

Mensaje de Datos y Firmas Electrónicas: Breves reflexiones sobre los ordenamientos jurídicos de Argentina y Venezuela

María Alejandra Ruiz Gómez*

RVDM, Nro. 7, 2021, pp-197-218

Resumen: Nadie estaba preparado para afrontar esta “nueva realidad”. La pregunta sería, ¿nuestros ordenamientos jurídicos tampoco? El incremento exponencial del uso de los medios tecnológicos nos hace virar la atención a la normativa que regula los elementos de una negociación electrónica, así como, a desempolvar algunas nociones que se creían olvidadas. A través del presente artículo haremos unas breves reflexiones sobre la Ley No. 25.506 de Firmas Digitales y la Ley Sobre Mensaje de Datos y Firmas Electrónicas, a fin de verificar sus diferencias, semejanzas, y su concordancia con los principios rectores del comercio electrónico.

Palabras claves: Mensaje de datos, documentos electrónicos, documentos digitales, firmas electrónicas, firmas digitales, tecnología, derecho.

Data Message and Electronic Signatures: Brief reflections on the legal systems of Argentina and Venezuela

Abstract: *No one was prepared to face this “new reality”. The question is, were our legal systems not prepared either? The exponential increase in the use of technological means makes us turn our attention to the rules that regulate the elements of an electronic negotiation, as well as to dust off some notions that were thought to have been forgotten. Through this article we will make some brief reflections on Law No. 25,506 on Digital Signatures and the Law on Data Messages and Electronic Signatures, in order to verify their differences, similarities, and their concordance with the guiding principles of electronic commerce.*

Keywords: *Data message, electronic documents, digital documents, electronic signatures, digital signatures, technology, law.*

Recibido: 11/11/2021

Aprobado: 04/12/2021

* Abogada *Magna Cum Laude* de la Universidad Central de Venezuela (2015) con Diplomado en Contratos y Litigios Internacionales de la Universidad Austral (2020). Asociada del Departamento de Resolución de Controversias de Baker Mckenzie Venezuela. Profesora de Teoría General del Proceso de la Universidad Monteávila. Directora del Instituto Venezolano de Derecho y Tecnología (INVEDET). Miembro de la Asociación Americana de Derecho Internacional Privado (ASADIP) y de otras asociaciones nacionales e internacionales. Tesista de la Maestría en Derecho Internacional Privado y Comparado de la Universidad Central de Venezuela. En el año 2020 fue nominada por Chambers and Partners en la categoría de "D&I Future Líder (South América)" y, de igual forma, ha sido reconocida por el prestigioso directorio Legal 500 como "Rising Star" de su área de práctica.

Mensaje de Datos y Firmas Electrónicas: Breves reflexiones sobre los ordenamientos jurídicos de Argentina y Venezuela

María Alejandra Ruiz Gómez*

RVDM, Nro. 7, 2021, pp-197-218

SUMARIO:

INTRODUCCIÓN. *1. Principios rectores de las regulaciones tecnológicas. 1.1. Equivalencia funcional. 1.2. Neutralidad tecnológica. 1.3. No discriminación de las firmas electrónicas extranjeras. 2. Argentina y Venezuela. 2.1. Principios que rigen sus textos normativos. Equivalencia Funcional, Neutralidad Tecnológica. 2.2. Diferencias entre los distintos términos utilizados en los textos normativos. a. ¿Mensaje de datos o Documentos Electrónicos? b. Documento Digital/ Mensaje de Datos: Argentina/Venezuela. c. ¿Firmas Electrónicas o Firmas Digitales? d. Firma electrónica/Firma digital: Argentina/Venezuela. 3. No discriminación de firmas electrónicas extranjeras.* CONCLUSIÓN. BIBLIOGRAFÍA.

INTRODUCCIÓN

La evolución tecnológica ha sido un proceso de nunca parar, no obstante, en la actualidad parece estar más presente que nunca. A lo largo de la historia, hemos observado cómo el Derecho se ha tenido que adaptar a los cambios sociales, quedando, en no pocas oportunidades, rezagado e inocuo para afrontar las nuevas realidades. Razón por la cual, a fin de buscar una solución óptima, doctrinarios se han encargado de verificar la idoneidad de las regulaciones existentes para determinar la necesidad de una nueva regulación. Sin embargo, tomando en cuenta la realidad actual, ¿podríamos afirmar que los distintos ordenamientos jurídicos no se encuentran preparados para afrontar lo que estamos viviendo hoy día?

* Abogada *Magna Cum Laude* de la Universidad Central de Venezuela (2015) con Diplomado en Contratos y Litigios Internacionales de la Universidad Austral (2020). Asociada del Departamento de Resolución de Controversias de Baker McKenzie Venezuela. Profesora de Teoría General del Proceso de la Universidad Monteávil. Directora del Instituto Venezolano de Derecho y Tecnología (INVEDET). Miembro de la Asociación Americana de Derecho Internacional Privado y Comparado de la Universidad Central de Venezuela. En el año 2020 fue nominada por Chambers and Partners en la categoría de "D&I Future Líder (South América)" y, de igual forma, ha sido reconocida por el prestigioso directorio Legal 500 como "Rising Star" de su área de práctica.

Pareciera que en la actualidad estamos viviendo un fenómeno indescriptible de crecimiento exponencial en el uso de las tecnologías. La utilización de videollamadas, mensajes instantáneos, correos electrónicos, redes sociales y plataformas tecnológicas en general, se ha multiplicado por el estado actual de circunstancias. Las medidas como el distanciamiento social, la paralización de las actividades laborales y la restricción de la movilización, tanto a nivel interno como externo, han provocado la búsqueda de soluciones para evitar un colapso económico. En este sentido, en virtud del COVID-19 las empresas han podido observar con mayor claridad las ventajas de las herramientas tecnológicas, ya existentes, para la continuación de los negocios, por lo que, su uso, más que una alternativa se convirtió en una obligación.

Sería irónico pensar que nos encontramos en una situación de novedad y que, por lo tanto, nuestras regulaciones no se encuentran preparadas para afrontar esta realidad, cuando es necesario desempolvar nociones que se encuentran vigentes desde el año 1996. Para ese entonces, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (“CNUDMI”) tomó en consideración que el comercio a nivel mundial se estaba adaptando a una nueva realidad, por lo que, diversos países de la región prepararon sus respectivos ordenamientos jurídicos basándose en la Ley Modelo de la CNUDMI sobre Comercio Electrónico (“LMSCE”), la cual fue el primer¹ instrumento en incorporar los principios base para la regulación tecnológica actual.² En este sentido, la nota explicativa de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas (“LMFE”) indica que la preparación de la Ley Modelo sobre Comercio Electrónico “*a comienzos del decenio de 1990 fue consecuencia del creciente empleo de medios modernos de comunicación, tales como el correo electrónico y el intercambio electrónico de datos (EDI) para la realización de operaciones comerciales internacionales. Se vio que las nuevas tecnologías se habían desarrollado con rapidez y seguirían desarrollándose a medida que continuara difundándose el acceso a soportes técnicos como las autopistas de la información y la Internet.*” Por lo cual, la CNUDMI previó en el año 1996 que nos encontrábamos frente a una evolución provocada por la tecnología, y en especial, por el empleo de nuevos medios de comunicación, que debía ser regulado.

