decir, de la entidad con la que el consumidor tiene el medio de pago) para autorizar el débito de su cuenta. Recibida la autorización, esta será comunicada a través de la red al comercio, el cual podrá proceder con la entrega del producto por cuanto la operación se entenderá que ha sido aprobada.

Sin embargo, el comercio aún no habrá recibido los recursos de la compra. Una vez autorizado el débito de la cuenta del consumidor, la operación se dirigirá a la cámara de compensación automatizada para que se realice la compensación y liquidación. Esto implica que la cámara de compensación recibirá el cúmulo de transacciones realizadas entre adquirentes y emisores y, de acuerdo con determinados ciclos intradía, ordenará los pagos netos entre unos y otros. Todo este proceso llevará a que el comercio que realizó la venta pueda recibir los recursos objeto de ella a través de su cuenta de adquirencia con la entidad adquirente.

Al analizarse este tipo de estructura para la realización de operaciones de comercio electrónico, la conclusión inicial a la que se puede llegar es que la vinculación de un comercio al sistema de pagos puede ser compleja y no resultar costo-eficiente. El comercio tiene que celebrar múltiples contratos para poder vincularse al sistema de pagos, y estos múltiples contratos generarán tarifas que el comercio (y el consumidor) deberá pagar para efectos de que una transacción pueda realizarse a través de su página ***web***. Los pagos se deberán realizar a lo largo de la cadena: pagos de acceso a la red, comisiones de adquirencia[232], tarifa interbancaria de intercambio[233], cuotas de manejo[334]. Todos estos costos asociados a una transacción hacen que esta no sea costo-eficiente e impida el acceso de un mayor número de comercios y consumidores al comercio electrónico. A esto se deben sumar los costos relacionados con los desarrollos de tecnología que tienen que adelantar los comercios para aceptar los pagos electrónicos a través de sus páginas ***web***.

El relacionamiento contractual complejo descrito hace que la vinculación de nuevos comercios sea difícil y que, en el caso de comercios con volúmenes mínimos de transaccionalidad, sea cercana a imposible. Sin embargo, el surgimiento de las pasarelas de pago ha permitido gestionar de mejor manera la relación entre los comercios y las entidades que hacen parte del sistema de pagos (simplificando el relacionamiento contractual entre unos y otros). En todo caso, las pasarelas de pago, como lo mencionábamos anteriormente, no son ajenas al sistema de pagos y, por el contrario, se vuelven parte de él, fungiendo como un facilitador entre este y el comercio.

Las pasarelas de pagos, de acuerdo con los servicios que proveen, han sido clasificadas como "***gateway***" y "agregadoras". Esta clasificación no tiene un origen legal, pero ha servido para entender los roles que pueden asumir dentro del sistema de pagos. Las ***gateway***, que podrían entenderse como el modelo más sencillo, proveen una solución tecnológica a los comercios (y en algunos casos servicios adicionales de conocimiento de cliente) para efectos de que sus transacciones puedan dirigirse o "enrutarse" hacia la cámara de compensación y liquidación. El proceso, en adelante, es el mismo que se llevaría a cabo sin la participación de una pasarela de pagos, con una leve diferencia, y es que el comercio recibirá de la pasarela de pagos la notificación de que la transacción ha sido aprobada por la entidad emisora. En este sentido, el comercio tendrá que seguir gestionando la vinculación con una entidad adquirente (la comisión de adquirencia, por lo tanto, estará a su cargo).

Por su parte, las pasarelas de pagos agregadoras proveen un servicio adicional y relevante al comercio, el cual consiste en que este no tendrá que vincularse a la red y a un establecimiento de crédito adquirente directamente por cuanto esto lo realizará la pasarela de pagos. La pasarela de pagos negociará independientemente una relación de adquirencia con el establecimiento de crédito y recibirá, a través de su cuenta de adquirencia, los pagos de múltiples comercios por múltiples operaciones, los cuales "agrega" y posteriormente dispersa a favor de los respectivos comercios. En este sentido, la comisión de adquirencia será la que negocie la pasarela de pagos con la entidad adquirente. De esta manera, el servicio de la pasarela de pagos agregadora será, además del desarrollo tecnológico y servicio de enrutamiento hacia la red, la agregación de los pagos en la cuenta adquirente de la pasarela de pagos, para su posterior transferencia al comercio.

Como se puede evidenciar, el rol de las pasarelas de pagos ha sido permitir que los comercios puedan aceptar pagos digitales para la compra de sus productos y servicios. Sin embargo, esta función de ninguna manera ha modificado realmente el sistema de pagos en Colombia. Los mismos actores, adquirentes, emisores y entidades administradoras de los sistemas de compensación y liquidación siguen siendo necesarios.

La red, por lo tanto, se vuelve compleja y de alguna manera estática. De la manera como se encuentra planteada jurídicamente en este momento, es difícil pensar en escalarla de manera que sea más eficiente y permita la vinculación de más comercios y de más consumidores. El rol de las pasarelas de pago, ***gateway*** y de agregación, ha sido muy valioso para permitir el acceso a la red de nuevos comercios. Sin embargo, más allá de estos nuevos actores, la aceptación de pagos electrónicos por parte de comercios está ligada a una serie de costos que se añaden por los diferentes eslabones de la red, tal y como se encuentra diseñada. Los costos arriba mencionados (costos de acceso a la red, comisión de adquirencia, tarifa interbancaria de intercambio y comisión de manejo) seguirán existiendo. Para el caso de comercios que no están en la capacidad de vincularse directamente a la red y a una entidad adquirente, tendrán que recurrir a una pasarela de pagos agregadora, quien a su vez cobrará una comisión por el servicio que presta.

