

JUAN ESTEBAN DURANGO RAVE

- Licenciado en Derecho de la Universidad Latinoamericana de Ciencia y Tecnología.
- Máster en Ciberderecho por la Universidad Católica de Murcia España.
 - Asesor legal en Derecho Digital en la firma GoLegal
- jdurango@golegalcr.com

6



Acreditación de las Actuaciones Electrónicas Personales: de la Firma Electrónica a la Identidad Digital Auto-Soberana

Juan Esteban Durango Rave

Licenciado en Derecho de la Universidad Latinoamericana de Ciencia y
Tecnología.

Máster en Ciberderecho por la Universidad Católica de Murcia España.

Asesor legal en Derecho Digital en la firma GoLegal

jdurango@golegalcr.com

Resumen

Un usuario promedio se expone a diario a cientos de interacciones recíprocas a través de entornos digitales, no solo con otras personas, sino también con plataformas digitales que prestan diversos servicios. Lo anterior representa retos que surgen de la forma en que dichos participantes acreditan sus actuaciones electrónicas, mecanismo que será fundamental para determinar la confianza entre las partes. Es aquí donde convergen en un solo ecosistema la necesidad de identificarse y manifestar el consentimiento a través de firmas electrónicas, criptografía, tecnología fiable, sistemas informáticos de autenticación y la identidad digital, todo bajo las reglas de la legalidad que otorga el ordenamiento jurídico. Lo que este texto plantea es un estudio de la eficacia y validez jurídica de los métodos de acreditación electrónica conocidos para personas físicas y disponibles en la actualidad, así como la manera en que éstos pueden generar confianza entre las personas bajo un contexto digital.

Palabras clave: firma electrónica, firma digital, certificado digital, criptografía, tecnología de llave pública, acreditación electrónica, autenticación, identidad digital, identidad digital auto-soberana.

SUMARIO

Introducción – I. FIRMA ELECTRÓNICA – a.- Antecedentes de la firma – b.- La Firma Electrónica – II. FIRMA DIGITAL Y FIRMA DIGITAL CERTIFICADA – III. IDENTIDAD DIGITAL – a.- Identidad Digital Auto-Soberana – IV. CONCLUSIONES – Referencias bibliográficas.

ACCREDITATION OF PERSONAL ELECTRONIC ACTIONS: FROM ELECTRONIC SIGNATURE TO SELF-SOVEREIGN DIGITAL IDENTITY

Abstract

An average user is exposed daily to hundreds of reciprocal interactions through digital environments, not only with other people, but also with digital platforms that provide various services. The foregoing represents challenges that arise from the way in which participants certify their electronic actions, a mechanism that will be essential to determine trust between the parties. In this digital ecosystem converge needs to identify and express consent through electronic signatures, cryptography, reliable technology, computerized authentication systems and digital identity, all under the rules of legality granted by the legal system. What this text raises is a study of the efficacy and legal validity of the electronic accreditation methods known to individuals and currently available, as well as the way in which they can generate trust between people in a digital context.

Keywords: electronic signature, digital signature, digital certificate, cryptography, public key technology, electronic accreditation, authentication, digital identity, self-sovereign digital identity.

INTRODUCCIÓN

Las acreditaciones electrónicas son mecanismos facilitadores de confianza en los actuales entornos digitales, en la actualidad los más conocidos para personas físicas son las firmas electrónicas, firmas digitales, los certificados digitales y la autenticación de la identidad digital, la cual con el ingreso de la Identidad Digital Auto-Soberana,¹⁵¹ promete un cambio revolucionario a la manera en que las personas gestionarán su identidad digital en el futuro.

Estos métodos de acreditaciones requieren el análisis de sus complejidades técnicas a la luz de lo dispuesto no solo por las leyes locales, sino por el Derecho Internacional, en el entendido que el mundo digital es un fenómeno local y global, por lo tanto, la doctrina y la regulación internacional, juegan un papel preponderante para realizar el análisis de estos instrumentos legales.

Nos adentramos en el estudio de una materia no muy explorada por el jurista, en parte por el desconocimiento de la terminología y los conceptos técnicos que envuelve su abordaje, por lo que será la ambición de este de este texto ser claro en el desarrollo de sus ideas logrando hacerse entender por la mayor cantidad de lectores.

Proponemos por lo tanto, el abordaje desde el concepto tradicional e histórico de la firma manuscrita, hasta llegar a los mecanismos que prometen ser en el futuro, los idóneos para la gestión de las acreditaciones electrónicas, como es el caso de la Identidad Digital Auto-Soberana.

I. FIRMA ELECTRÓNICA

a.- Antecedentes de la firma

La firma como elemento de identificación y manifestación de la voluntad tiene su origen en el uso de troqueles, anillos o sellos, los cuales fueron utilizados por personas o reinos para identificarse, dejando su marca única en objetos,

superficies o documentos oficiales¹. Siglos más tarde, dichas prácticas dieron paso a la utilización de sello y firma manuscrita en el mismo acto, ésta última al ser realizada por la persona siempre de la misma manera se le conoció con el nombre de rúbrica², un signo único e ilegible la mayoría de las veces y que a través de la historia moderna ha sido utilizada por las personas para firmar documentos.

Desde entonces, la firma manuscrita, firma ológrafa³ o autógrafa, es decir, aquella escrita a mano por su mismo autor, ha sido el principal instrumento utilizado por las personas para identificarse o manifestar su consentimiento relativo al contenido de un documento en formato físico. La Real Academia Española [RAE] (s.f.) en una de sus acepciones define la firma como el “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” (definición 2). De acuerdo con estas definiciones, es frecuente encontrar en nuestro ordenamiento el término de rúbrica como sinónimo de firma.

La firma se puede entender como un signo asociado a una persona y que la vincula con un acto específico, tal como lo expresa el autor colombiano Peña (2015) quien señala que la firma es el signo “por el cual el individuo se expresa mediante un acto físico en el que manuscibe sus iniciales o nombres y apellidos en las actividades de la vida cotidiana, en sus relaciones personales,

¹ “Los sellos empezaron teniendo forma circular o de disco y después cilíndrica, siendo originalmente de piedra y posteriormente de otros materiales entre los que el lapislázuli era muy apreciado; estaban grabados en su superficie con imágenes de dioses o con símbolos de poder. Con ellos se imprimía sobre la arcilla fresca o se sellaban puertas o tinajas. Es un objeto personal que identifica a su poseedor, de ahí que se utilizara por los que de una u otra manera ostentaba algún poder” (Robles, 2015, p. 39).

² “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” (Real Academia Española, s.f., definición 1).

³ También hológrafa.

económicas y desde luego jurídicas”. De ahí que el mismo autor llame este tipo de firma como *firma-signo*⁴, siendo el instrumento que identifica al firmante y a la vez otorga certeza no solo de la firma sobre el documento, sino que además permite asociar la voluntad del firmante respecto del contenido del documento, por lo tanto, bajo estas características, la *firma-signo* goza de plena validez jurídica.

Es innegable por lo tanto, la trascendencia jurídica que alcanza la firma manuscrita por ser el instrumento idóneo a través del cual el firmante manifiesta su voluntad con respecto al contenido de un documento, no solo vinculándose jurídicamente con lo que expresa, sino además como bien señala Peña (2015) obligándose frente a terceros bajo ciertas circunstancias. A lo anterior podría agregarse otros propósitos de la firma y es cuando ésta se consigna en un documento por el hecho de que la persona quiera dejar constancia que estuvo en un lugar, un día y una fecha determinada, tal es el caso cuando en algunas instituciones académicas los docentes solicitan la firma manuscrita a los alumnos para dejar prueba de su asistencia a clase, también al ingresar en algunos edificios, el encargado de la seguridad exige la firma a todas las personas que ingresan a las instalaciones.

Si bien en la normativa costarricense no existe una definición jurídica de firma, el Tribunal Primero Civil (2009) desarrolló el concepto destacando que la firma es lo que permite crear un nexo entre el documento y la persona, ésta puede ser una rúbrica (no ser legible) y su función primordial es servir como instrumento no solo de la autenticidad del documento, sino también de la manifestación de

⁴ La *firma-signo* es un concepto propuesto por Peña (2015) para representar la unión inescindible entre un sujeto y su representación.

voluntad del firmante⁵. Según lo anterior, es aceptable afirmar que la firma debe reunir las siguientes características: hecha a mano por su propio autor, vinculación y atribución del firmante con la aceptación del contenido del documento; identificar al autor de la firma a través de rasgos y patrones únicos atribuibles a esa persona (datos biométricos) y ser perdurable o longeva (íntegra).

b.- La Firma Electrónica

El desarrollo doctrinal de la firma electrónica se origina en el Derecho Mercantil Internacional, de manera precisa en los trabajos realizados por la Comisión de las Naciones para el Derecho Mercantil Internacional (CNUDMI), quienes desde la década de los años noventa observaron la importancia de las crecientes transacciones internacionales por medio del comercio electrónico, por lo cual desde entonces, la Asamblea General de la ONU ha procedido a la redacción y publicación de leyes modelo.