Así, para el año 1996 se incorporó i) el principio de neutralidad tecnológica y ii) el principio de equivalencia funcional. El primero de ellos consiste en el reconocimiento de la eficacia de las tecnologías existentes y las que están por existir, mientras que el

¹ En este sentido, ver la obra de la Prof. Claudia Madrid Martínez “Medios electrónicos de pago en comercio internacional”. Revista Venezolana de Legislación y Jurisprudencia. Caracas, 2018. p. 137 quien indica que el Principio de Equivalencia Funcional fue expresamente reconocido por primera vez en la LMSCE.

² Tanto ha sido el éxito de esta Ley Modelo que, de acuerdo a la información suministrada por la página web de la CNUDMI, 74 países se han inspirado en la misma. Para ver la situación actual y los países que la han incorporado a su regulación interna: https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce/status

segundo, consiste en otorgarle la misma eficacia jurídica a toda la información que se encuentre contenida en un mensaje de datos, tal y como se le otorga a un documento escrito. No obstante, adicionalmente a estos principios, a las leyes modelos posteriores³ se les sumó un principio poco comentado en la práctica, empero, a juicio de esta autora, importante en virtud de la internacionalidad de los negocios actuales, el cual sería, el principio de no discriminación de las firmas electrónicas extranjeras.

1. Principios rectores de las regulaciones tecnológicas

1.1. Equivalencia funcional

De acuerdo a la LMSCE, el principio de equivalencia funcional consiste en analizar la función que tiene la presentación de un documento escrito a fin de determinar la forma de satisfacer dicha función mediante la presentación de un documento creado a través de medios electrónicos. Sin pretender que la información creada a través de medios electrónicos sea el equivalente de un documento de papel, ya que su naturaleza es distinta. Lo único equivalente sería la función de ambas. En este sentido, la LMSCE no pretende definir un equivalente informático para todos los documentos escritos, sino que se busca determinar la función básica de cada uno de los requisitos de forma de la documentación sobre papel, con miras a determinar los criterios que, de ser cumplidos, permitirían un reconocimiento legal equivalente.

1.2. Neutralidad tecnológica

Por su parte, de acuerdo a la Ley Modelo CNUDMI sobre Firmas Electrónicas⁴ la neutralidad tecnológica hace referencia a la no discriminación de las herramientas tecnológicas utilizadas para comunicar o archivar de forma electrónica la información, ello tomando en cuenta la velocidad de los desarrollos tecnológicos. Por lo tanto, se pretende no sólo reconocer las tecnologías existentes, sino también abarcar a aquellas

³ Principalmente en la Ley Modelo sobre Firmas Electrónicas (2001). Así mismo la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales lo reconoce al expresar en su nota explicativa “De por sí, el lugar de origen de una firma electrónica no debería ser, en modo alguno, un factor determinante de que los certificados extranjeros o las firmas electrónicas deban reconocerse susceptibles de tener eficacia jurídica en un Estado Contratante, y en qué medida. La determinación de si una firma electrónica puede tener eficacia jurídica, o del grado en que pueda tenerla, no debería depender del lugar en que se haya creado la firma electrónica o del lugar en que se encuentre la infraestructura (jurídica o de otro tipo) que respalde la firma electrónica, sino que debe depender de su fiabilidad técnica.” Por su parte la Ley Modelo sobre Documentos Transmisibles Electrónicos (2017) no se refiere expresamente a la no discriminación de las firmas electrónicas extranjeras, sino a la no discriminación de los documentos transmisibles electrónicos extranjeros.

⁴ Para mayor información respecto a la Ley Modelo CNUDMI sobre Firmas Electrónicas consultar: https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_signatures#:~:text=La%20Ley%20Modelo%20sobre%20las%20Firmas%20Electr%C3%B3nicas%20se%20basa%20en,t%C3%A9cnicos%20y%20la%20equivalencia%20funcional.

que estén por existir en virtud de las innovaciones tecnológicas. En este sentido, la reciente Ley Modelo sobre Documentos Electrónicos Transmisibles⁵, al referirse al principio de neutralidad tecnológica, señala que al adoptar un enfoque neutral es posible recurrir a tecnologías novedosas, tales como, las de base registral, tokens, o registros descentralizados, lo que actualmente se conoce como tecnología blockchain.

1.3. No discriminación de las firmas electrónicas extranjeras

De acuerdo a la Ley Modelo sobre Firmas Electrónicas, este principio implica eliminar aquellas normas que no permiten el reconocimiento de una firma electrónica en virtud de i) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica, ii) el lugar en el que se encuentre el establecimiento del expedidor o del firmante. Por lo tanto, el lugar de origen no debe ser en ningún caso considerado un factor determinante para el reconocimiento de la eficacia jurídica de los certificados extranjeros o las firmas electrónicas extranjeras, en este sentido, la Ley Modelo señala 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.” De esta forma, la Ley Modelo señala que, para que una firma extranjera o certificado extranjero produzca los mismos efectos jurídicos que una firma nacional deberá presentar “un grado de fiabilidad sustancialmente equivalente” y que, para ello, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente. Adicionalmente, se señala que, con base en este principio, las partes podrán acordar la utilización de determinados tipos de firmas electrónicas o certificados y se deberá reconocer que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el mismo no sea válido o eficaz conforme al derecho aplicable. Por lo tanto, con este principio no se afecta a las normas de Derecho Internacional Privado.

En este sentido, todo ordenamiento jurídico que esté regido bajo dichos principios, podría perfectamente afrontar las novedades tecnológicas que se presenten respecto a las negociaciones electrónicas o al comercio electrónico en general, puesto que, buscan abarcar de manera omnicompreensiva cualquier supuesto de hecho sin restricciones. Así, el autor Morles Hernández señala que “si algo llama la atención de la actividad legislativa en materia de comercio electrónico y firma electrónica es el empeño de juristas y expertos en tecnologías informáticas por plasmar en fórmulas omnicompreensivas y sencillas los principales conceptos que se manejan en esta materia,

⁵ Para consultar la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos https://www.uncitral.org/pdf/spanish/texts/electcom/MLETR_ebook_S.pdf

para que cualquier persona, en cualquier parte del mundo, tenga la seguridad de que se están manejando las mismas ideas”⁶. La pregunta sería, si los ordenamientos jurídicos de Argentina y Venezuela se basan en los mismos principios.

