UCES

UNIVERSIDAD DE CIENCIAS EMPRESARIALES Y SOCIALES

Título tesis

Los desafíos de la firma digital en Argentina, el MERCOSUR y en la Unión Europea

Tesis de Doctorado en Derecho con orientación en Derecho Privado

Autor: Miguel Luis Jara

Tutor de Tesis: Graciela Ritto

Mes y año

Abril de 2022

Agradecimientos

A la UCES por abrirme sus puertas y guiarme en este camino de descubrimiento académico, a la Dra. Paola Alejandra Urbina por introducirme en el campo de la investigación, a la Dra. Graciela Ritto por la ayuda constante, al CALZ por acompañarme en mi crecimiento personal y profesional, y a la UNLZ por permitirme ser un estudiante de derecho de por vida.

RESUMEN

En los últimos años y sobre todo en el comienzo del siglo XXI, la irrupción de la firma digital y de los ecosistemas digitales que nacieron con ellas, ya sea que se trate de la República Argentina, el Mercado Común del Sur o la Unión Europea [U.E], evolucionaron exponencialmente avanzando sobre el derecho.

En este marco, surgieron las legislaciones en materia de firma digital e incluso yendo más allá con los servicios de confianza digitales expandiendo así sus posibilidades.

Actualmente se termina de establecer una suerte de falta de armonización en materia de firma digital y de los servicios que promueven la confianza digital en el MERCOSUR.

Así pues, nos propusimos conocer y analizar las legislaciones de nuestro país, del MERCOSUR y de la U.E, e identificar los elementos fundamentales de ellas para así determinar el grado de implementación de estas.

A tales fines, esperamos realizar conclusiones y propuestas para que se produzcan avances en el plano normativo digital y que este no quede rezagado atento a la velocidad con la que avanzan las nuevas tecnologías.