Las Leyes Modelo de la CNUDMI son disposiciones que persiguen la adopción de su texto en los países miembro y que al momento de elaborar las leyes internas, se inspiren en sus preceptos para lograr armonizar la regulación de los Estados en materia de comercio electrónico, mejorando no solo las relaciones económicas entre países con sistemas jurídicos diferentes, sino permitiendo a las empresas y ciudadanos de cada país participar con seguridad jurídica en un

⁵ “La firma es el lazo que une al firmante con el documento en que se pone, el nexo entre la persona y el documento. Para establecer ese lazo, la firma no necesita ni ser nominal ni ser legible; esto es, no requiere expresar de manera legible el nombre del firmante. La función primordial de la firma no es la identificación del firmante, sino la de ser el instrumento de su declaración de voluntad, que exige esa actuación personal del firmante en la que declara que aquello es un documento y no un simple borrador, además de que el firmante asume como propias las manifestaciones, declaraciones o acuerdos que contiene”. (Tribunal Primero Civil, 2009, Considerando III).

entorno global donde cada día más prevalecen las comunicaciones electrónicas (CNUDMI, 1996, pág. 80).

Con dicho propósito, la CNUDMI a través de la Asamblea General de la ONU aprueba diferentes Leyes Modelo en materia de Comercio Electrónico: en 1996 la Ley Modelo de la CNUDMI sobre Comercio Electrónico (LMCCE), años más tarde en el 2001, publica la Ley Modelo de la CNUDMI sobre Firmas Electrónicas (LMCFE) y en el año 2017, la Asamblea General aprueba la resolución para la publicación de la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos (LMCDTE).

En la LMCCE, la CNUDMI (1996) plantea un nuevo criterio denominado “criterio de equivalencia funcional”, el cual se basa en analizar los principales objetivos y funciones de los requisitos impuestos a los actos escritos sobre papel y de esta forma determinar cómo cumplir estos objetivos y funciones bajo las técnicas y parámetros del Comercio Electrónico (pág. 20). Diversos ordenamientos en la actualidad han establecido la equivalencia funcional como un principio jurídico pilar en materia de Comercio Electrónico y Firma Electrónica. Desde la doctrina se ha desarrollado este concepto, de manera concreta Illescas Ortiz (como se citó en Torres, 2012) afirma que:

La función jurídica que en toda su extensión cumple la instrumentación escrita y autógrafa – o eventualmente su expresión oral – respecto de cualquier acto jurídico, la cumple igualmente su instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, dimensión, alcance y finalidad del acto así instrumentado. La equivalencia funcional, en suma, implica aplicar a los mensajes de datos electrónicos una pauta de no discriminación respecto a las declaraciones de voluntad o ciencia manual, o gestualmente efectuadas por el mismo sujeto (pág. 7).

En consecuencia, no se impondrán requisitos legales más exigentes a los actos electrónicos que los ya establecidos a los actos escritos, físicos o presenciales, de tal manera que no se le negarán o restrinjan efectos jurídicos a un acto electrónico por el mero hecho de serlo, entendiéndose de manera equivalente los actos, documentos o comunicaciones en formato físico, como aquellos en formato electrónico. En este sentido, en la Ley Modelo sobre Comercio Electrónico, la CNUDMI (1996) para desarrollar el criterio de equivalencia funcional, consideró atribuir a la firma sobre papel las siguientes funciones: identificar a una persona; dar certeza de su participación en el acto de firmar; y asociar a esa persona con el contenido del documento. Por lo anterior, la CNUDMI señala que la adopción del principio de equivalencia funcional no deberá dar lugar a la imposición de normas de seguridad más estrictas a los usuarios en el marco del comercio electrónico, que los requisitos ya aplicables a la documentación consignada en papel (pág. 28).

En materia de firmas electrónicas, la CNUDMI (2001) a través de la LMCFE recomienda que los Estados al momento de incorporar esta Ley Modelo en su derecho interno, deberán tener en cuenta sus principios básicos: equivalencia funcional, neutralidad tecnológica, no discriminación entre las firmas electrónicas nacionales y extranjeras, la autonomía de las partes y el origen internacional de la Ley Modelo.

La neutralidad tecnológica es de igual forma un principio jurídico promovido y adoptado a nivel global, así la OCDE (2007) señaló que los países miembros apoyan el uso de firmas electrónicas como equivalentes a las firmas manuscritas y abogan por la neutralidad tecnológica en su uso. En lo relativo al comercio electrónico, este principio se define según Ibáñez y Rincón (como se citó en Torres, 2012) como aquel que propende que las normas del comercio electrónico puedan abarcar las tecnologías que propiciaron su reglamentación, junto con las tecnologías que se están desarrollando y están por desarrollarse (pág. 134). En

el mismo sentido, Madrid Parra (como se citó en Torres, 2012) afirmó que en cumplimiento de este principio, “el legislador dictará normas cuya aplicación no suponga una adopción por una determinada tecnología” (pág. 135).

Desde la perspectiva del Derecho Administrativo, la neutralidad tecnológica se le impone al Estado como una garantía hacia el administrado en la prestación de servicios y acceso a la información, así como una garantía de imparcialidad en la contratación administrativa. De acuerdo con la Procuraduría General de la República (2004) el Estado debe establecer un marco jurídico favorable a la competencia. Dicho régimen estaría basado en el principio de “neutralidad tecnológica”, lo que permitiría la propagación de las tecnologías de la información y la comunicación y un acceso más asequible a estas. De igual forma aclara la PGR, la “neutralidad tecnológica” entrañaría que el Estado no puede tomar decisiones que tiendan a favorecer la utilización de una determinada tecnología por encima de otra.

Desde el punto de vista normativo, el principio de neutralidad tecnológica se regula en el artículo 3, inciso h de la Ley de Telecomunicaciones No. 8642 como parte de sus principios rectores y en general ordena que es la posibilidad que tienen los operadores de redes y proveedores de servicios de telecomunicaciones para escoger las tecnologías por utilizar, siempre que estas dispongan de estándares comunes y garantizados (Asamblea Legislativa de La República de Costa Rica, 2008).

En Costa Rica, el legislador se inspiró en estos principios⁶ para regular lo relativo a documentos electrónicos y firmas digitales a través de la “Ley de Certificados, Firmas Digitales y Documentos Electrónicos No. 8454”, al establecer en el artículo 2 los principios de: regulación legal mínima, autonomía de la voluntad de los particulares para reglar sus relaciones e igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas. Así mismo, el artículo 3 establece el reconocimiento de la equivalencia funcional a toda manifestación con carácter representativo o declarativo transmitida por un medio electrónico o informático, imponiendo igualdad jurídica a los documentos o comunicaciones electrónicas o físicas. Mientras que el artículo 4 ordena que los documentos electrónicos tendrán fuerza probatoria en las mismas condiciones que los documentos físicos.

Si bien la ley 8454 adopta los principios de la LMCFE, carece en su normativa de una definición y desarrollo jurídico del concepto de firma electrónica, al contrario de otros ordenamientos como el de México, Colombia, Panamá o Europa, siendo que en nuestro país el legislador al regular lo relativo a firma electrónica, ha decidido utilizar el término Firma Digital, alejándose de la terminología utilizada no solo por la LMCFE, sino del concepto que en la actualidad prevalece en el Derecho internacional, lo cual es el concepto de firma electrónica.

Para desarrollar el concepto de firma electrónica, se recogerá lo normado en el ordenamiento costarricense, la jurisprudencia, así como lo erigido por el Derecho comparado y los preceptos de la LMCFE, en el entendido que la LMCFE son

⁶ De acuerdo con la CNUDMI, Costa Rica figura como uno de los países que se ha inspirado y ha incorporado en su ordenamiento local la Ley Modelo sobre Firmas Electrónicas y sus principios: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status

recomendaciones para la incorporación en los ordenamientos jurídicos internos, por lo tanto, no es limitante recoger sus principios y normas para interpretar los vacíos que pueda tener nuestra legislación en el tema.

En su artículo 2 inciso a), la LMCFE (2001) define firma electrónica como:

Los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos (pág. 1).

Acotado a lo anterior, la LMCFE reconoce que la finalidad de los mecanismos de firma electrónica es desarrollar medios técnicos que ofrezcan características de las firmas manuscritas en entornos electrónicos.

En Costa Rica, si bien el concepto de firma electrónica no se incluye en la Ley 8454, sí existe normativa desde la década de los noventa que ya regulaba este instrumento, tal es el caso de la Ley General de Aduanas de 1995, en la cual La Asamblea Legislativa de La República de Costa Rica (1995) define firma electrónica como el “Resultado de obtener, mediante mecanismos o dispositivos, un patrón, que biunívocamente se asocie a una persona física o jurídica y a su voluntad de firmar” (Art. 266, inciso 11), así mismo en sus artículos del 103 al 106, se equipara el código de usuario y la clave de acceso confidencial asignada a los funcionarios aduaneros, con la firma electrónica y a su vez a ésta con la firma autógrafa, así el artículo 103 en su segundo párrafo ordena que “Las firmas autógrafas que la Dirección General de Aduanas requiera podrán ser sustituidas por contraseñas o signos adecuados, como la firma electrónica, para la sustanciación de las actuaciones administrativas que se realicen por medios informáticos”. De igual forma el artículo 105 en su segundo párrafo que establece

que “Para todos los efectos legales, la clave de acceso confidencial y/o firma electrónica equivale a la firma autógrafa de los funcionarios, auxiliares y demás usuarios”.