2. Argentina y Venezuela

2.1. Principios que rigen sus textos normativos. Equivalencia Funcional, Neutralidad Tecnológica

Al realizar una revisión de ambos textos normativos, es notoria la diferencia en el ámbito de aplicación de ambas leyes. La Ley sobre Mensaje de Datos y Firmas Electrónicas venezolana tiene por objeto otorgar y reconocer eficacia y valor jurídico, tanto a la Firmas Electrónicas como a los Mensaje de Datos y, en general, a toda información inteligible en formato electrónico i) independiente del soporte material, e ii) independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. En este sentido, se puede apreciar que la Ley se inspira en la LMSCE y tiene como principios rectores, tanto a la equivalencia funcional como a la neutralidad tecnológica. Adicionalmente, la Exposición de Motivos señala que la misma se regirá por los principios de i) respeto a las formas documentales existentes, por lo que no se obliga a la utilización de la firma electrónica en lugar de la manuscrita, es decir, su utilización es voluntaria, ii) respeto a las firmas electrónicas preexistentes, iii) otorgamiento y reconocimiento jurídico de los Mensajes de Datos y las Firmas Electrónicas, iv) no discriminación del mensaje de datos firmado electrónicamente, buscando garantizar su fuerza ejecutoria, el efecto o la validez jurídica de una firma electrónica que no sea cuestionado por el solo motivo de que se presente bajo la forma de mensaje de datos, v) libertad contractual, reconociendo la autonomía de la voluntad de las partes al decidir utilizar las herramientas tecnológicas y en consecuencia, permite a las partes la escogencia de la modalidad de sus transacciones. En este sentido, se indica que las normas que se encuentren en dicha Ley deberán ser “desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas”.⁷

⁶ Morles Hernández, Alfredo (2001). Introducción. En: La Regulación del Comercio Electrónico en Venezuela. Academia de Ciencias Políticas y Sociales. Anauro Ediciones, C.A., Caracas, Venezuela. p. 14

⁷ Artículo 1.- El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos. El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas. La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que,

La Ley argentina No. 25.506 de Firma Digital, por su parte, tiene por objeto⁸ sólo reconocer la eficacia jurídica de la firma electrónica y la firma digital, sin referirse al otorgamiento o el reconocimiento de eficacia jurídica a los Mensajes de Datos, Documentos Electrónicos o Documentos Digitales. No obstante, al hacer una verificación de los artículos, si bien no se señala que se reconoce la validez y eficacia de los documentos digitales, en el Artículo 6⁹ se reconoce que el documento digital satisface el requerimiento de escritura. Así, en sentencia del 3 de septiembre de 2015, el Cámara Nacional de Apelaciones estableció:

“el art. 6 de la ley 25.506 establece que un documento digital satisface el requerimiento de escritura sin que sea menester, en este caso, formular distingo entre firma electrónica y firma digital, admitida como quedó por la accionante la recepción de los correos electrónicos referidos (...) véase que ahora, en línea con lo normado en el art. 6 de la denominada Ley Modelo de Firma Electrónica de la UNCITRAL (United Nations Commission on International Trade), el Código Civil y Comercial de la Nación Fecha de firma: 03/09/2015 autoriza la expresión escrita “por instrumentos firmados o no firmados (...) en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos” (art. 286).”¹⁰

De igual forma se señala que, cuando la ley requiera una firma manuscrita, dicha exigencia quedará satisfecha por una firma digital¹¹; por lo que se evidencia que la ley se rige por el principio de equivalencia funcional, en concordancia con los principios de la CNUDMI.

A pesar de ello, respecto al principio de neutralidad tecnológica, pareciera no ser tan amplia como la ley venezolana, si bien la ley venezolana señala expresamente que no se inclina a una determinada tecnología para las firmas y certificados electrónicos, la ley argentina no dice nada al respecto, sino que deja abierta la posibilidad de utilizar cualquier medio electrónico para la creación de una firma electrónica la cual, como veremos posteriormente, requiere menos requisitos legales para su validez. Así mismo, la Ley se limita a indicar en su Artículo 2 que los procedimientos de Firma Digital y verificación serán los determinados por la Autoridad de Aplicación en consonancia

de conformidad con la ley, requieran determinados actos o negocios jurídicos.

⁸ “**ARTICULO 1º** — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.”

⁹ “**ARTICULO 6º** — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.”

¹⁰ 27761/2011 - E-CORP S.A. c/ ADECCO ARGENTINA S.A. s/ORDINARIO. Disponible en: <http://public.diariojudicial.com/documentos/000/064/504/000064504.pdf>

¹¹ **ARTICULO 3º** — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

con estándares tecnológicos internacionales vigentes.¹² Empero, en lo que respecta al documento digital si se indica que se reconocen independientemente del soporte utilizado para su fijación, almacenamiento o archivo. Por lo que, a pesar de no indicarlo expresamente, el texto de sus normas no favorece a una determinada tecnología, ni para el documento digital ni para las firmas y certificados electrónicos¹³, por lo cual, se puede apreciar que la misma se rige también por el principio de la neutralidad tecnológica. Ahora bien, la ley argentina no hace referencia alguna respecto al resto de los principios en los que se basa la ley venezolana, no obstante, se observa que i) no obliga a ninguna de las partes a la utilización de la firma digital, y de acuerdo al autor Miguel Luis Jara “permite a las partes convenir la modalidad de sus transacciones”¹⁴, en este sentido, se respeta la libertad contractual.

2.2. Diferencias entre los distintos términos utilizados en los textos normativos

a. ¿Mensaje de datos o Documentos Electrónicos?

Términos como “mensajes de datos” y “firmas electrónicas” resultaron ser los más adecuados para definir los elementos que forman parte de una transacción electrónica, por lo que, es común verlos en los distintos instrumentos normativos latinoamericanos debido a la influencia que la Ley Modelo sobre Comercio Electrónico ha tenido en nuestro continente, específicamente en países como Venezuela, Colombia, Ecuador, Paraguay, Honduras, Panamá, México, República Dominicana, Trinidad y Tobago, parte de Canadá y Estados Unidos. Empero, a pesar de ser los términos más comunes, existen términos adicionales que pudieran crear confusiones al momento del estudio del tema y que deben ser analizados.

De acuerdo con la i) Ley Modelo sobre Comercio Electrónico y ii) la Ley Modelo Sobre Firmas Electrónicas, se entiende por mensajes de datos ***“la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos***

¹² **ARTICULO 2º** — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. a. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

¹³ Jara, Miguel Luis (2019) “La Ley de Firma Digital en Argentina. Análisis del marco normativo nacional y sus problemáticas”, Ratio Iuris, Revista de Derecho Privado. Año VII, Nº 2, Universidad de Ciencias Empresariales y Sociales, pp. 156-197.

¹⁴ Jara, Miguel. La Ley de Firma Digital...p. 160.

(EDI), el correo electrónico, el telegrama, el télex o el telefax”. Del mismo modo, la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales incluye la misma definición, con la única diferencia que agrega, a su vez, los “medios magnéticos”¹⁵. Básicamente, se refiere a toda información generada y transmitida de forma electrónica, “incluyendo textos, sonidos e imágenes”.