INDICE

Agradecimientos I

RESUMEN II

ÍNDICE DE ABREVIATURAS X

INTRODUCCIÓN 1

Capítulo I 5

Estado del Arte 5

I. Introducción 5

II. Ley de Firma Digital Argentina 5

III. Legislación en materia de firma digital en MERCOSUR 8

IV. Marco legislativo de la Unión Europea en materia de identificación electrónica y servicios de confianza 10

Capítulo II 12

Introito, evolución y avance en materia de firma electrónica 12

I. Introducción 12

II. Las revoluciones industriales 13

A. La actual revolución industrial 14

III. Avance de la informática 16

A. Derecho informático e informática jurídica 17

IV. Evolución de la firma electrónica 18

A. La firma en el derecho argentino 19

B. La firma por medios electrónicos 20

C. La firma electrónica en el derecho comparado 25

V. Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho internacional 30

VI. Aspectos generales sobre la firma electrónica avanzada 35

A. Infraestructura de firma electrónica avanzada o digital 35

B. El certificado licenciado, el certificado digital y las autoridades de registro 37

C. Tipos de certificados digitales 39

VII. Documento electrónico 40

VIII. Criptografía 42

A. Tipo de sistemas de criptografía 44

B. La función hash 46

IX. Blockchain y firma electrónica 47

A. El Blockchain en Argentina 48

X. Conclusión 50

Capítulo III 52

La firma digital en Argentina 52

I. Introducción 52

II. Generalidades 52

A. Principios generales 52

III. Antecedentes legislativos argentinos 55

IV. Ley de Firma Digital Argentina 25.506 57

A. Estructura de la Ley de Firma digital argentina 57

B. Conceptualizaciones 58

C. Diferenciación entre firma electrónica y firma digital 62

D. Naturaleza Jurídica 64

E. Documento digital en la Ley de Firma Digital argentina 64

F. De los certificados digitales y el certificador licenciado 67

G. Valor probatorio de la firma digital 68

H. La confianza digital 70

I. Firma digital y confidencialidad 72

J. Exclusiones. Marco interpretativo 72

K. La presunción de autoría 74

L. Presunción de integridad 75

V. Actualidad en materia de firma digital en argentina 76

A. Reglamentación de la Firma Digital en Argentina, Decreto Nº 182/2019 81

B. Aspectos principales del Decreto Nº 182/2019 82

VI. Firma digital en el Código Civil y Comercial de la Nación 85

A. Incorporación de nuevas tecnologías a la normativa de fondo 85

B. Problemas interpretativos derivados del uso de firma electrónica 88

VII. La firma digital en el Sector Público Nacional 90

A. La firma digital en el Sector Público Nacional 90

B. El Gobierno Electrónico en el Sector Público Nacional 96

C. Gestión Documental Electrónica 99

D. Marco legal del Sistema de Gestión Documental Electrónica 102

E. El Gobierno Abierto en el Sector Público Nacional 103

VIII. Conclusión 107

Capítulo IV 109

La firma electrónica en el MERCOSUR 109

I. Introducción 109

II. El MERCOSUR 110

A. Objetivos 112

B. El MERCOSUR en la actualidad 112

C. Organización del MERCOSUR 113

D. Acuerdos en materia de Firma electrónica en el MERCOSUR 117

III. Grupo Agenda Digital del MERCOSUR. Acuerdo de Reconocimiento mutuo de los certificados de firma digital y Acuerdo sobre comercio electrónico del MERCOSUR 119

A. Decisión N° 11/19 del Consejo Mercado Común: Reconocimiento mutuo de los certificados de firma digital 120

B. Aspectos principales del Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del Mercosur 121

C. Decisión N° 15/2021 Consejo Mercado Común. Acuerdo sobre comercio electrónico del MERCOSUR 124

IV. La Firma electrónica en el MERCOSUR 129

A. República Federativa del Brasil 130

B. República del Paraguay 135

C. República Oriental del Uruguay 144

D. El Estado Plurinacional Bolivia 150

E. República Bolivariana de Venezuela 151

VI. Estados asociados del MERCOSUR 152

A. República de Chile 152

B. República de Colombia 154

C. República del Ecuador 155

D. República Cooperativa de Guyana 156

E. República de Perú 156

F. República de Surinam 157

VII. Conclusión 158

Capítulo V 160

El Reglamento eIDAS. La Identificación Electrónica y los Servicios de Confianza en la Unión Europea 160

I. Introducción 160

II. La Unión Europea. El Tratado constitutivo de la Comunidad Europea 161

III. La Directiva 1999/93/CE: Marco regulatorio comunitario sobre la firma electrónica 162

IV. El Reglamento eIDAS (U.E.) Nº 910/2014 166

A. Origen y antecedentes 166

B. introducción al Reglamento eIDAS 169

V. Considerandos del Reglamento eIDAS 172

VI. Disposiciones generales del Reglamento eIDAS 175

A. Las definiciones en el Reglamento 176

B. El Principio de Mercado Interior, y el Reglamento 184

C. El tratamiento de la protección de datos personales en el Reglamento eIDAS 185

VII. Identificación electrónica en el Reglamento eIDAS 186

A. Reconocimiento de la Identificación Electrónica en la U.E 189

B. Las condiciones de notificación y la notificación de los sistemas de identificación electrónica 190

C. Niveles de seguridad de los sistemas de identificación electrónica 191

VIII. Servicios de confianza en el Reglamento eIDAS 192

A. Firma electrónica 193

B. Sellos electrónicos 196

C. Sello de tiempo electrónico 198

D. Servicio de entrega electrónica certificada 199

E. Autenticación de sitios web 200

IX. Los servicios de confianza cualificados 201

X. Documentos electrónicos en el Reglamento eIDAS 202

XI. Disposiciones finales 203

XII. Anexos del Reglamento elDAS 203

XIII. Modificación al Reglamento eIDAS. Perspectivas y futuro del Reglamento eIDAS 204

XIV. Conclusión 209

Capítulo VI 212

Marco Metodológico 212

I. Introducción 212

II. Antecedentes de la investigación 213

III. Planteamiento del problema y justificación 213

IV. Tipo de investigación 215

V. Unidades de análisis 215

VI. Criterio de selección de casos 216

VIII. Cumplimiento de objetivos 216

IX. Hipótesis 218

X. Tipo de diseño 219

XI. Problemas 220

XII. Estructura de la tesis 220

Capitulo VII 222

Conclusiones finales y propuestas 222

I. Conclusiones finales 222

II. Propuestas y recomendaciones 227

Bibliografía y fuentes de información 231

A. Bibliografía 231

B. Fuentes de información 234

ÍNDICE DE ABREVIATURAS

ABA American Bar Association [Barra de Abogados Americana].

ALADI Asociación Latinoamericana de Integración.

art./arts. artículo/artículos.

B.O Boletín Oficial.

cap. Capítulo.

CC Código Civil de la Nación.

CCyCN Código Civil y Comercial de la Nación.

CN Constitución Nacional.