De forma semejante, La Corte Suprema de Justicia (2013) en el Reglamento sobre Expediente Judicial Electrónico ante el Poder Judicial, en su artículo 2, establece como requisitos para la validez de las piezas procesales la firma digital, electrónica y holográfica, pudiendo ser dicha firma: la firma digital certificada; firma electrónica mediante registro como usuario en el Poder Judicial; y la firma holográfica mediante dispositivo o capturador de firmas utilizado por despachos y fiscalías electrónicas. Ejemplo de lo anterior se puede apreciar en las sentencias firmadas por los Jueces y Magistrados de la Corte Suprema de Justicia, quienes estampan una firma electrónica holográfica en sus resoluciones judiciales.

La jurisprudencia ha ampliado los criterios del artículo 2 del Reglamento supra al considerar una comunicación firmada electrónicamente como aquella enviada a través del correo electrónico del usuario inscrito ante el sistema de gestión del Poder Judicial, la Sala Tercera (2019) en resolución afirmó que:

es posible concluir entonces que pese a la ausencia de la firma, en caso de que el documento se remita desde una cuenta de correo electrónico validada por la institución se consideraría válido para todos los efectos, en el tanto, se entendería firmado electrónicamente (Considerando III).

Por otra parte y acudiendo a la doctrina internacional, el autor Alamillo Domingo (2019) manifiesta que la firma electrónica es “un artefacto técnico que va a ser reconocido jurídicamente en función de una serie de propiedades que lo hacen relevante como fuente de prueba electrónica, al objeto de atribuir un documento a una persona y, en su caso, también identificar a dicha persona” (pág. 335).

Para mayor amplitud en la definición del concepto en el marco del derecho comparado, estas son algunas definiciones adoptadas en las regulaciones extranjeras:

1.- Argentina

La Ley 25.506 de Firma Digital del 2001, en el artículo 5 denomina firma electrónica “al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales ser considerado firma digital. En caso de ser desconoce la firma electrónica corresponde a quien la invoca acreditar su validez” (Honorable Congreso de la Nación Argentina, 2001).

2.- Colombia

La Ley 527 de 1999 regula lo relativo a firma electrónica en el artículo 7, señalando que:

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.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma. (Congreso de Colombia, 1999).

Consiente de la importancia de la firma electrónica como un instrumento de seguridad jurídica necesario para la realización de negocios en el marco del comercio electrónico, La Presidencia de La República emite el Decreto 2364 del año 2012, en el cual se reglamenta el artículo 7 de la Ley 527 de 1999, por lo que en el artículo 3 se establecen los criterios y métodos técnicos que pueden ser considerados como firma electrónica, 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” (Presidencia de La República, art. 3).

3.- Estados Unidos

La UETA Act (The Uniform Electronic Transactions Act) y la E-Sign Act (Electronic Signatures in Global and National Commerce Act) son las dos leyes que regulan la firma electrónica en Estados Unidos. La UETA fue promulgada en 1999 y ha sido a su vez incorporada por 49 Estados, este marco normativo establece la equivalencia legal de los registros electrónicos con los documentos en papel firmados manualmente, así mismo la E-Sign del año 2000, es una ley federal que busca facilitar el uso de registros electrónicos y firmas entre Estados y en el Comercio Internacional. Ambas leyes coinciden en señalar que la firma electrónica es un sonido electrónico, símbolo o proceso adjunto o lógicamente asociado a un registro (E-Sign incluye “contrato”) y ejecutado o adoptado por una persona con la intención de firmar (UETA Sección 2 inciso 7, E-Sign Sección 106 inciso 5).

4.- Unión Europea:

Por su parte, la Unión Europea a través del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de junio de 2014 (Reglamento eIDAS), regula lo referente a identificación electrónica, servicios de confianza y transacciones electrónicas dentro de la comunidad europea, estableciendo un marco de confianza y seguridad jurídica no solo para los más de 500 millones de ciudadanos que la conforman, sino para todo aquel que realiza transacciones electrónicas en este mercado. De acuerdo con el artículo 3, inciso 10, se entiende por firma electrónica “los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar. (Parlamento Europeo y el Consejo, 2014).

5.- México:

La definición de firma electrónica en México se incluye en el Código de Comercio y se inspira de manera clara en los preceptos de La Ley Modelo de la CNUDMI sobre Firmas Electrónicas, en ese sentido, el artículo 89 consagra que firma electrónica son:

Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio (Cámara de Diputados, Código de Comercio, 1889).

6.- Panamá

La Ley 51 de 2008 panameña que regula los documentos electrónicos y las firmas electrónicas, inicialmente definió firma electrónica como el “conjunto de sonidos, símbolos o datos vinculados con un documento electrónico, que ha sido

adoptado o utilizado por una persona con la intención precisa de identificarse y aceptar o adherirse al contenido de un documento electrónico” (Art. 2 inciso 20), pero luego, a través de la Ley 82 de 9 noviembre de 2012 se modifica dicha definición, por lo que a partir de esa reforma, el artículo 2, inciso 20 de la Ley 51 de 2008 define firma electrónica como el “Método técnico para identificar a una persona y para indicar que esa persona aprueba la información que figura en un mensaje de datos o documento electrónico” (Asamblea Nacional, Ley 82 de 2012, Art. 7).

7.- Perú

El ordenamiento jurídico de Perú, regula la firma electrónica en la Ley 27269 Ley de Firmas y Certificados Digitales, dicho marco normativo entiende por firma electrónica “cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita” (Art. 1 párr. 2). Así mismo su ámbito de aplicación aplica a las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos y que puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos (El Congreso de la República, 2000).

Visto lo anterior, se destaca la amplia adopción a nivel jurídico del concepto de firma electrónica en las diversas jurisdicciones revisadas, las cuales han adoptado o al menos seguido los preceptos y definiciones de la Ley Modelo Sobre Firmas Electrónicas, de manera que ordenamientos como el de Argentina, Estados Unidos, Europa, México, Panamá y Perú, permiten interpretar de sus redacciones que la firma electrónica es un mecanismo a través del cual se consignan, vinculan, adjuntan, integran, añaden, anejan o asocian datos electrónicos a un mensaje de datos (documento electrónico) y que éstos datos a su vez deben permitir identificar y vincular al firmante con el contenido del

documento y el mismo acto. Si bien las definiciones del ordenamiento colombiano no incluyen las acepciones aquí descritas, si contempla criterios técnicos más precisos acerca de los mecanismos que pueden ser considerados como firma electrónica: códigos, contraseñas, datos biométricos, o claves criptográficas privadas.

La firma electrónica es un procedimiento que está subordinado a la tecnología, debe ser no solo un mecanismo seguro que aporte la mayor cantidad de evidencias digitales para garantizar la veracidad del acto, sino además confiable para garantizar la identificación del firmante y la integridad del documento. En la firma electrónica prevalece el procedimiento técnico respecto al signo de la firma manuscrita y los métodos deben generar confianza en busca de la validez y eficacia probatoria, de manera acertada Peña (2015) llama a este instrumento *firma-método*.

La firma digital al ser un método ejecutado a través de un procedimiento digital y que a su vez permite reunir los criterios y requisitos de firma electrónica aquí estudiados, se considera en definitiva un tipo de firma electrónica, una especie de ésta. Es por lo anterior, que los preceptos y principios que rigen la firma digital en el ordenamiento costarricense a través de la Ley No 8454, son extrapolables y de aplicación al uso e implementación de cualquier otra firma electrónica. De esta forma y atendiendo a la normativa nacional e internacional repasada, a los principios de equivalencia funcional, neutralidad tecnológica y autonomía de las partes, así como también a los preceptos de las Leyes Modelos, se entiende que en el ordenamiento costarricense una firma electrónica podrá ser entre otras:

- El nombre de usuario y su clave de acceso confidencial a un sistema informático.

- La clave de un solo uso OTP (*One Time Password*) para ingresar a un sistema informático o para ejecutar cualquier acto con consecuencias jurídicas.
- El PIN de una tarjeta de débito.
- La firma agregada al final de un correo electrónico.
- Un correo electrónico.
- Marcar una casilla en el navegador (*Clic-Wrap*) o la navegación dentro de un sitio web (*Browser-Wrap*).
- La firma autógrafa estampada con lápiz óptico o con el dedo sobre un dispositivo electrónico.
- Los datos biométricos del firmante adjuntos a un documento electrónico: huella digital, reconocimiento facial, un video, un sel-fie, un audio.
- Las firmas electrónicas emitidas al amparo de un certificado suministrado por un ente certificador o servicio de confianza.
- La Firma Digital.