No obstante, la Convención agrega el término “*Comunicaciones Electrónicas*”, puesto que es el objeto principal de regulación de la Convención, y en este sentido indica que, se entenderá por “Comunicación”, “*toda exposición, declaración, reclamación, aviso o solicitud, incluida una oferta y la aceptación de una oferta, que las partes hayan de hacer o decidan hacer en relación con la **formación o el cumplimiento de un contrato***”; de esta forma, “Comunicación electrónica” será “*toda comunicación que las partes hagan por medio de mensajes de datos*”. En consecuencia, se empiezan a distinguir los Mensajes de Datos de las Comunicaciones Electrónicas, ya que éstas no sólo se generan y transmiten por medios electrónicos, sino que, se realiza con ocasión a un contrato, específicamente, en relación con la formación o el cumplimiento de un contrato entre las partes. Haciendo la salvedad, que no se trata de cualquier contrato, sino de un contrato de naturaleza comercial.¹⁶

Por su parte, la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos agrega un nuevo término que genera confusión como lo es el de “Documento Electrónico”, el cual se entiende como toda “información generada, comunicada, recibida o archivada por medios electrónicos, **incluida, cuando proceda, toda la información lógicamente asociada o vinculada de alguna otra forma a ella de modo que forme parte del documento**, se haya generado simultáneamente o no”. En este texto, no se hace referencia alguna al término Mensaje de Datos, no obstante, en la nota explicativa se señala que la definición del Documento Electrónico se basa en la definición de Mensaje de Datos que se encuentra en la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Empero, se utilizó un término distinto con el fin de aclarar

¹⁵ “Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos, el correo electrónico, el telegrama, el télex o el telefax”

¹⁶ “1. La presente Convención no será aplicable a las comunicaciones electrónicas relacionadas con:

- a) Contratos concluidos con fines personales, familiares o domésticos;
- b) i) Operaciones en un mercado de valores reglamentado; ii) operaciones de cambio de divisas; iii) sistemas de pago interbancarios, acuerdos de pago interbancarios o sistemas de compensación y de liquidación relacionados con valores bursátiles u otros títulos o activos financieros; iv) la transferencia de garantías reales constituidas sobre valores bursátiles u otros títulos o activos financieros que obren en poder de un intermediario y que puedan ser objeto de un acuerdo de venta, de préstamo, de tenencia o de recompra.

2. La presente Convención no será aplicable a las letras de cambio, pagarés, cartas de porte, conocimientos de embarque o resguardos de almacén, ni a ningún documento o título transferible que faculte a su portador o beneficiario para reclamar la entrega de las mercancías o el pago de una suma de dinero.”

que los Documentos Electrónicos i) pueden contener información de carácter compuesto, es decir, ii) se incluye, dentro de la definición, toda la información lógicamente asociada o vinculada a la información generada, comunicada, recibida o archivada por medios electrónicos, iii) que incluso la información asociada o vinculada puede ser anterior o posterior a la información generada, comunicada, recibida o archivada por medios electrónicos.

De estas tres definiciones, podemos observar que la más amplia es la que ofrece la LMSCE, por lo tanto, la relación existente entre el Mensaje de Datos y la Comunicación Electrónica o Documento Electrónico es de continente a contenido. Ahora bien, a pesar de que la Ley Modelo sobre Documentos Transmisibles Electrónicos quiso agregar un elemento distintivo al término Documento Electrónico, lo cierto es que en la práctica dicho término se utilizaba como sinónimo al de Mensaje de Datos, y es que siguiendo a la autora Ana María Mesa Elnesser “hablar de documentos electrónicos, mensajes de datos y soporte digital de la información de actos y contratos pueden ser utilizados como sinónimos para los fines de instrumento documental”¹⁷.

No obstante, la autora Patricia Ramos señala que se deben diferenciar los términos Mensaje de Datos y Documentos Electrónicos, puesto que, el Mensaje de Datos constituye un Documento Electrónico sólo cuando ese intercambio de información produce efectos jurídicos, en este sentido, “*todo documento electrónico es un mensaje de datos, pero no todo mensaje de datos es un documento electrónico.*”¹⁸

Ahora bien, existen instrumentos normativos y ordenamientos jurídicos que ni siquiera hacen referencia al término Mensaje de Datos, sino que prefieren y, consideran más adecuado, utilizar solamente el término Documento Electrónico o Documento Digital. En este sentido, la Resolución No. 37/96 sobre el Reconocimiento de la Eficacia Jurídica del Documento Electrónico, la Firma Electrónica y la Firma Electrónica Avanzada en el Ámbito del Mercosur (“Resolución No. 37/96”)¹⁹, señala que el Documento Electrónico y Documento Digital se utilizan indistintamente y que se refieren a la “**representación digital de actos o hechos** con independencia del soporte utilizado para su fijación, almacenamiento o archivo”.

¹⁷ Mesa Elnesser, Ana María, (2017) “Cifrado de extremo a extremo de Whatsapp: un análisis a partir de la prueba documental”, en: Agudelo Mejía, D; Pabón Giraldo, M; Toro Garzón, L., Bustamante Rúa, M.; Vargas Vélez, O (Coords.) *Derecho procesal contemporáneo: perspectivas y desafíos*, Universidad de Medellín, Edición: Primera, Colombia.

¹⁸ Ramos Perez, Patricia, (2011), “Reconocimiento del Documento Electrónico Certificado Extranjero”, consultado: http://saber.ucv.ve/bitstream/123456789/3755/1/T026800004916-0-patriciaramos_finalpublicacion-000.pdf el 8/7/2020.

¹⁹ Texto disponible en: <http://www.sice.oas.org/trade/mrcsrs/resolutions/Res3706.pdf>

b. Documento Digital/ Mensaje de Datos: Argentina/Venezuela

Al haber analizado los términos que se encuentran en los distintos textos normativos antes señalados, de acuerdo con los ordenamientos jurídicos objeto del presente estudio, ¿cuál sería entonces el término más idóneo? La Ley argentina N° 25.506 de Firma Digital, a pesar de tener la misma definición que la Resolución No. 37/96 prefiere la utilización del término “Documento Digital” y en consecuencia señala en su Artículo 6 que “Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo...”. En este sentido, a lo largo de su texto no se hace referencia alguna al término Mensaje de Datos, pese a que autores señalan que se tomó en cuenta a la LMSCE como un antecedente importante para la redacción de la misma²⁰.

No obstante, ¿por qué a pesar de tener la misma definición de la Resolución No. 37/96 el legislador argentino prefirió el término Documento Digital? De acuerdo con Jorge Oscar Rossi²¹ los especialistas consideran que es el término más adecuado, por lo que, correspondería referirse a documento digital y no a documento electrónico en virtud de que el procesamiento informático consiste en procesar dígitos binarios y no electrones. En consecuencia, el autor señala que el vocablo electrónico “*se utiliza erróneamente, a pesar de su popularidad*”.