CNUDMI Comisión de Naciones Unidas para el Derecho. Mercantil Internacional.

DNI Documento Nacional de Identidad.

DNU Decreto de necesidad y urgencia.

eIDAS electronic IDentification, Authentication and trust Services [Servicios de identificación, autenticación y confianza electrónica].

GDE Gestión Documental Electrónica.

ID Identificación.

LFD Ley de Firma Digital.

MERCOSUR Mercado Común del Sur.

ONU Organización de las Naciones Unidas

Pág. Página/páginas.

RAE Real Academia de la Lengua Española.

GDPR/RGPD Reglamento general de protección de datos personales

SigG Gesetz über Rahmenbedingungen für elektronische Signaturen – Signaturgesetz [Ley de Condiciones Marco de la Firma Electrónica - Ley de Firma].

TAD Trámites a Distancia.

TIC Tecnologías de la Información y la Comunicación.

UNCITRAL United Nations Commission on International Trade Law. [Comisión de las Naciones Unidas para el Derecho Mercantil Internacional].

U.E Unión Europea.

WWW World Wide Web [Red amplia mundial].

INTRODUCCIÓN

"El Código Civil y Comercial de la Nación es a la vida privada lo que la Constitución Nacional es a la pública" (párr.1), frase atribuida al jurista argentino Ricardo Lorenzetti (La Nación, 2015), y por nuestra parte, nos atrevemos a agregar que: "la Ley de Firma Digital lo es para vida digital de las personas".

El presente trabajo introducirá a los lectores en el mundo de la firma digital, el documento digital y los ecosistemas digitales, con especial énfasis en la República Argentina, en los países que integran el MERCOSUR, y en la U.E

En este viaje de investigación estaremos rodeados de normas con más de dos décadas de recorrido, lo que nos permite afirmar que estamos frente a un instituto relativamente joven, disruptivo en muchos casos, lleno de novedades y descubrimientos.

Establecemos que en la actualidad lo digital reina en los expedientes digitales y en los procesos judiciales, así como también en el sector público, a través del gobierno electrónico. También lo digital es la regla en el mercado electrónico a través de las transacciones electrónicas nacionales e internacionales.

Remarcamos el contexto histórico que estamos viviendo en todo el mundo. Por un lado, nos encontramos atravesando la cuarta revolución industrial, por otro lado, la pandemia ocasionada por el Covid 19 y su consiguiente cuarentena, crearon una revolución exponencial de las tecnologías y de la implementación de estas.

Podemos afirmar que estamos frente a una nueva revolución copernicana, nos encontramos frente a ideas impensables en otra época y sobre todo en otra época del derecho. Estamos en condiciones de hablar de una migración de lo físico a lo digital, todo ello a través de las herramientas digitales que permiten llevar adelante actos jurídicos o hechos jurídicos tradicionales.

Históricamente, las transacciones necesitaban de un espacio físico y herramientas físicas para materializarlas, sin embargo, la ruptura de lo físico y

tangible hacia lo digital y lo virtual hizo necesaria la regulación por parte de los estados a través de las legislaciones en materia digital.

Por todo lo que mencionamos es que veremos en esta investigación el origen, la evolución y las perspectivas de futuro de la firma electrónica, para después ver de cerca la Ley de Firma Digital [LFD] Argentina, sus reglamentos, y también su posterior incorporación en el Código Civil y Comercial de la Nación [CCyCN] Argentina reformado; después avanzaremos sobre la legislación del derecho comparado de los países miembros del MERCOSUR, y la legislación del proceso de integración regional en sí. Y, por último, tocará el turno al Reglamento eIDAS, una legislación disruptiva y paradigmática, que actualmente cuenta con una propuesta de modificación desde el parlamento europeo.

La realización de esta tesis de Doctorado en Derecho con orientación en Derecho Privado se justifica desde el punto de vista de un interés profesional y a nivel académico que definen el tema seleccionado y la gran importancia que conlleva.

En primer lugar, el interés profesional que nos lleva a realizar la presente tesis se centra en que las áreas de conocimiento que se van a abordar están directamente relacionadas con el trabajo que desarrollamos en la comisión de derecho informático del Colegio de Abogados de la Provincia de Bs. As [COLPROBA], y en la comisión de informática jurídica de la Federación Argentina de Colegios de Abogados [FACA], en donde encontramos nuestra labor totalmente ligada a la firma digital.