Ante los diferentes tipos de firma electrónica que los mecanismos tecnológicos pueden ofrecer, es fundamental señalar bajo que criterios técnicos y jurídicos tendrán mayor validez legal y solidez probatoria la firma electrónica, es decir que ofrezca la necesaria confianza y fiabilidad para dar certeza de la identidad de la persona y la integridad del documento. La Ley Modelo sobre Firma Electrónica expresa los requisitos y características de lo que se considera una firma electrónica fiable, en el artículo 3 la CNUDMI (2001) considera una firma fiable si: a) los datos de creación de la firma corresponden exclusivamente al firmante; b) los datos de creación de la firma estaban al momento de firmar, bajo el control exclusivo del firmante; c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma (integridad de la firma); y d) es posible detectar cualquier alteración de la información hecha después de firmar (integridad del documento).

Lo anterior es lo que la doctrina internacional considera como una firma electrónica fiable y en diversas jurisdicciones se ha regulado llamándola firma electrónica avanzada, tal es el caso del Reglamento eIDAS el cual considera como tal a la firma electrónica que cumple ciertos requisitos: estar vinculada al firmante de manera única, que permita la identificación del firmante, ser creada utilizando datos de creación con alto nivel de confianza y bajo control exclusivo del firmante y estar vinculada con los datos firmados de tal modo que una ulterior modificación de los datos sea detectable.

Similar definición ofrece el Código de Comercio Mexicano en el artículo 97, al establecer que una firma electrónica avanzada debe reunir las siguientes características: i) que los datos de creación de la firma correspondan exclusivamente al firmante; ii) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante; iii) poder detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y garantizar la integridad del mensaje de datos, es decir la no alteración del documento electrónico. Similares criterios consagra el Decreto 2364 de 2012 de Colombia, para considerar una firma electrónica confiable.

En Costa Rica no se hace mención dentro del ordenamiento al término firma electrónica avanzada, fiable o confiable. Sin embargo, las definiciones anteriores tanto la recogida por la Ley Modelo sobre Firmas Electrónicas como las de los diferentes ordenamientos jurídicos extranjeros, se asemejan de manera clara con los criterios plasmados en la definición de firma digital de nuestra Ley 8454. El artículo 8 en su primer párrafo expresa que firma digital es cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico. Por consiguiente, cuando hablamos de firma digital en nuestro ordenamiento estamos haciendo referencia

a una firma fiable o firma electrónica avanzada según la terminología en la materia aceptada mayoritariamente en el Derecho comparado.

De manera práctica y desde una perspectiva técnica ¿qué requiere una firma electrónica para ser fiable, avanzada o firma digital de acuerdo a nuestro ordenamiento? Existen en la actualidad múltiples plataformas que a través del uso de software y hardware ofrecen la posibilidad de realizar firmas electrónicas, éstas según las características técnicas podrán ser firmas electrónicas simples o avanzadas. Un caso para citar es el de una firma manuscrita o rúbrica plasmada con pluma digital o con el dedo sobre un dispositivo electrónico, dicho acto electrónico tendrá que valorarse a la luz del principio de equivalencia funcional y no podrá negársele efectividad jurídica, por ser este acto equivalente al de una persona que realiza la firma con pluma de tinta sobre un documento de papel.

Lo anterior es un ejemplo de firma electrónica simple, la cuál podría garantizar la identidad de la persona si durante la firma, un tercero verifica su rúbrica con la impresa en su documento de identidad, o bien si la realizó frente a terceros que han validado su identidad, es el caso de los repartidores de mercancías que para formalizar la entrega del producto o servicio, solicitan al receptor firmar sobre una tableta electrónica o sobre el teléfono móvil el cual contiene una aplicación para tal efecto, otro ejemplo es cuando en algunos bancos o empresas comerciales para recoger el consentimiento de los usuarios o clientes, solicitan la firma manuscrita sobre algún dispositivo electrónico, ya sea una tableta o un dispositivo con tecnología Wacom.

Si los casos descritos arriba el firmante negará la firma, dicha rúbrica podría ser cotejada y analizada en un peritaje informático. La eficacia de este peritaje dependerá en gran medida de las funcionalidades técnicas de la plataforma electrónica utilizada para la captura de la firma, ya que ésta podría recoger

rasgos personalísimos del firmante como lo son los datos biométricos, por ejemplo, la fuerza ejercida durante la realización de los trazos. Esta información sería confiable a la luz de los resultados obtenidos por el perito para comprobar la autenticidad de la firma. De modo similar sucede cuando una firma realizada con pluma sobre papel es repudiada por el firmante, ésta deberá ser analizada por un perito calígrafo quien realizará una prueba caligráfica para dar certeza sobre su autenticidad.

Sin embargo, para ser firma electrónica avanzada o firma digital (regulación costarricense) en el método anterior se está omitiendo el mecanismo que garantice la integridad y no alteración ulterior tanto de los datos como del propio documento electrónico, requisito pilar para considerar una firma fiable. La integridad es definida por el Reglamento 33018⁷ como la propiedad de un documento electrónico que denota que su contenido y características de identificación han permanecido inalterables desde el momento de su emisión (Ministerio de Ciencia y Tecnología, 2006, art. 2.27). Por consiguiente, algunos mecanismos conocidos para garantizar la integridad del documento podrían ser, correr una función *hash* sobre el documento una vez firmado electrónicamente o estampar un sello de tiempo electrónico sobre todo el documento electrónico.

La función *hash* también se conoce como función resumen y es el resultado de obtener una versión reducida (resumida) de un mensaje de datos (Alamillo, 2018), esta versión resumida es una cadena de dígitos (*hash*) o digesto, obtenidos a partir del resultado de correr un algoritmo sobre el documento electrónico, es una huella digital única, por lo tanto, si ese documento electrónico origen es alterado en un solo *bit*, al volver a correr el algoritmo sobre el mismo documento el *hash* obtenido será diferente al primero, lo cual probará que el

⁷ Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 33018.

documento ha sido modificado y ha perdido su integridad. Este mecanismo es utilizado por la informática forense para garantizar la cadena de custodia de las evidencias digitales, el *hash* obtenido al momento de recopilar la evidencia tendrá que ser el mismo *hash* al momento de presentarla ante el juzgador, si estos no coinciden querrá decir que la evidencia ha sido alterada.

Por otra parte, el sello de tiempo electrónico es un método conformado por “datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante” (Parlamento Europeo, Reglamento eIDAS, art. 3 inciso 33). Un sello de tiempo por lo tanto permite relacionar un conjunto de datos electrónicos con un tiempo específico, estableciendo certeza de que ese mensaje de datos existía en la fecha y hora que el sello fue estampado en el documento. En consecuencia, si el documento electrónico que ha sido estampado con el sello de tiempo es modificado, el sello de tiempo electrónico se destruye y el mensaje de datos o documento electrónica perderá su integridad.

Por lo tanto, si las partes acuerdan de manera previa manifestar el consentimiento a través de una firma manuscrita realizada sobre un dispositivo electrónico que capture los datos biométricos del firmante, que reúna además otras evidencias digitales que permitan identificar unívocamente al usuario: correo electrónico personal, sms, *one time password*, huella digital, intercambio de claves de acceso, y que de igual forma agregué un *hash* o un sello de tiempo electrónico sobre el documento una vez impuesta la firma, satisface los requisitos de integridad, identificación y vinculación jurídica exigida por el artículo 8 primer párrafo de la Ley 8454, pudiendo considerarse firma digital y atribuírsele el valor equivalente consagrado en el artículo 9 de la misma ley y en consecuencia tener el mismo valor y eficacia probatoria de su equivalente funcional firmado en manuscrito.

En resumen, no hay impedimento legal para utilizar firmas electrónicas en nuestro ordenamiento, a la luz de los principios de equivalencia funcional, neutralidad tecnológica y autonomía de las partes. De igual forma se podrá entender como firma electrónica avanzada, aquella que cumpla con los criterios exigibles de una firma fiable según la Ley Modelo sobre Firma Electrónica, o las características de la firma digital establecidas por el artículo 8 de nuestra Ley 8454.

II. FIRMA DIGITAL Y FIRMA DIGITAL CERTIFICADA

La firma digital desde un punto de vista técnico se asocia a un mecanismo numérico y matemático, de manera concreta a infraestructura de llave pública (tecnología PKI), por tal razón en diferentes ordenamientos lo han regulado desde esta perspectiva, así por ejemplo en Colombia la Ley 527 de 1999, define firma digital como un valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático para vincular al iniciador del mensaje (...) (art. 1.c), igualmente en Perú la Ley de Firmas y Certificados Digitales del año 2000, establece que la firma digital utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único (...) (art. 3); Argentina en su Ley de Firma Digital No 25.506 del 2011, expresa que por firma digital se entiende el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante (...) (art. 2).