Así, el Documento Digital según Jorge Oscar Rossi “es una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información (actos, hechos o datos), con independencia del soporte utilizado para almacenar o archivar dicha información”, y a pesar de existir distintas modalidades de almacenamiento y transmisión, el documento no pierde su cualidad numérica, es decir digital, es por ello que, los especialistas consideran dicho término es el más conveniente²². No es objetivo de este artículo entrar a discutir los detalles técnicos del Documento Digital, puesto que también, así como lo indica el autor, esta tecnología resulta un tanto novedosa para los abogados. No obstante, es notoria la divergencia de términos utilizados a lo largo de los ordenamientos jurídicos latinoamericanos e incluso la errónea utilización de los mismos en nuestra práctica.

²⁰ Márquez, José F. (2002), “Introducción a la obra “Ley de Firma Digital Argentina”, Abeledo Perrot, Buenos Aires, consultado en [http://www.cea.unc.edu.ar/acaderc/doctrina/articulos/la-ley-de-firma-digital-argentina/at_download/file] el 8/7/2020

²¹ Oscar Rossi, Jorge (2007), “Documento y firma digital: para entrar en tema”, consultado en: http://www.saij.gob.ar/doctrina/dacf080089-rossi_documento_firma_digital_para.htm el 8/7/2020.

²² Oscar Rossi, J (2007), “Documento y firma digital: para entrar en tema”, consultado en: http://www.saij.gob.ar/doctrina/dacf080089-rossi_documento_firma_digital_para.htm el 8/7/2020.

Ahora bien, el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas venezolana, prefiere a su vez, la utilización del término Mensaje de Datos, señalando que su principal objetivo es “adoptar un marco normativo que avale los desarrollos tecnológicos sobre seguridad en materia de comunicación y negocios electrónicos, para dar pleno valor jurídico a los mensajes de datos que hagan uso de estas tecnologías”. Por lo tanto, se define al Mensaje de Datos como “toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio”. Es clara la influencia que tuvo la LMSCE sobre la ley venezolana, sin embargo, podemos también observar que la definición de mensaje de datos no es la misma, agregando que la información tiene que ser inteligible. La razón de ello según el autor venezolano Pedro Jedlicka estriba en que se busca evitar establecer limitaciones para asumir una “posición tecnológicamente neutra”²³ que tienda a impedir la obsolescencia de la normativa.

Sin duda, entre la ley venezolana y la ley argentina existen diferencias tanto en los términos como en la redacción de la definición de dichos términos. La primera se enfoca en definir el objeto de lo que se debe entender por Mensaje de Datos, lo cual sería toda información inteligible en formato electrónico o similar; mientras que, la segunda busca resaltar el objetivo del documento digital, el cual es representar digitalmente actos y hechos.

c. ¿Firmas Electrónicas o Firmas Digitales?

Pareciera no haber tantas diferencias respecto al significado de firma electrónica entre los distintos instrumentos normativos. Para la Ley Modelo sobre Firmas Electrónicas, son aquellos “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”. De igual forma, la Resolución No. 37/96 señala que son aquellos “datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados por el firmante como medio de identificación”. En ambos conceptos prevalecen los siguientes elementos; i) son datos en forma electrónica, ii) utilizados para identificar al firmante, iii) asociados a otros datos electrónicos o a un mensaje de datos.

²³ Jedlicka, Pedro. (2004) “Comentarios de los Mensajes de Datos como Medios de Prueba”. En: Aspectos Legales del Comercio Electrónico. Caracas. Cámara Venezolana de Comercio Electrónico. pp. 177-198

Así, la LMSFE señala que dentro del concepto de firmas electrónicas se encuentran tanto i) las firmas numéricas basadas en la criptografía de la clave pública o privada, como, ii) aquellas firmas electrónicas basadas en técnicas distintas de la criptografía de la clave pública, a saber, las que se realizan a través de dispositivos biométricos, las que se basan en el uso de número de identificación personal, versiones digitalizadas de firmas manuscritas, o simplemente la selección de un signo afirmativo en la pantalla electrónica mediante el ratón. Por lo cual, engloba de manera genérica las distintas técnicas con el fin de no limitar o discriminar el uso de ninguna tecnología.

No obstante, en otros textos normativos podemos observar la referencia a la Firma Electrónica Avanzada o incluso a la Firma Digital. En este sentido la Resolución No. 37/96 utiliza indistintamente los términos Firma Electrónica Avanzada y Firma Digital, y en consecuencia, se entiende a la Firma Electrónica Avanzada como aquella que cumple con los siguientes requisitos: “a) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca; b) ser creada por medios que el firmante pueda mantener bajo su exclusivo control; c) ser susceptible de verificación por terceros; d) estar vinculada a estos datos de tal modo que cualquier alteración subsiguiente en los mismos sea detectable; y e) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido y válido al momento de la firma.”

En este sentido, Patricia Ramos señala que existen confusiones terminológicas entre firmas electrónicas y firmas electrónicas avanzadas o digitales, por lo que es necesario determinar que “la relación entre las distintas denominaciones es de continente a contenido, siendo la firma electrónica el continente y las firmas digitales o electrónicas avanzadas el contenido”²⁴.

d. Firma electrónica/Firma digital: Argentina/Venezuela

No obstante, al remitirnos a la Ley argentina No. 25.506, también hace referencia tanto a la Firma Digital como a la Firma Electrónica, en este sentido, se señala que se entiende por Firma Digital al resultado de aplicar a un documento digital un procedimiento matemático que i) requiere información de exclusivo conocimiento del firmante, es decir, la misma debe estar bajo su absoluto control, ii) debe ser susceptible de verificación por terceras partes, iii) dicha verificación debe simultáneamente permitir identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma²⁵. Para que recaiga una presunción iuris tantum de autoría sobre la firma digital

²⁴ Ramos, Patricia, Reconocimiento del Documento Electrónico ... consultado: http://saber.ucev.ve/bitstream/123456789/3755/1/T026800004916-0-patriciaramos_finalpublicacion-000.pdf el 8/7/2020.

²⁵ “ARTICULO 2º — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un

ésta debe ser certificada, ya que a través de dicho certificado se vincula los datos de verificación de firma a su titular²⁶. Por otro lado, la Firma Electrónica es aquella que no cumple con los requisitos señalados para que se considere una Firma Digital, es decir, “aquel 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 para ser considerada firma digital”. De esta forma, se deja abierta a la posibilidad de que el signatario utilice el medio electrónico de su preferencia con el fin de crear la firma electrónica que le ayude a atribuir su autoría a un documento digital y, en consecuencia, le sirva de medio de identificación; si bien la Firma Digital prevalece sobre la Firma Electrónica, el poder judicial también le reconoce su valor, utilidad e importancia, así, la Cámara Nacional de Apelaciones en lo Comercial, en sentencia de fecha 15 de mayo de 2008 señala:

“No está de más recordar que tal clave (numérica en el caso), ostenta la calidad de firma electrónica, a la luz de lo dispuesto por la Ley 25.506 (artículo 5). Si bien no tiene los mismos efectos de la firma digital (art. 3 de la norma citada), no puede ignorarse que tal clave tiene amplio uso en nuestra vida diaria amén de tener por finalidad, bien que no única, la identificación del cliente, como ocurre con la firma ológrafa. De hecho, esta clave personal o firma electrónica es constantemente utilizada para múltiples actividades, muchas de ellas de claro contenido económico. Uso que se ha generalizado a partir de la llamada “bancarización”.”