En segundo lugar, el interés académico que puede suscitar el tema elegido, desde un plano general, se concreta en nuestra carrera como docente universitario, donde siempre tenemos contacto con la temática perteneciente al Derecho Informático de la presente tesis.

Este trabajo se justifica metodológicamente pues la manera como se aborda servirá como referencia a todos aquellos que utilicen la LFD, algo que actualmente está sucediendo de manera masiva en nuestra profesión y en otros ámbitos.

Es menester que evaluemos cuál es el alcance actual de la ley de firma digital en la legislación argentina, en el MERCOSUR, además de ello considerando la normativa de sus integrantes y finalmente, como venimos mencionando la labor de la U.E.

Las leyes de firma electrónica, se encuentran siendo utilizadas en casi todo el mundo de manera eficaz y efectiva, favoreciendo de forma revolucionaria los procesos judiciales y las operaciones comerciales de los ciudadanos. El acogimiento de sus institutos, características y principios que trataremos significan un paso evolutivo en el derecho en todas sus facetas sin ningún lugar a dudas.

Sin embargo, nos planteamos que en el MERCOSUR existen barreras que dificultan la seguridad jurídica debido a la falta de armonización legislativa relativa a la firma electrónica.

Esta investigación reviste relevancia social pues realizaremos una propuesta jurídica que contemple un marco legal y jurídico común que se podría utilizar como referencia para la aplicación de las firmas electrónicas en el MERCOSUR.

La pregunta que trataremos de responder con esta investigación es: **¿Por qué existen barreras en cuanto a la firma electrónica en el MERCOSUR? ¿Cómo armonizar las legislaciones en torno a firmas electrónicas en el MERCOSUR?**

La Hipótesis que pretendemos demostrar en este trabajo es la siguiente: La creación de un marco jurídico contribuye a la armonización de las legislaciones en torno a las firmas electrónicas en el ámbito del MERCOSUR.

Por lo tanto, en la presente tesis postulamos la necesidad de lograr una adecuada armonización legislativa sobre firma electrónica en el ámbito del MERCOSUR.

Nos proponemos responder la misma a través del cumplimiento de los siguientes "**Objetivos generales**":

Establecer por qué existen barreras en cuanto a la firma electrónica en el MERCOSUR.

Determinar cómo armonizar las legislaciones en torno a firmas electrónicas en el MERCOSUR.

Y de los siguientes "**Objetivos específicos":**

Conocer la legislación, doctrina y jurisprudencia en el MERCOSUR y la U.E respecto de la Ley de firma digital y firma electrónica.

Identificar los elementos fundamentales de la Ley de firma digital y electrónica argentina, la de los países integrantes del MERCOSUR, y de sus Estados Asociados y la U.E.

Determinar el grado de adopción e implementación de la firma digital y de la firma electrónica en el MERCOSUR y la U.E.

Realizar propuestas que contemplen la armonización de la firma digital y firma electrónica de las diferentes legislaciones del MERCOSUR.

En cuanto a los resultados esperados, estos serían la elaboración de un documento académico que refleje el derecho vigente de Argentina, del MERCOSUR y de los aspectos evolutivos que pudieran darse en el futuro respecto de la LFD, de manera que sirva como material de consulta para los interesados en la materia específica, contribuyendo así a la doctrina y a los académicos.

Los resultados de la investigación serán puestos a consideración de la comunidad y de todos los actores del derecho. Entendemos que servirán como aporte para el desarrollo del instituto de la firma electrónica y todos sus aspectos, cuya importancia social sin dudas resulta relevante.

Capítulo I

Estado del Arte

I. Introducción

Comenzamos el presente capítulo estableciendo que, durante el proceso de elaboración de la presente tesis doctoral, una de las principales tareas fue la de conocer y analizar el estado del arte de los tres pilares que hacen a la temática central de la investigación. En nuestro caso estos pilares se centran en la firma electrónica, las regulaciones en materia de firma electrónica y, por último, los marcos legales transnacionales en la materia, ya sea en el ámbito del MERCOSUR o de la U.E.

Aclaramos además que el campo de investigación de la presente tesis, se encuadra dentro de derecho informático y a su vez dentro del derecho civil privado.

Por lo tanto, realizaremos una recopilación de los avances más importantes y actuales respecto a los temas principales del estado del arte. Decimos que esto lo venimos realizando desde hace varios años, reiterando nuestra intención de lograr así una investigación que realice un aporte académico al derecho civil privado, al derecho informático y a la comunidad académica.