Por lo tanto, si bien la llegada de las pasarelas de pago al sistema de pagos colombiano ha dado pie al acceso de más comercios, el esquema de funcionamiento de este no ha cambiado y puede dificultar el acceso de nuevos comercios y consumidores y el desarrollo de nuevas tecnologías que, apalancadas en el sistema, permitan la profundización del sistema de pagos digital en Colombia. Este tipo de dificultades no es exclusivo de Colombia y se ha presentado en diferentes jurisdicciones, las cuales han modificado sus sistemas de pagos de maneras muy distintas las unas de las otras para permitir el desarrollo de estos y la profundización en la utilización de mecanismos digitales en la gestión de pagos y transferencias.

Los pagos digitales, entonces, están actualmente limitados por un sistema que tiene

232. Comisión cobrada por las entidades adquirentes a los propietarios de los establecimientos de comercio en los cuales los tarjetahabientes realizan adquisiciones con tarjetas débito o crédito (artículo 2.1.4.1.1 del Decreto 2555 de 2010).

233. Comisión a favor de las entidades emisoras y a cargo de las entidades adquirentes (artículo 2.1.4.1.1 del Decreto 2555 de 2010).

234. Comisión cobrada por las entidades emisoras a los tarjetahabientes (artículo 2.1.4.1.1 del Decreto 2555 de 2010).

una serie de "peajes" que se tienen que cruzar, que implican unos costos asociados y que restringen la participación u operación de nuevos participantes. El Regulador en Colombia ha planteado abordar este asunto desde una perspectiva de definición de las actividades, más que de los actores, de manera que se permita la inclusión de nuevos jugadores en algunos de los eslabones de la cadena. Estos jugadores (y no nos referimos a las pasarelas de pago), presumimos, estarán sometidos a la vigilancia de la Superintendencia Financiera de Colombia.

El plantea miento de abordar el problema a partir de la definición de actividades podría ser complementado por la descripción de estas actividades, pero no por la circunscripción del desarrollo de estas por parte de determinadas entidades financieras. Por el contrario, la evolución del marco legal del sistema de pagos podría comprender el desarrollo de este tipo de actividades, cumpliendo ciertos estándares, por diferentes actores de la industria, sin que estos tengan que ser necesariamente entidades vigiladas.

La solución de muchos de los asuntos que hemos venido mencionando parte de la apertura de los sistemas de pago a nuevos actores y nuevas tecnologías. Esto no implica el reemplazo de las redes existentes, sino, por el contrario, el apalancamiento en estas, sin perder de vista la oportunidad de simplificación que se deriva de los desarrollos tecnológicos.

Un asunto clave que se discutirá y que tomará forma regulatoriamente en el futuro será la definición de nuevos actores (sin necesariamente limitarlos a un tipo definido de entidades) que puedan realizar la actividad de adquirencia, permitiendo que entidades diferentes a las que actualmente —por norma— pueden realizar esta actividad hagan parte de los sistemas de pago de bajo valor con esta calidad.

Como se ha visto, la adquirencia es uno de los ejes fundamentales para la vinculación de comercios y personas al sistema de pagos. Esto permitirá una reducción de los costos de vinculación al sistema, dadas la competencia y las economías de escala que probablemente se podrán explotar. Esta nueva definición de actores que podrán realizar la actividad de adquirencia tendrá que venir acompañada de reglas de juego y de gobierno corporativo claras que impidan que los sistemas "incumbentes" nieguen el acceso de los nuevos actores a los sistemas de pago. En este sentido, el rol de adquirencia debería abrirse a diferentes actores y, así mismo, a estos nuevos actores se les debe garantizar, a través de reglas claras (y no restrictivas), el acceso a los sistemas de pago actuales.

Ahora bien, una simplificación de los sistemas de pagos también podrá estar dada por la apertura de información desde las entidades "incumbentes" hacia las entidades emergentes. La apertura de API[235] por parte de las entidades financieras permite que, en un ambiente de pagos, las aplicaciones desarrolladas por empresas no financieras puedan obtener información y validación de datos en tiempo real que, de manera sencilla, evite que tenga que actuar todo un sistema de pagos en procura de validación de información para que se sepa, por ejemplo, que una cuenta ha sido debitada para el pago de una venta.

En Colombia, la apertura de API se ha venido dando de manera particular por las entidades financieras, sin requerimiento legal, y simplemente por el deseo de la entidad financiera de permitir el acceso, bajo ciertas condiciones y reglas, a terceras partes. Sin embargo, para que las API puedan tener un real efecto en un sistema de pagos, resulta necesario que estas se encuentren disponibles en las diferentes entidades que hacen parte de este y no solo en algunas. En algunos casos, la decisión ha sido la de obligar, bajo ciertas reglas, que las entidades den apertura a sus API para el acceso de terceros. Este no es el caso en Colombia, aun cuando en virtud de las discusiones del Regulador sobre ***open banking*** una medida de esta naturaleza o que regule la apertura de API puede acercarse a ser una realidad.

En particular, y en relación con el sistema de pagos actual, más que un pronóstico sobre lo que puede deparar el futuro, el Regulador debe propugnar para que el sistema de pagos esté preparado y no sea una barrera para la entrada de nuevos actores ni para la incorporación de tecnología que permita hacer más eficientes los procesos, donde así sea posible. Una nueva definición de los roles de los participantes dentro del sistema, una apertura para que estas actividades sean desarrolladas por más tipo de entidades y reglas claras de gobierno corporativo para garantizar el acceso a nuevos participantes son un punto de partida. La apertura de API, por su lado, continúa siendo una alternativa para, además de lo anterior, permitir mayores eficiencias y reducción de costos dentro del sistema.

235. Siglas en inglés de *Application Programming Interface*: *"son conjuntos de reglas que las aplicaciones pueden seguir para comunicarse entre ellas, sirviendo de interfaz entre programas diferentes"* (BBVA, 2018). Las API permiten la comunicación entre diferentes programas, accediendo y compartiendo información que permite evitar esquemas rígidos de verificación y que la verificación pueda pasar a ser inmediata.