(...)

“De igual manera que a nadie se le ocurriría entregar a un tercero un papel con su firma manuscrita y menos si tal “papel” es un formulario de cheque, lo mismo debería ocurrir con la firma electrónica y, en algún tiempo, con la ya inminente firma digital. Es posible que en nuestro país exista cierta ignorancia o, cuanto menos, una insuficiente conciencia masiva sobre la trascendencia que, en nuestra adolescente sociedad digital, tiene tanto la firma electrónica como la digital. Se trata, a mi juicio, de un cambio cultural que como tal, requiera de un tiempo mayor en tanto exige adoptar o cuanto luego consolidar, conductas que hasta el inicio de esta “era digital” eran inimaginables.”²⁷

Por su parte, la Ley sobre Mensaje de Datos y Firmas Electrónicas venezolana, señala que la firma electrónica es “aquella información creada o utilizada por el signatario, asociada al mensaje de datos, que permita atribuirle su autoría bajo el contexto en

procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.”

²⁶ “ARTICULO 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.”

²⁷ “Bieniauskas, Carlos c/ Banco de la Ciudad de Buenos Aires”. Texto disponible en: <http://www.sajj.gob.ar/camara-nacional-apelaciones-comercial-nacional-ciudad-autonoma-buenos-aires-bieniauskas-carlos-banco-ciudad-buenos-aires-fa08971926-2008-05-15/123456789-629-1798-0ots-eupmocsollaf>

el cual ha sido empleado”. Si bien en el texto de la Ley no hace distinción expresa entre Firma Electrónica y Firma Digital o Avanzada, la jurisprudencia ha establecido que en la Ley existen cuatro tipos de firmas electrónicas: Firma simple, Firma acordada, Firma avanzada y Firma digital. En este sentido, la Sala de Casación Penal del Tribunal Supremo de Justicia de Venezuela mediante sentencia N° 446 del 11 de noviembre de 2016, indicó que i) **la firma electrónica simple**, es aquella creada o utilizada por el signatario que no cumple con los requisitos señalados por la ley para homologar su validez y eficacia probatoria con los de la firma autógrafa; en este caso, la ley no desecha su utilización sino que impone su apreciación judicial conforme a las reglas de la sana crítica, ii) **la firma electrónica concordada o pactada**, es aquella que cumple con los requisitos acordados por las partes para tal efecto, en este sentido, es necesario que se demuestre en juicio el cumplimiento del acuerdo establecido por las partes para que posea la misma validez y eficacia probatoria que la firma autógrafa, en consecuencia, las partes tienen la facultad de establecer los requisitos que deberá cumplir la firma electrónica para tener el mismo valor y eficacia probatoria que la firma autógrafa, iii) **la firma electrónica calificada o avanzada**, es aquella que tiene igual validez y eficacia probatoria que la ley otorga a la firma autógrafa, únicamente si se demuestra que permite garantizar que los datos utilizados para su generación puedan producirse solo una vez, y asegurar, razonablemente, su confidencialidad; que ofrece seguridad suficiente de que no pueda ser falsificada con la tecnología existente; y que no se altera la integridad del mensaje de datos; iv) por último, **la firma electrónica certificada o firma digital** la cual es aquella que utiliza un sistema de criptografía asimétrica o de clave pública, que está certificada por un Proveedor de Servicios de Certificación, de ahí que sobre ella pesa una presunción, *iuris tantum*, de autenticidad y tiene idéntica validez jurídica que su equivalente autógrafa.²⁸ De esta forma, se le reconoce la posibilidad de adoptar el tipo de firma electrónica que desee, tal y como se indica en la nota explicativa de la LMSFE, es decir, aquellas firmas numéricas basadas en la criptografía de la clave pública o privada, como aquellas firmas electrónicas basadas en técnicas distintas de la criptografía de la clave pública, bien sea por dispositivos biométricos, número de identificación personal, versiones digitalizadas de firmas manuscritas, o simplemente la selección de un signo distintivo por las partes.

e. No discriminación de firmas electrónicas extranjeras

Una vez verificadas las diferencias existentes entre los términos utilizados en los distintos textos normativos, quedaría entonces verificar si dentro de los mismos se establece el principio de no discriminación de las firmas electrónicas extranjeras. Tal

²⁸ Texto disponible en: <https://app.vlex.com/#vid/andres-lietor-martinez-654900421>

y como señalé, de acuerdo a la Ley Modelo sobre Firmas Electrónicas, este principio consiste en eliminar aquellas normas que no permiten el reconocimiento de una firma electrónica extranjera en razón del lugar en donde se haya creado, utilizado o expedido el certificado, así como, del lugar del establecimiento del firmante o del que expide el certificado. Por lo que, la Ley Modelo indica que el no reconocimiento de una firma electrónica extranjera debería estar fundamentado por razones de fiabilidad técnica. Es indudable la cantidad de compañías que se han visto forzadas a utilizar documentos digitales o electrónicos y, en consecuencia, a la utilización de firmas electrónicas, pero no es menos cierto, que a pesar de que han transcurrido muchos años desde la publicación de la Ley Modelo sobre Comercio Electrónico y la Ley Modelo sobre Firmas Electrónicas, existe cierto escepticismo respecto al uso de estas herramientas tecnológicas y es que como indica Claudia Madrid, no existe en el mundo digital “una garantía absoluta sobre la identidad de las personas, tampoco existe seguridad sobre la no intervención de un mensaje de datos por terceros no autorizados”.²⁹

En este sentido, la Ley Modelo busca otorgar una seguridad jurídica a aquellos que utilizan firmas electrónicas, independientemente del lugar en donde se originen, así como, aquellos que necesariamente se encuentran frente a relaciones jurídicas con elementos de extranjería, puesto que es indudable la internacionalidad de los negocios actuales. Razón por la cual, considero que es uno de los principios que deben regir los textos normativos de los distintos países, pues genera una mayor confiabilidad y confianza en el uso de las firmas electrónicas. Ahora bien, respecto a la ley venezolana, los certificados electrónicos³⁰, que sean emitidos por proveedores de servicios de certificación extranjera, tendrán la misma validez y eficacia jurídica que una Firma Digital, siempre que tales certificados se encuentren garantizados por un Proveedor de Servicios de Certificación nacional debidamente acreditado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) y, por lo tanto, garantice en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos de seguridad, validez y vigencia del certificado.³¹

²⁹ Madrid Martínez, Claudia (2018) “Medios electrónicos de pago en comercio internacional”. Revista Venezolana de Legislación y Jurisprudencia. Caracas, p. 137

³⁰ Artículo 2: (...) “Certificado Electrónico: Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.”