En Costa Rica mientras tanto, ni en la Ley 8454 ni el Reglamento 33018⁸ de manera expresa se atribuye a la firma digital un método asociado a un mecanismo numérico o matemático, decantándose más el legislador por otorgarle a la firma digital la definición de firma electrónica avanzada ya analizada anteriormente, esto se deduce al considerar en el artículo 8 de la Ley,

⁸ Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 33018.

que los datos electrónicos de la firma se adjuntan al documento electrónico a través de un proceso lógico y no matemático o criptográfico. De acuerdo con lo anterior, es factible considerar que el legislador de manera un poco confusa definió firma digital acercándose más al significado de firma electrónica fiable, en vez del significado técnico de firma digital como instrumento asociado a un mecanismo matemático. Una redacción más armoniosa con la doctrina dominante hubiera sido llamar a la firma digital, firma electrónica avanzada.

Por otra parte, no debe confundirse firma digital con firma digitalizada, la cual se considera es una firma electrónica con muy poco valor probatorio y por lo tanto de escasa eficacia jurídica. La firma digitalizada es la que agrega una imagen de una firma manuscrita a un documento electrónico, o la firma manuscrita estampada en un documento físico y luego escaneada (digitalizada). Bajo estos supuestos, dicha firma no logrará cumplir con los requisitos mínimos de atribución e identificación que debe reunir una firma electrónica, mucho menos con los requisitos de una firma electrónica avanzada. Por lo tanto, no se recomienda su utilización, este criterio ha sido además manifestado por La Sala Tercera de la Corte (2008) al afirmar que la rúbrica debe interpretarse en un sentido amplio y no perderse de vista que de acuerdo con los avances tecnológicos, la firma hológrafa ha evolucionado a la firma digital, concepto que no equivale a la digitalización de la signatura (escaneo) (Resolución N° 00941 - 2008).

Continuando con el análisis de la firma digital desde una óptica técnica, Alamillo (2019) acota que el algoritmo de firma digital se basa en una cifra asimétrica, formada por una clave pública y otra privada, que permite “firmar” documentos con la clave privada y verificar la firma digital con la clave pública. Criptográficamente, firmar digitalmente es generar un dato matemático asociado al objeto digital (pág. 40). Es por esta razón que la infraestructura de llave pública se considera uno de los mecanismos mas seguros para firmar electrónica

o digitalmente un documento, ya que este método permite verificar el emisor del mensaje de datos y la integridad del documento.

Sin embargo, Peña (2015) sostiene que la firma digital *per se* no genera confiabilidad técnica completa respecto del autor o emisor del mensaje de datos, sino únicamente respecto del mensaje. Para este último fin es necesario que la ley establezca una presunción, de manera que es el certificado digital emitido por una autoridad certificadora, el instrumento a través del cual se atribuye esta presunción legal a la firma digital, denominándola Firma Digital Certificada.

Dicho lo anterior, se entenderá por certificado todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma (CNUDMI, 2001, art. 2.b). El Reglamento eIDAS por su parte, define que el certificado de firma electrónica es una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona; mientras que el certificado cualificado de firma electrónica es un certificado que ha sido expedido por un prestador cualificado de servicios de confianza (Art. 3, incisos 14 y 15).

La Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 8454, en el artículo 11 señala que un certificado digital es un mecanismo electrónico o digital mediante el que se puede garantizar, confirmar o validar técnicamente: a) la vinculación jurídica entre un documento, una firma digital y una persona; b) la integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada; c) la autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.

Por consiguiente, la diferencia entre firma digital y firma digital certificada la otorga el certificado digital que ampara a esta última, dicho certificado emplea

criptografía de clave pública y clave privada y deberá ser emitido por una autoridad certificadora autorizada por la Dirección de Certificadores de Firma Digital (DCFD) una dependencia del Ministerio de Ciencia, Tecnología y Telecomunicaciones, que se encarga de la administración y supervisión del sistema de certificación digital. La autoridad certificadora deberá cumplir con lo establecido en la Sección II de la Ley, lo dispuesto en el Reglamento, así como los requerimientos técnicos de la Política de Certificados para la jerarquía nacional de certificadores registrados, entre otros requisitos. En la actualidad es el Banco Central de Costa Rica, el único emisor de certificados digitales autorizado y reconocido por la DCFD, siendo el servicio de confianza exclusivo en el país para la emisión de certificados digitales.

La Firma Digital Certificada es emitida por un tercero de confianza autorizado (Autoridad Certificadora del SINPE del Banco Central de Costa Rica). Para emitir un certificado al solicitante, los emisores quien a su vez son oficinas autorizadas para emitir certificados de la Autoridad Certificadora del SINPE, deberán validar de manera presencial la identidad del solicitante del certificado digital, una vez esta persona ha pagado los costos de solicitud de la firma y ha cumplido con el resto de requisitos, el emisor emite y entrega al solicitante una tarjeta que contiene un chip con los certificados digitales (un certificado de firma y un certificado de identificación), así como la llave pública y privada de los certificados, un dispositivo físico para insertar la tarjeta y un PIN, dichos elementos conforman lo que se conoce como la Firma Digital Certificada. Posteriormente la persona titular del certificado deberá instalar en su equipo de cómputo el firmador (software de la firma), para poder utilizar la tarjeta y el dispositivo de la Firma Digital Certificada, de esta forma, podrá estar listo para firmar documentos electrónicos y autenticarse en portales bancarios o de instituciones públicas.

Respecto a su fuerza probatoria, solamente a la Firma Digital Certificada (FDC) se le atribuye presunción de autoría y responsabilidad (artículo 10 de la Ley 8454), es decir que, salvo prueba en contrario, todo documento electrónico asociado a una FDC se presumirá, de la autoría y responsabilidad del titular del correspondiente certificado digital. Quien firme utilizando una FDC no podrá negar su consentimiento respecto a lo firmado y no podrá repudiar la firma, por lo cual tendrá la carga de la prueba si niega la autenticidad de ésta y tendrá que demostrar su invalidez.

De igual manera, el Reglamento No. 33018, señala la diferencia entre los efectos legales de los certificados digitales emitidos en el país por un certificador autorizado versus las firmas y certificados emitidos por otros certificadores, ya sea dentro o fuera del país, el artículo 10 le otorga pleno efecto legal frente a terceros y al Estado, a los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital.

Sin embargo, en el segundo párrafo de la norma, se establece que las firmas y certificados emitidos dentro o fuera del país que no pertenezcan a un certificador registrado ante la DCFD, no surtirán efectos por sí solos, pero podrán ser empleados como elemento de convicción complementario para establecer la existencia y alcances de un determinado acto o negocio.

Se entiende entonces, que la presunción legal no ocurre con la firma digital, que al no estar amparada en un certificado digital emitido por la autoridad certificadora, obliga a que la carga de la prueba sea para quien pretende demostrar la veracidad y validez de dicha firma. A la luz de lo dicho en el artículo 10 del Reglamento, del principio de equivalencia, neutralidad tecnológica y de autonomía de las partes, si la firma digital contiene un certificado digital emitido por otro certificador (local o extranjero) y el cual también emplea criptografía de clave pública, deberá ser aceptado éste por la autoridad judicial correspondiente

para que a través de un peritaje y otras evidencias digitales, se pueda llegar a la convicción de que el mecanismo técnico permite con certeza determinar de que la firma es auténtica y por lo tanto válida, en consecuencia, no se le podrá negar efectos jurídicos *ad portas* a un documento firmado con una firma digital certificada no emitida por la autoridad certificadora costarricense.

Tal caso se ha evidenciado en resoluciones de algunos Tribunales Civiles que han rechazado el cobro de títulos valores firmados con firmas electrónicas avanzadas (firma digital) y amparadas en certificados digitales de proveedores extranjeros, así en la resolución 0024-2019 del Tribunal de Apelación Civil y Trabajo de Alajuela (2019) el juzgador manifestó:

En el asunto que nos ocupa, no hay pruebas de que S.L. se encuentre autorizada y registrada ante la Dirección de Certificadores de Firma Digital. En consecuencia, al documento aportado con la demanda no se le pueden atribuir los efectos propios de una firma digital certificada. A lo sumo, se le podría tener como un documento probatorio complementario, en los términos señalados en el párrafo segundo del artículo 10 del reglamento indicado. No obstante, el documento base de un proceso monitorio dinerario debe valerse por sí mismo; no siendo factible, al menos en esta vía privilegiada, que se le complemente con fuentes de prueba adicionales.

En el anterior caso, el juzgador rechaza de previo los efectos jurídicos de la firma al no estar amparada en un certificado emitido por autoridad certificadora nacional, sin entrar a valorar a través de un peritaje informático las características técnicas de la firma, procedimiento que podría demostrar o no la autoría, autenticidad e integridad de la firma y el documento electrónico. Entiende el Tribunal que el único método válido para firmar títulos valores es una Firma Digital Certificada, pero no hay ninguna norma en nuestro ordenamiento que así

lo ordene, sería el equivalente a exigir que la firma de un título valor tenga que venir autenticada por notario. Así mismo, de ser así como lo interpreta el Tribunal, personas que no pueden optar por un certificado digital, como lo son las personas extranjeras⁹, o costarricenses que no residan en el país y por lo tanto no tienen acceso a una oficina de un emisor de certificados, tendrían un impedimento legal para firmar títulos valores en formato electrónico.