02

Consideraciones respecto de las billeteras digitales

Por lo pronto, bajo la sombrilla del sistema de pagos actual se han desarrollado nuevos mecanismos para vincular los instrumentos de pago y para crear nuevos instrumentos de pago. En las primeras de toque, las billeteras digitales hicieron su aparición como un mecanismo a través del cual un usuario podía utilizar uno o varios de sus diferentes instrumentos de pago para efectos de realizar transacciones. Las billeteras digitales, bajo esta concepción, funcionan de una manera similar a una billetera tradicional en la que el usuario guarda los diferentes instrumentos de pago con los que cuenta, con lo cual logran una funcionalidad similar. Ahora bien, las billeteras digitales involucran y se enlazan con los instrumentos mediante encriptación y certificados digitales, con el fin de poder comunicarse de manera segura con los mecanismos de pago utilizados y con las entidades encargadas de ellos.

Por lo tanto, una billetera digital, en esta forma de entenderse, permitirá a un usuario incluir dentro de un mismo mecanismo digital varios de sus instrumentos de pago (digitales también) para efectos de que el usuario pueda recurrir a ellos en las operaciones electrónicas que desee realizar.

Bajo la definición de billeteras digitales o de monederos electrónicos han entrado otro tipo de servicios adicionales. Las normas respecto de la gestión de recursos en otras jurisdicciones han dado pie para que entidades no reguladas (es decir, que no requieren de una licencia o autorización por parte del Estado) puedan gestionar recursos de manera digital sin necesidad de vinculación, al menos directa, de instituciones financieras. Estas billeteras han permitido que, bajo esquemas ómnibus, las entidades no reguladas reciban recursos de sus usuarios con el fin de acreditar una billetera virtual mediante la cual podrán realizar pagos, transferencias y retiros. Los recursos, por su parte, son administrados en cuentas propias de la entidad no regulada, la cual se compromete contractualmente a segregarlos de sus recursos propios. Este tipo de nuevo servicio, del cual encontramos registro en otros países, tiene serias limitaciones en Colombia debido al delito de captación masiva y habitual de dineros del público[236].

Las normas sobre captación masiva y habitual de dineros del público, es decir, aquellas que nos dan los parámetros para entender en qué casos se presenta la captación masiva y habitual, han supuesto un impedimento para el desarrollo de este tipo de nuevos servicios bajo las billeteras digitales[237]. Esto se debe a que las normas de captación masiva y habitual definen este delito de una manera que no permite dar viabilidad, al menos en su forma más cruda, al servicio como se plantea en otros países. A manera de resumen, se entiende que se presenta captación masiva y habitual[238] cuando una persona natural o jurídica se encuentra en alguno de los siguientes casos[239]:

a. Su pasivo con el público[240]está compuesto por obligaciones con más de veinte personas o por más de cincuenta obligaciones. Las obligaciones podrán haber sido contraídas directamente o a través de interpuesta persona[241].

b. Cuando de manera conjunta o separada haya celebrado en un periodo de tres meses consecutivos más de veinte contratos de mandato con el objeto de administrar dineros de sus mandantes: (i) bajo la modalidad de libre administración; o (ii) para invertirlos en títulos o valores a juicio del mandatario; o (iii) haya vendido títulos de crédito o de inversión con la obligación para el comprador de transferirle la propiedad de títulos de la misma especie, a la vista o en un plazo convenido, y contra reembolso de un precio[242].

La interpretación de estos casos hace ver de tajo que una billetera digital, en la cual se reciben recursos de terceros, gestionados y administrados directamente por la billetera digital, podrá entrar dentro de aquello que se entiende como captación masiva y habitual de dineros del público. En la medida en que una entidad no regulada pretenda administrar directamente recursos del público, superando los límites mencionados arriba, se podrá encontrar con el tipo de captación masiva y habitual de dineros del público.

Estas limitaciones, evidentes, han provocado una confluencia de intereses entre el sector financiero "incumbente" y las empresas emergentes, dada por el interés del primero de continuar en la profundización de la digitalización de sus servicios y en la atracción de nuevos clientes (muchos de ellos no bancarizados) y en el interés de las segundas de poder ofrecer servicios financieros regulados a sus clientes. Por lo tanto, muchas de las billeteras digitales que han tenido eco en Colombia han visto su fundamento en la alianza de entidades financieras y no financieras, vinculando productos regulados de las primeras a las plataformas de las segundas, con el fin de ofrecer un espectro más amplio de productos y servicios a favor de los usuarios.

236. *"Artículo 316. Captación masiva y habitual de dineros. El que desarrolle, promueva, patrocine, induzca, financie, colabore, o realice cualquier otro acto para captar dinero del público en forma masiva y habitual sin contar con la previa autorización de la autoridad competente, incurrirá en prisión de ciento veinte (120) a doscientos cuarenta (240) meses y multa hasta de cincuenta mil (50.000) salarios mínimos legales mensuales vigentes.*

Si para dichos fines el agente hace uso de los medios de comunicación social u otros de divulgación colectiva, la pena se aumentará hasta en una cuarta parte".

237. En el momento de escribir este capítulo, la URF tenía dentro de su agenda el estudio de las normas de captación masiva y habitual.

238. Artículo 2.18.2.1. del Decreto 1068 de 2015.

239. A estos casos se les debe sumar, además, alguna de las siguientes condiciones, de acuerdo con el parágrafo 1 del artículo 2.18.2.1. del Decreto 1068 de 2015: *"[…] Que el valor total de los dineros recibidos por el conjunto de las operaciones indicadas sobrepase el 50% del patrimonio líquido de aquella persona; o b) Que las operaciones respectivas hayan sido el resultado de haber realizado ofertas públicas o privadas a personas innominadas, o de haber utilizado cualquier otro sistema con efectos idénticos o similares".*

240. De acuerdo con el artículo 2.18.2.1. del Decreto 1068 de 2015, se entiende como pasivo con el público: *"[…] el monto de las obligaciones contraídas por haber recibido dinero a título de mutuo o a cualquiera otro en que no se prevea como contraprestación el suministro de bienes o servicios"*.