³¹ “Artículo 44.- Los Certificados Electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida en el presente Decreto-Ley, siempre que tales certificados sean garantizados por un Proveedor de Servicios de Certificación, debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado. Los certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, carecerán de los efectos jurídicos que se atribuyen en el presente Capítulo, sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.”

No obstante, aquellos certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación nacional carecerán de los efectos jurídicos que la ley atribuye a las Firmas Digitales, empero, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica. Por lo tanto, la ley venezolana busca garantizar el cumplimiento de los requisitos de seguridad, validez y vigencia del certificado, sin tomar en cuenta el lugar de su expedición. Tanto así, que en la Exposición de Motivos se indica que el principio de otorgamiento y reconocimiento jurídico de los Mensajes de Datos y las Firmas Electrónicas “asegura el otorgamiento y reconocimiento jurídico de los mensajes de datos, las firmas electrónicas y los servicios de certificación provistos por los proveedores de servicios de certificación, **incluyendo mecanismos de reconocimiento a nivel internacional.**” Por lo que, es claro el reconocimiento del principio de no discriminación de las firmas digitales extranjeras. Sobre el resto de las firmas señaladas en el capítulo anterior, a saber, firma simple, acordada o avanzada, que se hayan originado en el extranjero, la ley no señala nada al respecto. No obstante, tomando en cuenta lo señalado en la Ley, las normas “deberán ser desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas”³².

Por su parte, la Ley argentina No. 25. 506 señala en su Artículo 16 lo siguiente:

“Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

- a. Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales **y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o**
- b. Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.”

A su vez, la Resolución No. 37/96 señala:

Art. 5- Firma electrónica avanzada: Reconocimiento Mutuo Con el objetivo de alcanzar el reconocimiento mutuo de las firmas electrónicas avanzadas y de los certificados digitales, **los Estados Partes podrán celebrar, entre sí, acuerdos de reconocimiento mutuo.** A tales efectos, el GMC aprobará las Directrices para la celebración de dichos acuerdos. Dichas Directrices reflejarán el estado de la materia al momento de su aprobación y podrán ser actualizadas a propuesta del SGT N° 13, de manera de acompañar la evolución de las tecnologías a ellas relacionadas.

³² Artículo 1 de la Ley Sobre Mensaje de Datos y Firmas Electrónicas. Ver nota al pie No. 6

A través de los Acuerdos de Reconocimiento Mutuo se otorgará a las firmas electrónicas avanzadas, que cumplan con las condiciones dispuestas en ellos, el mismo valor jurídico y probatorio que el otorgado a las firmas manuscritas. **Los Estados Partes reconocerán la autenticidad e integridad de un documento electrónico firmado con una firma electrónica avanzada, admitiéndola como prueba documental en procesos judiciales, conforme lo que se disponga en los Acuerdos de Reconocimiento Mutuo.** Los Estados Partes indicarán, en el ámbito del SGT N° 13, cuáles serán los organismos competentes habilitados para suscribir Acuerdos de Reconocimiento Mutuo.

En este sentido, el ordenamiento jurídico argentino exige, en primer lugar, que se cumplan los requisitos establecidos para los certificados nacionales, y adicionalmente, que se encuentre vigente un acuerdo de reciprocidad firmado entre la República de Argentina y el país de origen del certificado extranjero. Respecto esta disposición, la misma va en contra del principio de no discriminación de firmas electrónicas extranjeras, en virtud de que expresamente señala que se le reconocerá validez tomando como factor determinante el país donde se origina el certificado extranjero. En este sentido, si esta fuese la única norma prevista para otorgar el reconocimiento de la firma electrónica extranjera, no sólo estaría impidiendo el reconocimiento de aquellas que si tienen una fiabilidad técnica requerida, sino que se les estaría negando el reconocimiento de las firmas electrónicas a una gran cantidad de países existentes, puesto que en la actualidad Argentina sólo tiene sólo un acuerdo de reciprocidad con Chile³³ y recientemente firmó un “Acuerdo De Reconocimiento Mutuo de Certificados de Firma Digital del Mercosur”³⁴ en diciembre del 2019. No obstante, gracias a la conjunción “o” también se pueden reconocer a los certificados electrónicos extranjeros siempre que los certificados sean reconocidos por un certificador licenciado que garantice la validez y vigencia y, a su vez, sea validado por la autoridad de aplicación. Por lo que, a pesar de la primera disposición, la ley argentina abre sus puertas para el reconocimiento de certificados extranjeros a aquellos que tengan una fiabilidad técnica.

No podemos concluir sin señalar, a modo de referencia, las normas del reciente Acuerdo que permite el reconocimiento de los certificados digitales emitidos por los Estados Parte del Mercosur, el cual establece:

“Artículo 1: 1. El presente Acuerdo tiene por objeto el reconocimiento mutuo de certificados de firma digital, emitidos por prestadores de servicios de certificación acreditados o certificadores licenciados, a los fines de otorgar a la firma digital el mismo valor jurídico y probatorio que el otorgado a las firmas manuscritas, de conformidad con el respectivo ordenamiento jurídico interno de cada Parte.

³³ Texto disponible en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312884/res436.pdf>

³⁴ Mayor información en : <https://www.mercosur.int/documentos-y-normativa/normativa/> (Decisión 11/2019)

Artículo 2. 1. A los efectos del presente Acuerdo, se entenderá por “firma digital” los datos en forma electrónica resultantes de la aplicación de un proceso matemático a un documento digital, que se vale de un elemento criptográfico, que requiere información de exclusivo control del firmante, la que es asociada a una persona o entidad originaria, identificada de forma inequívoca, y emitida por un prestador de servicios de certificación acreditado por cada una de las Partes.

Artículo 3. Los certificados de firma digital emitidos en una Parte tendrán la misma validez jurídica en otra Parte, siempre que sean emitidos por un prestador de servicios de certificación acreditado conforme a las siguientes condiciones: a) que respondan a estándares reconocidos internacionalmente, conforme lo establezca la autoridad designada por cada Parte en el artículo 8; b) que contengan, como mínimo, datos que permitan:

- (i) identificar inequívocamente a su titular y al prestador de servicios de certificación que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
 - (ii) ser susceptible de verificación respecto de su estado de revocación;
 - (iii) detallar la información verificada incluida en el certificado digital;
 - (iv) contemplar las informaciones necesarias para la verificación de la firma, e
 - (v) identificar la política de certificación bajo la cual fue emitido.
- c) que hayan sido emitidos por un prestador de servicios de certificación acreditado bajo el sistema nacional respectivo de acreditación y control de las infraestructuras de claves públicas.”