Lo que consagra la Ley 8454 en su artículo 9 es que la firma digital tiene valor equivalente y eficacia probatoria en las mismas condiciones que una firma manuscrita, por lo tanto, si la parte interesada demuestra que la firma electrónica estampada en el pagaré goza de integridad, identifica al deudor y lo vincula jurídicamente con el documento electrónico, dicha firma es equivalente a una firma manuscrita. Lo contrario sería negar no solo los preceptos del artículo 9 (valor equivalente), sino además impedir a la aplicación de los principios de equivalencia funcional, neutralidad tecnológica y autonomía de las partes.

En suma, la Ley Modelo sobre Firmas Electrónicas establece la no discriminación de las firmas electrónicas extranjeras, es decir, que el lugar de origen en sí no debe ser en ningún caso un factor para determinar si puede reconocerse la capacidad de los certificados extranjeros o las firmas electrónicas para tener eficacia jurídica en un ordenamiento jurídico, ya que la determinación de si un certificado o una firma electrónica pueden tener eficacia jurídica, y hasta qué punto pueden tenerla, no debe depender del lugar en que se haya emitido el certificado o la firma electrónica sino de su fiabilidad técnica (2001, pág. 43).

⁹ De acuerdo con las Política de Certificados para la jerarquía nacional de certificadores registrados el documento de identidad, la cédula de residencia o la cédula jurídica (Anexo A).

Finalmente, la presunción legal de la Firma Digital Certificada solo es aplicable en las vías jurisdiccionales costarricenses, si dicha firma es utilizada para actos que tengan eficacia fuera de nuestra jurisdicción, será en ese ordenamiento jurídico que deberá demostrar su validez legal ante la autoridad judicial de acuerdo con los preceptos legales de ese país.

III. IDENTIDAD DIGITAL

En la actualidad gran cantidad de personas interactúan la mayoría de su tiempo en un entorno predominantemente digital, durante sus interacciones personales, sociales, educativas, culturales y económicas convergen con otras personas y sistemas informáticos a través del ciberespacio¹⁰. La gestión de la identidad en el entorno digital se convierte por lo tanto en piedra angular para la generación de confianza durante dichas interacciones, de lo contrario, las personas tendrían vedado acceder a recursos e información que requieren para la ejecución de sus actividades diarias: envío y recibo de correos electrónicos, realizar transacciones bancarias en línea, charlar en línea con colegas y familiares, interactuar en sus redes sociales, realizar trámites en portales de la administración pública, etc.

Se requiere por ende una identidad digital con un mínimo de fiabilidad que garantice en gran medida, que la persona es quien dice ser y es titular de los atributos que la identifican.

En el mundo de la identidad digital una información adjunta a la identidad de alguien o algo se denomina atributo de identidad (EU Blockchain Observatory Forum [EU BOF], 2019, pág. 12). El reto será entonces determinar cuáles serán esos atributos válidos considerando en principio que la identidad no es estática,

¹⁰ Ciberespacio: Ámbito virtual creado por medios informáticos. RAE, Consultado Abril 28 de 2021.
Recuperado de <https://dle.rae.es/ciberespacio?m=form>

es dinámica y es una colección de atributos individuales que describen una entidad y determinan las transacciones en las que esa entidad puede participar. Si bien la cantidad de atributos puede ser infinito, se pueden clasificar en tres grupos: i) atributos inherentes; ii) atributos acumulados; y iii) atributos asignados. Los primeros refieren a los atributos intrínsecos a la persona: edad, rasgos físicos, datos biométricos; los segundos son los atributos que son acumulados durante el tiempo: salud, preferencias y comportamientos, estudios; y los atributos asignados son aquellos que reflejan las relaciones que la persona mantiene con otros organismos: número de identificación nacional, correo electrónico, número de licencia (World Economic Forum, 2016, pág. 41).

La identidad digital para Peña (2015) sobresale cada vez más como el valor fundamental para el siglo XXI como atributo de la persona digital que participa, interactúa, consume y ejerce sus derechos al acceso a la información, a la comunicación, a la libre expresión y al desarrollo libre de la personalidad y de actividades comerciales y sociales relevantes.

Se entiende por lo tanto identidad digital como un conjunto finito de atributos que permite a una entidad ser identificado como única y probar su identidad frente a terceros electrónicamente, siendo factible que nuestra persona digital se componga a su vez de varias identidades digitales, las cuales podrán usar unos u otros atributos de acuerdo con el contexto (Allende, 2020, pág. 12). Cuando pensamos en la identidad digital, por lo tanto, se necesita ver no como una sola cosa, sino más bien como la suma total de todos los atributos que existen sobre la persona en el ámbito digital, una constante colección creciente y en evolución de puntos de datos (EU Blockchain Observatory Forum, 2019, pág. 12).

En otro orden de ideas, la identidad digital de acuerdo con Barros, Gómez, Pareja y Pedak (2017) puede clasificarse en:

- i. Identidad digital legal: es la que requiere estar vinculada a la identidad legal de una persona física o jurídica. Es necesaria, por ejemplo, para realizar transacciones con el gobierno o con instituciones financieras reguladas.
- ii. Identidad digital simple: es aquella que no requiere estar vinculada a una identidad legal física. Se utiliza, por ejemplo, para conectarse a redes sociales (pág. 7).

En Costa Rica es válido considerar que la identidad digital legal se gestiona a través del certificado digital de identificación emitido por la autoridad certificadora, la cual luego de un proceso de verificación y registro presencial (cara a cara) de la persona, procede el emisor a entregar el certificado al solicitante, para que ésta se identifique con plena presunción legal ante las instituciones públicas o privadas en el entorno digital. De esta forma se garantizará el no repudio de las actuaciones electrónicas del ciudadano en los entornos que acepten el certificado digital como medio de autenticación.

La identidad digital puede tener validez en un determinado dominio, para Barros et al (2017) puede ser válida únicamente para interactuar con una institución, empresa o en una red social determinada o puede, en cambio, tener un reconocimiento más general (por ejemplo, en un Estado). Esto implica que una persona física puede tener más de una identidad digital a través de múltiples dominios, y utilizar cada una para una función o contexto diferentes. Lo que no puedes suceder es que dos personas físicas tengan la misma identidad digital legal (pág. 7).

La gestión de los sistemas de identidad digital combinan procesos y tecnologías que potencian el uso de los datos identificatorios de las personas, y requiere: i) un modelo de gobernanza y un modelo de negocio; ii) un marco legal apropiado y actualizado; iii) la simplificación y estandarización de procesos y sistemas; iv)

el establecimiento de mecanismos de interoperabilidad que faciliten la coordinación entre los diferentes organismos, y v) la promoción y coordinación del ecosistema de uso de la identidad (Barros et al., 2017, Pág. 6). Dentro del marco legal apropiado se deberá considerar el tipo de identidad digital (legal o simple) a gestionar para determinar la forma de atribuir el vínculo jurídico, ya sea éste a través de la presunción legal otorgada por el ordenamiento a los certificados digitales de identificación o a través de un contrato privado (términos y condiciones, condiciones de uso, contrato de adhesión) que permitan atribuir efectos legales a las actuaciones electrónicas de la identidad digital simple dentro de ese dominio específico.

Como parte de la gestión de la identidad digital, es fundamental el proceso de autenticación, según la norma internacional ISO7IEC 2382:2015 (como se citó en Alamillo, 2019, pág. 57), la autenticación es el acto de verificar la identidad alegada por una entidad, por lo que se entiende que este mecanismo de verificación permitirá atribuir efectos legales a las actuaciones electrónicas de una persona física.

De acuerdo con el artículo 2 inciso 1 del Reglamento de Firma Digital, la autenticación para verificar la identidad de una persona puede ser de dos tipos: i) durante el proceso de registro donde se evalúan las credenciales de la entidad (persona), como evidencia de que realmente es quien dice ser; ii) durante el uso de la identidad, es el acto de comparar electrónicamente las credenciales y la identidad enviada (Ej., código de usuario y contraseña, certificado digital, etc.) con valores previamente almacenados para comprobar la identidad.

Según la Guía de Identidad Digital del NIST, el paradigma clásico de los sistemas de autenticación identifica tres factores como los pilares de la autenticación: i) algo que la persona sabe (contraseñas, usuarios); ii) algo que la persona tiene (tarjeta de identificación o una clave criptográfica); iii) algo que la persona es

(datos biométricos). La solidez del sistema por lo tanto, estará determinado en gran medida por la cantidad de factores a incorporar, entre más factores utilice el sistema más robusto y confiable será (Grass, Garcia y Fenton, 2017, pág. 12).