241. Numeral 1 del artículo 2.18.2.1. del Decreto 1068 de 2015.

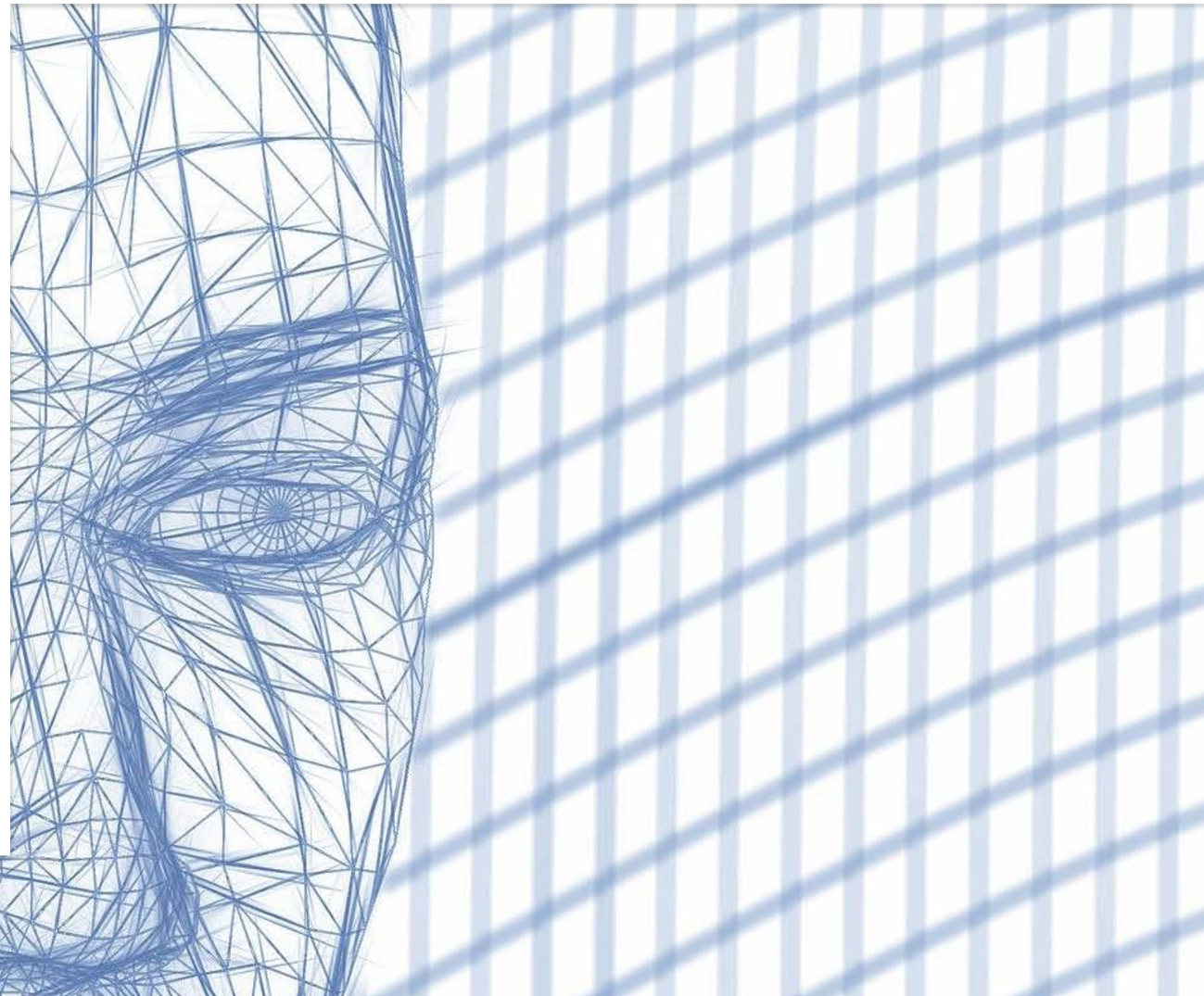
242. Numeral 2 del artículo 2.18.2.1. del Decreto 1068 de 2015.

Estas alianzas tienen como principal promotor la utilización de nuevos productos financieros (***i.e.***, los depósitos electrónicos[243]) y de facilidades en el cumplimiento de asuntos regulatorios por parte de la Superintendencia Financiera de Colombia en el marco de La Arenera[244].

Los depósitos electrónicos y la llegada de las SEDPES han dado un marco de acción más amplio para la vinculación y bancarización de nuevos clientes. Uno de los principales motores de esta vinculación de nuevos clientes es la posibilidad de realización de este procedimiento de manera digital (completamente), con requisitos de información (conocimiento del cliente) mucho menores que los exigidos para otros productos.

En relación con La Arenera, dentro del marco de esta iniciativa de la Superintendencia Financiera de Colombia, se ha pretendido identificar las barreras que las instrucciones de la Superintendencia, diseñadas en un momento y en circunstancias diferentes, pueden estar generando a la innovación financiera. De golpe, uno de los asuntos que mayor relevancia ha tomado es el de las instrucciones a las entidades vigiladas en relación con conocimiento de clientes. La información, los documentos y los procedimientos para conocimiento de clientes, con el fin de dar apertura a determinados productos financieros, ha sido una barrera para que estas entidades puedan dar un salto cualitativo en materia de digitalización. Tanto la apertura del producto como su utilización deben poder hacerse de manera digital para efectos de que la digitalización de los servicios financieros sea una realidad. La posibilidad de lograr que determinados requerimientos actuales, diseñados en contextos diferentes, puedan ser reemplazados por mecanismos digitales de conocimiento de clientes facilitará la vinculación de nuevos clientes a diferentes productos financieros.