El análisis de las normas anteriores escapa del objetivo del presente artículo, sin embargo, podemos destacar, i) la intención de los países del Mercosur de reconocer los certificados digitales extranjeros basados en el principio de equivalencia funcional; ii) la inclusión del elemento criptográfico en la definición de firma digital, iii) la inclusión de elementos adicionales requeridos para verificar la fiabilidad técnica del certificado digital extranjero.

CONCLUSIONES

De acuerdo con lo señalado por el autor Tomas Mann, “*sólo a través de la comparación nos distinguimos y sabemos cómo somos para convertirnos en lo que debemos ser*”³⁵. Sin embargo, tal y como indica Tatiana B. De Maekelt debemos preguntarnos *qué se debe comparar. Así como la equivalencia funcional es el principio rector de todos los instrumentos normativos que regulan los medios tecnológicos;*

³⁵ Citado en: De Maekelt B. T. (2002), “El Derecho Comparado, Ayer y Hoy”, en: Parra Aranguren, F. *Libro Homenaje A Fernando Parra Aranguren*, Facultad De Ciencias Jurídicas y Política de la Universidad Central de Venezuela, Separata del Tomo II, Caracas, p. 85

también es el principio rector del Derecho Comparado, es decir, es la guía de todos los que nos atrevemos a adentrar en un texto normativo ajeno al propio. En este sentido, “sólo un derecho comparado funcional, puede responder a las exigencias de las ciencias jurídicas modernas porque parte de una base real acorde con la problemática de cada caso concreto”³⁶. Por lo cual, a lo largo del artículo, pudimos observar que, a pesar de existir distintos términos o definiciones, todos tenían la misma función, es decir, reconocer i) la existencia de la tecnología, ii) la utilización de dicha tecnología y iii) la eficacia y validez del resultado de la utilización de dicha tecnología, en menor o mayor medida. Es importante, rescatar la importancia de los principios contenidos en los instrumentos de soft law en nuestro continente, y en nuestra normativa. Por lo cual, si bien los términos son muy importantes para conocer la materia, para utilizarlos de la mejor manera, y para evitar confusiones, lo cierto es que, podemos estar en presencia de miles de términos, pero lo importante es que regulen o busquen obtener el mismo resultado. En ocasiones el reconocimiento del otro, de sus diferencias y de sus distintos puntos de vistas para describir un fenómeno, es esencial para lograr, en el fondo, una armonización de soluciones.

BIBLIOGRAFÍA

- Barbero, O. “Introducción al Derecho Privado”. (Rosario, Editorial Juris, 2004).
- Jara, M.L. “La Ley de Firma Digital en Argentina. Análisis del marco normativo nacional y sus problemáticas”, Ratio Iuris, Revista de Derecho Privado. Año VII, N° 2, Universidad de Ciencias Empresariales y Sociales. (Buenos Aires, Universidad de Ciencias Empresariales y Sociales, 2019).
- Jedlicka, P. “Comentarios de los Mensajes de Datos como Medios de Prueba”. En: Aspectos Legales del Comercio Electrónico. (Caracas, Cámara Venezolana de Comercio Electrónico, 2004).
- Madrid Martínez, C. “Medios electrónicos de pago en comercio internacional”, Revista Venezolana de Legislación y Jurisprudencia. (Caracas, RVLJ, 2018).
- Maelkelt B. T. “El Derecho Comparado, Ayer y Hoy”, en: Parra Aranguren, F, Libro Homenaje A Fernando Parra Aranguren, Facultad De Ciencias Jurídicas y Política de la Universidad Central de Venezuela, Separata del Tomo II. (Caracas, UCV, 2002).
- Márquez, José F. “Introducción a la obra “Ley de Firma Digital Argentina”, , consultado en [http://www.cea.unc.edu.ar/acaderc/doctrina/articulos/la-ley-de-firma-digital-argentina/at_download/file] el 8/7/2020. (Buenos Aires, Abeledo Perrot, 2002).
- Mesa Elnesser, A. “Cifrado de extremo a extremo de Whatsapp: un análisis a partir de la prueba documental”, en: Agudelo Mejía, D; Pabón Giraldo, M; Toro Garzón, L., Bustamante Rúa, M.; Vargas Vélez, O (Coords.) Derecho procesal contemporáneo: perspectivas y desafíos, Edición: Primera. (Medellín, Universidad de Medellín, 2017).

³⁶ De Maelkelt B. T, El Derecho Comparado, Ayer y Hoy... p. 98

- Oscar Rossi, J. “Documento y firma digital: para entrar en tema”, consultado en: http://www.saij.gob.ar/doctrina/dacf080089-rossi_documento_firma_digital_para.htm el 8/7/2020. (Buenos Aires, 2007).
- Ramos Perez, P. “Reconocimiento del Documento Electrónico Certificado Extranjero”, consultado: http://saber.ucv.ve/bitstream/123456789/3755/1/T026800004916-0-patriciamos_finalpublicacion-000.pdf el 8/7/2020. (Caracas, UCV, 2011).
- La Red Martínez, D. L.; Valesani, M. E.; Mariño, S. I. “La Firma Digital en la Argentina”, consultado en: http://tid.ies21.edu.ar/149/me/129_149_mm.PDF el 11/7/2020.
- Sala de Casación Penal del Tribunal Supremo de Justicia, Andrés Lietor Martínez, 11/11/ 2016. Cámara Nacional De Apelaciones en lo Comercial, “Bieniauskas, Carlos c. Banco de la Ciudad de Buenos Aires”, 15/05/2008.
- Cámara Nacional De Apelaciones, “E-Corp S.A. C/ Adecco Argentina S.A. S/ Ordinario”, 3/09/2015
- Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, consultado en: https://www.uncitral.org/pdf/spanish/texts/electcom/06-57455_Ebook.pdf
- Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001, consultado en: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/ml-elecsig-s.pdf>
- Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996, consultado en: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf
- Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos, consultado en: https://www.uncitral.org/pdf/spanish/texts/electcom/MLETR_ebook_S.pdf
- Resolución No. 37/96 sobre el Reconocimiento de la Eficacia Jurídica del Documento Electrónico, la Firma Electrónica y la Firma Electrónica Avanzada en el Ámbito del Mercosur, consultado en: <http://www.sice.oas.org/trade/mrcsrs/resolutions/Res3706.pdf>
- Ley No. 25.506 de Firma Digital (texto actualizado), sancionada el 14 de noviembre 2001, promulgada de hecho el 11 de diciembre de 2001, consultada en: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/texact.htm>
- Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas, Gaceta Oficial No. 37.148, publicada el 28 de febrero de 2001, consultada en: http://www.oas.org/juridico/spanish/mesicic3_ven_anexo19.pdf
- MERCOSUR/CMC/DEC. N° 11/19, Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del Mercosur, consultado en: <https://www.mercosur.int/documentos-y-normativa/normativa/>