En los mecanismos de autenticación predominante, es el agente verificador quien debe comprobar las credenciales de la entidad (usuario) y validar su identidad, es decir, debe haber existido un proceso de autenticación previo de la persona para lograr acceder a los servicios del verificador, esto lo convierte en el proveedor de la identidad y del servicio a la vez. Pero desde la perspectiva actual, en la que un usuario promedio interactúa con decenas de plataformas digitales las cuales a su vez recopilan atributos de la persona de acuerdo con la naturaleza de las funcionalidades ofrecidas, los riesgos emergen y amenazan la privacidad y los datos personales de la persona usuaria, además de exponerla a potenciales suplantaciones de identidad al existir la posibilidad de que alguien pueda robar los datos personales almacenados en los diferentes sistemas de información. Sumado a lo anterior, es una tarea caótica para el usuario la gestión de múltiples identidades digitales para satisfacer los requerimientos de cada plataforma digital.

Cabe destacar además que a consecuencia de la dependencia de las personas de los servicios digitales, el uso masivo de la población global de algunos servicios en la web como las redes sociales alcanza en la actualidad la cifra de cuatro mil doscientos millones de usuarios activos¹¹, lo cual facilita a terceros autenticar a sus usuarios a través de los mecanismos de estas plataformas predominantes, esto es lo que se conoce como delegación de autenticación.

¹¹ Cifras según el portal Statista a mayo 3 de 2021: <https://www.statista.com/statistics/617136/digital-population-worldwide/>

Alamillo (2018) señala que con la delegación de autenticación, nos encontramos ante la autenticación como servicio prestado por terceros; esto es, la identificación y autenticación por proveedores de credenciales, también denominados proveedores de identidad digital (pág. 68).

Un ejemplo de lo anterior son los servicios que encontramos en la web que nos permiten acceder a sus funcionalidades utilizando el servicio de autenticación de Google, Facebook o LinkedIn entre otros. Consciente las plataformas que miles de millones de usuarios cuentan con identidad digital en estos servicios líderes de Internet, lo más práctico es crear un mecanismo que permita al usuario autenticarse en su sistema utilizando las credenciales ya creadas en otro sistema. Lo que aquí sucede es que la nueva plataforma va a confiar en la identificación que haya realizado el usuario en las plataformas mencionadas, así como en las medidas de seguridad para autenticación, seguramente porque, tras un análisis de riesgos, habrá llegado a la conclusión que resulta más seguro delegar el proceso que implementarlo (Alamillo, 2018, pág. 73).

a.- Identidad Digital Auto-Soberana

Con el desarrollo durante la última década de las tecnologías de registro distribuido (*Distributed Ledger Technology – DLT*), ha sobresalido el concepto de Identidad Digital Auto-Soberana, una identidad descentralizada en la que los atributos de identificación ya no estarán en control de un verificador central, sino en control de la misma entidad.

En el paradigma de la identidad centralizada que se analizó anteriormente, la identidad de una persona es proporcionada por alguna entidad externa, el verificador, y en el caso de la autenticación delegada, un tercero es el encargado de gestionar el mecanismo. En el paradigma de identidad descentralizada, el objetivo es poner al usuario en el centro del marco y así eliminar la necesidad de que terceros emitan y administren la identidad (EU BOF, 2019, pág. 12).

De manera muy resumida, las tecnologías *DLT* o *Blockchain* se caracterizan por estar basadas en criptografía de clave pública lo cual garantiza seguridad e integridad de la información, además crean registros inmutables y públicos que se pueden gestionar de forma descentralizada. Por tal razón, las funcionalidades y características de *Blockchain*, permiten que sea la tecnología idónea para operar el mecanismo de Identidad Digital Auto-Soberana.

Una aproximación a la definición de Identidad Auto-Soberana (IAS) la ofrece Sovrin (como se citó en Allende, 2020) al señalar que la “identidad auto-soberana (IAS) es un término utilizado para describir el movimiento digital que reconoce que un individuo debe poseer y controlar su identidad sin la intervención de las autoridades administrativas. La IAS permite a las personas interactuar en el mundo digital con la misma libertad y capacidad de confianza que en el mundo físico” (pág. 27). Así en el mundo de la identidad descentralizada, los usuarios crean sus propias identidades digitales. Por lo general, esto comienza con un usuario que crea su propio identificador o identificadores únicos y luego adjunta información a ese identificador de una manera que permite demostrar su autenticidad (EU BOF, 2019, pág. 13).

Según Allen (como se citó en Alamillo, 2019), las identidades auto-soberanas deben atender a los siguientes principios: existencia de la identidad de una persona independientemente de administradores o proveedores de identidad; control por la persona de sus identidades digitales; acceso completo por las personas a sus datos; transparencia de los sistemas y algoritmos; persistencia de las identidades digitales (las identidades deben ser longevas, duraderas); portabilidad de las identidades digitales; interoperabilidad de las identidades digitales; cumplimiento de la economía de datos; y protección de los derechos de la persona.

La idea general de la identidad auto-soberana se basa en repositorios personales portables en los que podemos almacenar y administrar todas nuestras claves privadas, nuestros autenticadores y nuestros tokens y credenciales digitales de manera segura y confiable. Estos repositorios se conocen como billeteras digitales (Allende, 2020, pág. 28).

Un caso de uso típico sería que un usuario obtuviera credenciales de su colegio profesional, por ejemplo, del Colegio de Abogados y Abogadas de Costa Rica, esta institución emitiría una credencial que certificaría que dicha persona es un profesional agremiado a su Colegio y que esta habilitado para ejercer la profesión, esta certificación se registraría en una *Blockchain* y sería accesible solamente por las personas a las que el Abogado o Abogada decida compartir esa credencial, por lo tanto, si la persona profesional en Derecho requiere demostrar en el Poder Judicial que está autorizado para ejercer la abogacía, solo tendrá que compartir con la institución a través de una billetera digital el acceso a sus credenciales. Gracias a diversas técnicas criptográficas, como las firmas digitales, es posible obtener prueba sólida de que la credencial es genuina (es decir, emitido realmente por la autoridad designada y no manipulado desde entonces) y que la persona que presenta esa credencial es la persona referida (EU BOF, 2019, pág. 13).

Desde un punto de vista más técnico, la IAS se basa en un tipo de identificador denominado DID, que no es más que una URL (identificador universal uniforme de recursos), similar a la dirección de un sitio web, esta URL relaciona un sujeto con un documento de identificación descentralizada, de esta forma, a través de un DID se puede acceder a los contenidos de dicho DID para obtener los atributos de la persona (Alamillo, 2019, pág 77 y 78).

En la actualidad la IAS es un instrumento en desarrollo y que aún le falta consolidarse como un mecanismo masivo de identificación, pero que de acuerdo

con sus características promete regresarle a la persona la soberanía sobre sus identidades digitales, ofreciendo un método seguro para el resguardo y la gestión de sus datos personales. Sin embargo a nivel jurídico existen limitaciones, ya que los marcos normativos sobre protección de datos personales y sistemas de identificación están basados en relaciones de usuario-proveedor (Chomczyk, 2020), es decir, un tercero es el encargado de guardar las credenciales del usuario, prestar el servicio y a su vez ofrecer el mecanismo de autenticación, siendo un reto desde ya analizar las implicaciones legales de la IAS en el entendido que bajo este marco de trabajo, las credenciales del usuario son gestionadas por el mismo a través de una plataforma descentralizada como Blockchain.

IV. CONCLUSIONES

Aunque nuestro ordenamiento jurídico no contemple en la ley especial de Firma Digital el concepto de firma electrónica, no es limitante la utilización de este mecanismo como un instrumento de acreditación electrónica, todo dependerá de la fiabilidad y seguridad brindada por la tecnología utilizada para generar la firma. Dicha fiabilidad estará dada por la capacidad del método tecnológico de poder identificar al firmante y garantizar a su vez la integridad de la firma y el documento electrónico.

A la luz de los principios de equivalencia funcional, neutralidad tecnológica y autonomía de las partes, no podrá el juzgador imponer mayores exigencias a la firma electrónica con respecto a las firmas manuscritas realizadas sobre formato papel. No se le podrá negar efectos jurídicos de previo a una firma electrónica, sin antes valorar la fiabilidad de la tecnología utilizada para determinar la identificación del firmante, así como la integridad y autenticidad del documento, lo anterior se logrará a través de un peritaje informático de la firma estampada y las evidencias digitales generadas.

Para mayor seguridad jurídica a las transacciones en el marco del comercio electrónico, se sugiere incluir una definición de firma electrónica dentro del cuerpo normativo de la Ley 8454, lo cual fortalecería los principios de autonomía de las partes, equivalencia funcional y neutralidad tecnológica, asimismo impulsaría las actividades comerciales por estos medios y homologaría nuestra normativa con la regulación internacional predominante en esta materia, este último elemento muy necesario en un mundo digital donde predominan las transacciones transfronterizas no presenciales.