Por lo anterior, en el marco de las billeteras digitales, su diseño y progresión en Colombia ha venido dado por la vinculación de entidades financieras en la operación de las billeteras digitales. En tal sentido, estas han pasado de ser únicamente mecanismos de acumulación de diferentes tipos de instrumentos de pago a verdaderos mecanismos de innovación en el relacionamiento entre empresas emergentes y entidades financieras. Esta innovación ha estado apalancada en la utilización de los productos financieros existentes (especialmente los depósitos electrónicos) y en la utilización de las nuevas herramientas ofrecidas por la Superintendencia Financiera (en especial La Arenera). La migración a otro tipo de billeteras digitales o monederos electrónicos, tales como los discutidos a lo largo de esta sección, solo será realidad en la medida en que el marco legal, y en especial la definición de captación masiva y habitual, sean reformados.



243. De acuerdo con el artículo 2.1.15.1.1. del Decreto 2555 de 2010, los depósitos electrónicos son: *"[…] depósitos a la vista semejables a las cuentas de ahorro, a nombre de personas naturales o jurídicas, y deberán cumplir con al menos las siguientes condiciones: a) El depósito debe estar asociado a uno o más instrumentos o mecanismos que permiten a su titular, mediante documentos físicos o mensajes de datos, extinguir una obligación dineraria y/o transferir fondos y/o hacer retiros. b) El contrato deberá establecer de manera clara, los canales a los cuales se tendrá acceso, así como aquellos que se encuentren restringidos. c) El contrato deberá establecer un plazo máximo de vigencia cuando el depósito permanezca sin fondos, luego del cual se dará su terminación unilateral. Dicho plazo no podrá superar los tres (3) meses. d) El contrato deberá establecer si el establecimiento de crédito o la Sociedad Especializada en Depósitos y Pagos Electrónicos - SEDPE ofrece o no el reconocimiento de una tasa de interés por la captación de recursos mediante depósitos electrónicos".*

244. La Superintendencia Financiera ha definido La Arenera como: *"[…] el marco que ha dispuesto la SFC para la realización de pruebas de innovaciones tecnológicas y financieras en un espacio controlado y supervisado. En este espacio, las entidades innovadoras podrán poner a prueba nuevos modelos de negocios, aplicaciones, procesos o productos que tengan componentes de innovación en tecnologías, que tengan impacto en los servicios financieros y que representen un beneficio para el consumidor financiero, faciliten la inclusión financiera, desarrollen los mercados financieros o mejoren la competencia entre entidades vigiladas".*

03

Consideraciones respecto de los criptoactivos

Discutir la evolución de los sistemas de pago en las anteriores secciones ha partido de la base de un sistema de pagos basado en una moneda de curso legal, en un sistema monetario en el que le es reconocida esta calidad a una sola moneda y, por lo tanto, el sistema de pagos nacional se rige y desenvuelve de acuerdo con el uso de esta moneda. Sin embargo, el mercado en los últimos años ha visto el surgimiento de un medio de pago completamente diferente, tanto por su creación como por los usos que se les ha dado: los criptoactivos.

Definir los criptoactivos, antes llamados criptomonedas, ha sido la tarea de las diferentes autoridades financieras, cambiarias y monetarias de los países. En el caso de Colombia, tanto el Banco de la República como la Superintendencia Financiera y la Dirección de Impuestos y Aduanas Nacionales, en lo que a cada uno respecta, han hecho un acercamiento a los criptoactivos. El Banco de la República, particularmente, ha tenido un acercamiento teórico que ha resultado muy útil y ha dado luces a otras autoridades para entender este tipo de activos digitales.

Es relevante mencionar que el Banco de la República, en su análisis de los criptoactivos, menciona que estos no pueden ser considerados como dinero, aun cuando tienen funciones de medio de pago, depósito de valor y unidad de cuenta (Banco de la República, 2018). Esto es precisamente lo importante de los criptoactivos como se encuentran hoy concebidos, y es que las partes de una transacción pueden decidir satisfacer la obligación de pago mediante la entrega de criptoactivos por parte del pagador. Sin embargo, este seguirá siendo el bemol en cualquier consideración de los criptoactivos: por no ser moneda de curso legal, su aceptación como medio de pago será esencial para que pueda fungir de esta manera.

Por este motivo, y muchos otros que los diferentes bancos centrales y autoridades han esgrimido, el uso del término "criptomoneda" ha sido reemplazado por el uso del término "criptoactivo". A los criptoactivos se los considera activos digitales y no moneda, y a los criptoactivos, en su calidad de activo, les es reconocida también su capacidad de ser medio de pago[245] siempre y cuando exista aceptación entre las partes.

Al ser considerados un medio de pago, entendiendo que las partes dentro de un determinado sistema en donde se pueden negociar criptoactivos han aceptado que estos podrán ser utilizados para satisfacer sus obligaciones, necesariamente se tiene que empezar a estudiar los criptoactivos como un ambiente adicional a los sistemas de pagos y transferencias. Por lo pronto, es necesario considerar que hasta tanto los criptoactivos adquieran una virtud de permanencia nos referimos a que las partes dentro del sistema retengan sus criptoactivos sin una voluntad de convertirlos en moneda legal en el corto o mediano plazo—, su utilización continuará estrechamente ligada a los sistemas bancarios, en la medida en que solo a través de estos se podrá realizar el *cash-out* de los activos digitales adquiridos y posteriormente vendidos.

Es precisamente en este punto donde la tensión regulatoria ha llegado a tocar la transaccionalidad con criptoactivos. Todo el sistema se desenvuelve bajo el marco del derecho mercantil y de la libertad de las personas de comprar y vender activos entre ellos. En tal sentido, este es un sistema que no se encuentra específicamente regulado pero que encuentra en las normas de derecho civil y mercantil las reglas que regirán la compraventa de los activos entre las partes y su utilización como medio de pago. Será la voluntad de las partes, al decidir que el pago de un bien o un servicio se puede saldar con la transferencia de criptoactivos entre ellas, la que facultará para que la transacción se satisfaga de esta manera.

Debe recordarse que nuestras normas prevén que ***"el pago efectivo es la prestación de lo que se debe"***[246] y, aún más importante, que ***"el pago se hará bajo todos respectos en conformidad al tenor de la obligación; sin perjuicio de lo que en los casos especiales dispongan las leyes. […] El acreedor no podrá ser obligado a recibir otra cosa que lo que se le deba, ni aún a pretexto de ser de igual o mayor valor la ofrecida"***[247]. De esta manera, nuestras normas contemplan la posibilidad de que las partes pacten maneras diferentes de satisfacer sus obligaciones. Ahora bien, la tensión regulatoria que se plantea al inicio de este párrafo se ha presentado en la operación de las plataformas a través de las cuales se realizan las operaciones de compraventa de criptoactivos y la utilización de cuentas para recibir los recursos, en moneda legal, producto de las operaciones con criptoactivos.

Las decisiones de las entidades financieras en diferentes países a cargo de estas cuentas, típicamente cuentas de ahorro y corrientes, en las que en algunos casos han decidido terminar la relación contractual con su cliente, han llevado a diferentes pronunciamientos por parte de las autoridades de los países correspondientes. Las respuestas, por supuesto, no son homogéneas. En el caso de Chile las autoridades tomaron una decisión desde el punto de vista de competencia para evitar el cierre de las cuentas. En el caso de Colombia, los pronunciamientos de la Superintendencia Financiera han tenido diferentes propósitos dentro de su ámbito de supervisión: (i) por un lado, advertir respecto de los riesgos que pueden existir para los usuarios la inversión en criptoactivos; y (ii) por otro lado, mencionarles a las entidades vigiladas que la operación en criptoactivos no se encuentra legalmente permitida para ellas. Ahora bien, en ningún caso los pronunciamientos han buscado prohibir la utilización de criptoactivos por parte de personas en Colombia, ni tampoco les impiden a los bancos que los titulares de sus cuentas bancarias reciban los recursos provenientes de las operaciones que realicen con criptoactivos en Colombia.

En todo caso, las entidades financieras en Colombia continúan viendo las operaciones con este tipo de activos con lupa con el fin de cumplir con los sistemas de administración de riesgos, especialmente de

245. Resulta relevante mencionar que en el análisis de este tipo de activos digitales, el Banco de la República (2018), ha dado una descripción, conceptual, de lo que es un medio de pago: "(…) un medio de pago es un bien material o virtual que es aceptado en el intercambio, no para consumirlo o usarlo en actividades productivas, sino para ser intercambiado de nuevo por bienes o servicios en el futuro."

246. Artículo 1626 del Código Civil.

247. Artículo 1627 del Código Civil.

administración del riesgo lavado de activos y financiación del terrorismo. En respuesta a esto, y en el marco de entender las operaciones con criptoactivos como una actividad mercantil, se ha venido buscando un marco de "formalización"[248] para efectos de transar con criptoactivos a partir de plataformas que satisfagan determinados requerimientos y que a su vez den tranquilidad a las entidades financieras en relación con el cumplimiento de sus sistemas de administración de riesgos.

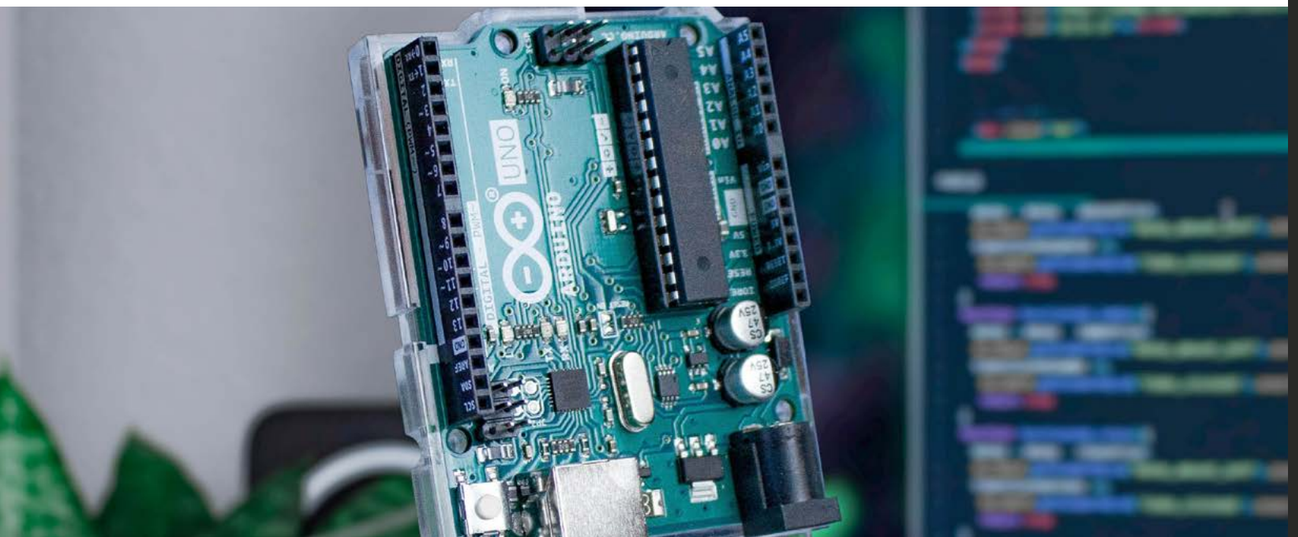
La evolución del mercado de criptoactivos, en la medida en que continúe desarrollándose, permitirá entrar al debate sobre incluir estos como activos admisibles para las entidades financieras en Colombia y también abrirá campo a la discusión de estos —o mejor, alguna subcategoría de estos— dentro del mercado de valores colombiano. Por lo pronto, dadas sus características y funcionalidad, no parece tangible el acercamiento de los criptoactivos al término "valor" y, por supuesto, no debería verse como semejable una emisión primaria de valores a una emisión primaria de criptoactivos[249].