Una firma digital en nuestro ordenamiento es equivalente a la firma electrónica avanzada consagrada en la mayoría de los ordenamientos jurídicos que se han inspirado en las Leyes Modelo de la CNUDMI, dicha firma deberá cumplir tres requisitos para ser fiable: permitir identificar al firmante, vincularlo jurídicamente con el acto de la firma y verificar la integridad (no alteración) del documento electrónico firmado. De otra parte, la firma digital certificada es una firma digital generada a través de un método matemático criptográfico, amparada por un certificado digital emitido por la autoridad certificadora y que goza de plena presunción legal. En suma, la firma digital y la firma digital certificada son dos instrumentos diferentes, por lo tanto, si una norma establece como válido el uso de firma digital para determinado acto, se deberá entender que acepta cualquiera de los dos tipos de firma, tal es el caso del reformado artículo 460 del Código de Comercio que le otorga a la factura electrónica el título de ejecutividad siempre y cuando cuente con firma digital, lo cual se aprecia como correcto pues de esta forma se cumple con el valor equivalente consagrado en el artículo 9 de la Ley 8454, el cual reconoce el mismo valor y eficacia probatoria a los documentos firmados con firma digital que a los firmados en manuscrito.

Por sus características y su enfoque centrado en la persona, la Identidad Digital Auto-Soberana promete convertirse en el mecanismo de identificación más seguro y fiable para las acreditaciones electrónicas, no solo por las garantías

que ofrece a la protección de los datos personales de los ciudadanos, sino por la interoperabilidad y alcance que ofrece como un mecanismo de identificación universal. Es un tema que en la actualidad todavía se desarrolla jurídicamente, pero que en los próximos años veremos un incremento en su utilización y por ende surge la necesidad de comenzar a realizar los análisis jurídicos pertinentes.

REFERENCIAS BIBLIOGRÁFICAS

Alamillo Domingo, Ignacio. (2019). *Identificación, Firma y otras Pruebas Electrónicas. La regulación jurídico-administrativa de la acreditación de las transacciones electrónicas*. Editorial Aranzadi, Pamplona: España.

Allende L. (2020). Identidad Digital Auto-soberana El futuro de la identidad digital: auto-soberanía, billeteras digitales y blockchain. BID, BID LAB & LACCHAIN. Recuperado el 3 de mayo de 2021, de: <https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf>

Asamblea Legislativa de La República de Costa Rica. 2005. *Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 8454*. Recuperado de Sinalevi: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=55666

Asamblea Legislativa de La República de Costa Rica. 1995. *Ley General de Aduanas N° 7557*. Recuperado el 28 de abril de 2021, de Sinalevi: http://www.pgrweb.go.cr/SCIJ/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=25886

Asamblea Legislativa de La República de Costa Rica. 2008. *Ley General de Telecomunicaciones No 8642*. Recuperado el 28 de abril de 2021, de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=63431

Asamblea Nacional. (2008). *Ley 51 de 22 de Julio de 2008 Que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de*

servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico. Panamá. Recuperado de: https://www.firmaelectronica.gob.pa/documentos/Ley_51-Firma_electronicas_almacenamiento_tecnologico_y_comercio_electronico.pdf

Asamblea Nacional. (2012). *Ley 82 de 9 de noviembre de 2012 Que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley 51 de 2008 y adopta otras disposiciones.* Panamá. Recuperado el 28 de abril de 2021, de: https://www.firmaelectronica.gob.pa/documentos/Ley_82-Que_modifica_la_Ley_51_de_2008.pdf

Barros, A., Gómez, C., Pareja, A., Pedak, M. (2017). *La Gestión de la Identidad y su impacto en la economía digital.* Banco Interamericano de Desarrollo (BID). Recuperado el 30 de abril de 2021, de: <https://publications.iadb.org/publications/spanish/document/La-gesti%C3%B3n-de-la-identidad-y-su-impacto-en-la-econom%C3%ADa-digital.pdf>

Cámara de Diputados del H. Congreso de la Unión. (1889). *Código de Comercio.* México. Recuperado el 28 de abril de 2021, de: http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_de_Comercio.pdf

Congreso de Colombia. (1999). *Ley 527 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. Diario Oficial No 43.673 de 21 de agosto de 1999. Recuperado el 28 de abril de 2021, de: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.htm
I

Congreso de la República. (2000). *Ley No 27269 Ley de Firmas y Certificados Digitales.* Perú. Recuperado el 28 de abril de 2021, de: https://cdn.www.gob.pe/uploads/document/file/356833/NORMA_1887_LEY_27269_Modificada_por_LEY_27310.pdf

CNUDMI. (1996). *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno.* New York. Recuperado el 25 de abril de 2021, de: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf

CNUDMI. (2017). *Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos.* New York. Recuperado el 25 de abril de 2021, de: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/mletr_ebook_s.pdf

CNUDMI. (2001). *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno.* New York. Recuperado el 25 de abril de 2021, de: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/ml-elecsig-s.pdf>

Congress of the United States of America. (2000). *ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT.* Estados Unidos. Recuperado el 28 de abril de 2021, de:

<https://www.govinfo.gov/content/pkg/PLAW-106publ229/html/PLAW-106publ229.htm>

Chomczyk, Andrés. (2020). Regulación de blockchain e identidad digital en América Latina El futuro de la identidad digital. BID, BID LAB, DIDI, AB, LACCHAIN. Recuperado el 3 de mayo de 2021, de: <https://publications.iadb.org/publications/spanish/document/Regulacion-de-blockchain-e-identidad-digital-en-America-Latina-El-futuro-de-la-identidad-digital.pdf>

Departamento de Certificadores de Firma Digital Dirección de Gobernanza Digital Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2018). *Política de Certificados para la jerarquía nacional de certificadores registrados, versión 1.2 de 21 de Febrero 2018*.

EU Blockchain Observatory Forum. (2019). *Blockchain and digital identity*. Recuperado el 3 de mayo de 2021, de: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

Grassi, Paul A., Garcia, Michael E., Fenton, James L. (2017). Digital Identity Guidelines. NIST Special Publication 800-63-3. NIST National Institute of Standards and Technology, U.S Department of Commerce. Recuperado de: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

Honorable Congreso de la Nación de Argentina. (2001). *Ley 25.506 de 2001 Ley de Firma Digital*. Promulgada de Hecho: Diciembre 11 de 2001. Recuperado el 27 de abril de 2021, de: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/texact.htm>

Ministerio de Ciencia y Tecnología. (2006). *Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 33018*. San José Costa Rica. Recuperado el 20 de abril de 2021, de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=56884

OECD. (2007). *Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*. OECD Committee for Information, Computer and Communications Policy (ICCP). Recuperado el 25 de abril de 2021, de <https://www.oecd.org/sti/ieconomy/38921342.pdf>

PARLAMENTO Y CONSEJO EUROPEO. (2014). *REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE*. Recuperado el 25 de abril de 2021, de: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014R0910>

Peña Valenzuela, Daniel. (2015). *De la firma manuscrita a las firmas electrónica y digital: Derecho internacional de los negocios*. Tomo V. Universidad Externado. Edición de Kindle.

Presidencia de la República de Colombia. (2012). *Decreto 2364 de 2012 Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones*. Colombia. Recuperado el 22 de abril de 2021, de: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50583#2364>

Procuraduría General de la República. 2004. *Sobre el Principio de Neutralidad Tecnológica en las Compras Públicas*, OJ-083-204. San José.

Real Academia Española. (s.f.). Firma. En *Diccionario de la lengua española*. Recuperado el 10 de abril de 2021, de <https://dle.rae.es/firma?m=form>

Real Academia Española. (s.f.). Rúbrica. En *Diccionario de la lengua española*. Recuperado el 10 de abril de 2021, de <https://dle.rae.es/r%C3%BAbrica>

Robles Llorente, Miguel A. (2015). *La escritura y la firma manuscrita como elementos coadyuvantes de la seguridad documental*. (Tesis de Doctorado). Universidad Autónoma de Barcelona. Recuperado el 28 de marzo de 2021, de <https://www.tesisenred.net/bitstream/handle/10803/315287/marl.pdf?sequence=1;La>

Sala Tercera de la Corte Suprema de Justicia. (2019). *Resolución N° 229-2019, de las 12:00 horas del 22 de febrero de 2019*. Recuperado de: <https://nexuspj.poder-judicial.go.cr/document/sen-1-0006-910187>

Torres Torres, Ana Y. (2012). *Principios Fundamentales del Comercio Electrónico y su desarrollo legislativo en Colombia y Latinoamérica*. Universidad de Los Andes. Editorial Temis. Bogotá, Colombia.

Tribunal Primero Civil. (2009). *Resolución N° 2009-00293 de las ocho horas cinco minutos del diecisiete de abril de dos mil nueve*, San José, Costa Rica.

Uniform Law Commission. (1999). *UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)*. Estados Unidos. Recuperado el 25 de abril de 2021, de: <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile>

[e.ashx?DocumentFileKey=2c38eebd-69af-aafc-ddc3-b3d292bf805a&forceDialog=0](#)

TRIBUNA LIBRE

EDICIÓN
DIGITAL

Edición 8/1, Octubre 2021
Costa Rica