Así mismo, el uso reiterado de criptoactivos como medio de pago y medio para realizar transferencias podrá ser un factor para reducir la volatilidad de estos activos digitales. Por lo pronto, su uso ha estado enfocado en la proyección que la inversión en ellos puede generar. No obstante, su función como medio de pago, y creciente aceptación por parte de comercios y clientes, hace evidente que este medio seguirá siendo utilizado.

En este sentido, la utilización de criptoactivos como un medio de pago alternativo y desvinculado del sistema de pagos es una realidad que encuentra su fundamento en las normas de derecho civil y mercantil y que, por la facilidad en su uso, pretende ahorrar costos y hacer eficientes e inmediatas las transacciones entre los diferentes actores del sistema. Así mismo, y más allá del desarrollo de los criptoactivos como un medio de pagos alternativo al tradicional, la tecnología que los respalda es una oportunidad de desarrollo por parte de los sistemas de pago actuales, con el fin de hacer sus operaciones más eficientes, seguras e inmediatas.

248. El término "formalización" lo utilizamos para identificar un potencial marco regulatorio o legal específico para las plataformas de criptoactivos. Actualmente muchas, si no la mayoría de plataformas de criptoactivos, actúan bajo reglas estrictas de procedimiento y gobierno corporativo, muchas de ellas con estándares de administración de riesgos tan altos como las entidades financieras tradicionales. Sin embargo, existe también un denominado "mercado negro" que, por fuera de los sistemas y plataformas reconocidas de transaccionalidad con criptoactivos, realizan operaciones, principalmente en efectivo, para la compraventa de criptoactivos.

249. Comúnmente conocidos como *Initial Coin Offerings*.



Conclusiones

Colombia tiene que adoptar y crear un ambiente de pagos que permita la interconexión e interoperabilidad de los diferentes actores, medios e instrumentos de pago para que tengan un relacionamiento fluido, eficiente y con menores costos. Este nuevo ambiente debe permitir la incorporación de nuevos actores y no debe comportar un obstáculo para los desarrollos tecnológicos. Los sistemas de pagos en Colombia, ahora y aquellos que surjan en el futuro, deben funcionar con base en la coexistencia y la posibilidad de interoperabilidad entre ellos.

A todo lo anterior se deben sumar asuntos de gran complejidad, como lo son la preferencia del uso del efectivo por parte de los consumidores, la inclusión financiera y bancarización de las personas y, de manera primordial, la necesidad de llegar a un nivel adecuado de educación financiera que permita a las personas el conocimiento y entendimiento de los medios e instrumentos de pago disponibles.

Dentro de los asuntos que todavía deben resolverse y para los cuales los sistemas de pago actuales deberán evolucionar, se encuentran los pagos y transferencias internacionales. Se debe procurar que, con la misma facilidad que se pueden realizar pagos y transferencias nacionales, se puedan hacer pagos y transferencias internacionales. Para esto, las normas cambiarias en Colombia deberán evolucionar. Por lo pronto, los criptoactivos, por su desarraigo nacional, se han convertido en una alternativa real y eficiente para la transferencia de valor entre personas ubicadas en diferentes países. Esta misma facilidad es la que debe buscarse en los sistemas de pagos en moneda y divisas.

Por último, se debe reconocer que Colombia, desde la regulación y supervisión, sigue buscando la forma de que las innovaciones tecnológicas, tanto las utilizadas en otros países como las desarrolladas nacionalmente, tengan cabida dentro del sistema legal colombiano. Esta labor se ha visto favorecida por el conocimiento especializado que han ido adquiriendo tanto el supervisor como el regulador de estas nuevas tecnologías. En todo caso, los esfuerzos regulatorios siempre tendrán que responder al factor de innovación y, en muchos casos, de emprendimiento ligados a los desarrollos digitales.

Bibliografía

Ali, R., Barrdear, J., Clews, R. y Southgate, J. (2014). Innovations in Payment Technologies and the Emergence of Digital Currencies. Bank of England Quarterly Bulletin 2014 Q3. Recuperado de SSRN: https://ssrn.com/abstract=2499397.

Arango Arango, C. A., Barrera Rego, M. M., Bernal Ramírez, J. F. y Boada Ortiz, A. (2018). Criptoactivos. Bogotá: Banco de la República. Documentos Técnicos o de Trabajo 04.

Asobancaria. (2018). Construyendo el ecosistema de pagos digitales en Colombia. Semana Económica, 1122. [En línea]. Recu

perado de https://www.asobancaria.com/semanseconomicas/Semanas%20de%202018/1122%20(C-15-02-2018).pdf.

Banco de la República. (2018). Reporte de Sistemas de Pago. Bogotá: Banco de la República. ISSN-2215-9363. Recuperado de http://www.banrep.gov.co/sites/default/files/publicaciones/archivos/reporte-sistemas-de-pago-2018.pdf.

Buckley, R. P. y Mas, I. (2016). The Coming of Age of Digital Payments as a Field of Expertise. Journal of Law, Technology & Policy, 1, 71-87. Recuperado de https://ssrn.com/abstract=1552754.

Committee on Payment and Settlement Systems (CPSS), Banco Mundial y Centro de Estudios Monetarios Latinoamericanos (CEMLA) (2002). Glosario de términos utilizados en los sistemas de pagos y liquidaciones. Primera edición. México: Centro de Estudios Monetarios Latinoamericanos y Banco Mundial. [En línea]. Recuperado de http://documentos.bancomundial.org/curated/es/886111468045090144/pdf/456480WP0SPANI1ms0glossary01PUBLIC1.pdf.

Committee on Payment and Settlement Systems (CPSS) (2003). A glossary of terms used in payments and settlement systems. Bank for International Settlements. ISBN 92-9197-133-2. Recuperado de https://www.bis.org/cpmi/glossary_030301.pdf.

G20 Australian Presidency (2014). The Opportunities of Digitizing Payments. [En línea]. International Bank for Reconstruction and Development/The World Bank. Formato en html con imágenes. Recuperado de file:///K:/Users/mariaam/Downloads/G20%20Report_Final%20(1).pdf.

Guersent, O. (2016). Transformación digital en los medios de pago. En: La transformación digital de los instrumentos de pago. Funcas. ISSN 0210-9107.

Luther, W. J. (2015). Bitcoin and the Future of Digital Payments. [En línea]. Recuperado de SSRN: https://ssrn.com/abstract=2631314.

Ortega, F. y León, C. (2017). Las transferencias compensadas por ACH Colombia: Un análisis desde la perspectiva de topología de redes. Borradores de Economía, 990. Bogotá: Banco de la República.

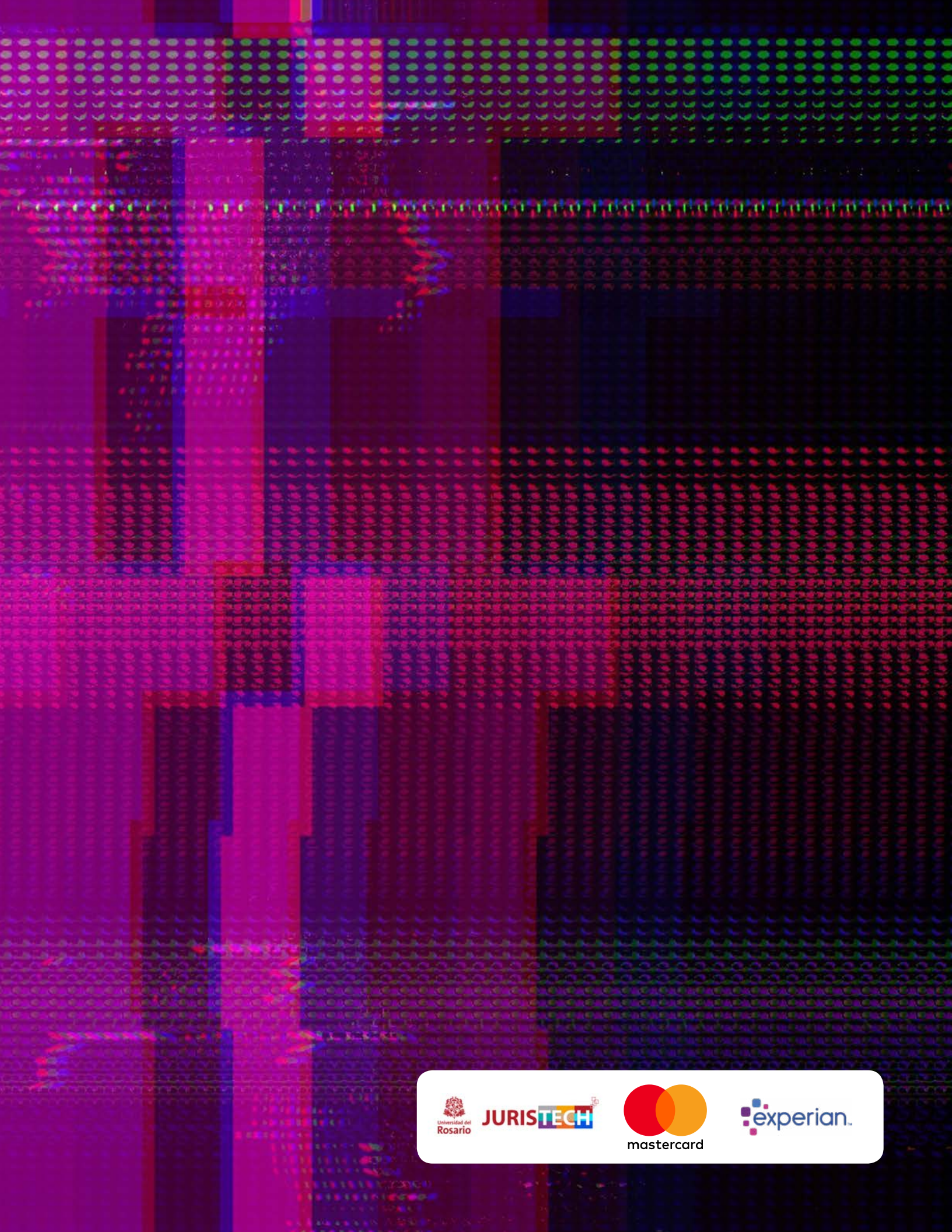
Pérez, J. (2016). Transformación digital en los medios de pago. En: La nueva era digital de los medios de pagos. Funcas. ISSN 0210-9107. Recuperado de file:///K:/Users/mariaam/Downloads/PEE149.pdf.

Radcliffe, D. y Voorhies, R. A. (2012). Digital Pathway to Financial Inclusion. [En línea]. Recuperado de SSRN: https://ssrn.com/abstract=2186926

Unidad de Proyección Normativa y Estudios de Regulación Financiera (URF) (2018). Estudio sobre los sistemas de pago de bajo valor y su regulación. Bogotá: Unidad de Proyección Normativa y Estudios de Regulación Financiera.

Uribe Escobar, J. D. Los sistemas de pago de bajo valor en Colombia. Revista del Banco de la República (1043), 5-12.

Wallace, D. (2018). Open Banking and the Evolution of Digital Payments. [En línea]. Recuperado de https://www.finextra.com/blogposting/16087/open-banking-and-the-evolution-of-digital-payments.


Universidad del Rosario
JURISTECH
mastercard
experian