II. Ley de Firma Digital Argentina

En el presente trabajo, nos abocamos al análisis de autores nacionales e internacionales, legislaciones actualizadas y artículos doctrinales, pero principalmente nos centramos en la legislación, siendo sin lugar a dudas la verdadera protagonista la legislación en materia de firma digital o electrónica, que en algunos países como el nuestro estuvo muchos años sin implementarse de manera efectiva y que se llegó a reglamentar, de manera tardía.

La firma digital se consagra en nuestro país a través de la Ley Nacional Argentina 25.506 del año 2001, por lo que podemos hablar de más de 20 años de implementación con y que su respectiva reglamentación, que ha sido actualizada. Sobre este punto decimos que, en los últimos años existieron avances en materia legislativa nacional, como por ejemplo el Decreto Reglamentario 182 del 2019.

Decimos que uno de los objetos de estudio de la presente tesis doctoral y que se hallan a nivel nacional es la LFD Argentina. La firma electrónica, la firma digital, los documentos electrónicos, la infraestructura y todo el ecosistema digital emanado de ella es tratada por la doctrina nacional en múltiples obras que revisamos en el presente trabajo de investigación.

Muchas legislaciones parten de la legislación de la Ley Modelo de la *United Nations Commission on International Trade Law* [UNCITRAL], como por ejemplo lo hace nuestro país, que incorpora en su ordenamiento positivo casi todos los conceptos de igual pero no de idéntica manera.

En la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, en el art. 2. definiciones se establece que

> Por “firma electrónica” se entenderán 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.

La firma digital en la República Argentina es definida en el art. 2 de la LFD siguiendo la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil [CNUDMI] sobre las firmas electrónicas, al establecer que este mecanismo de firma es resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante. Esta herramienta digital fue incorporada en el CCyCN en la última gran reforma, más precisamente con la Ley 26. 994, cuyo texto fue aprobado por el Congreso de la Nación Argentina el 1 de octubre de 2014, promulgado el 7 de octubre de 2014 y publicado en el Boletín Oficial [B.O] de la República Argentina el 8 de octubre del mismo año. A razón de ello, se incorporó en el último párrafo del art. 288 del

CCyCN, que en los instrumentos generados por medios electrónicos el requisito de la firma queda satisfecho si se utiliza una firma digital, asegurando así la autoría e integridad del instrumento.

Sobre este punto seguimos a Altmark y Molina Quiroga (2012), al establecer que uno de los aspectos más trascendentes de la LFD, es el de equiparar la firma manuscrita u ológrafa con la firma digital. Todo ello siempre basándose en el denominado criterio o principio de equivalencia funcional, tal como lo recomienda Ley Modelo de la CNUDMI sobre las Firmas Electrónicas que veremos más adelante.

También la Ley modelo de la CNUDMI, trata al documento digital, y de cómo este una vez firmado digitalmente, garantiza la inalterabilidad del documento digital otorgándole no repudio. Siempre manteniendo la neutralidad tecnológica, concepto heredado de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) que permite que: “El artículo 5 enuncia el principio fundamental de que los mensajes de datos no deben ser objeto de discriminación, es decir, de que esos mensajes deberán ser tratados sin disparidad alguna respecto de los documentos consignados sobre papel” (p. 20).

Otro punto a tener en cuenta es la Reglamentación de la Firma Digital Argentina publicada en el B.O el 12 de marzo de 2019, el Decreto Nº 182/2019. De acuerdo a los considerandos expuestos por la norma resultaba necesaria llevar adelante una adecuación de la Reglamentación de la Ley 25.506 y su modificatoria ley Nº 27.446 (Ley de Simplificación y Desburocratización de la Administración Pública Nacional), actualizando su contenido en función a los nuevos avances tecnológicos y la experiencia previa en la implementación de la Infraestructura de Firma Digital en la República Argentina.

Sostenemos como surgieron nuevos paradigmas en el derecho que deberemos tratar como por ejemplo la denominada “confianza digital”, que para la ley de firma digital de nuestro país es considerada como uno de los pilares fundamentales de esta norma. Por eso, esta confianza es necesaria para lograr adoptar como medio de uso habitual lo digital en contraposición de lo físico, para así promover las

transacciones y el mercado digital o por otro lado compulsar los procesos judiciales casi en su totalidad digitales y sus correspondientes expedientes digitales.

Adelantando lo que veremos más adelante en profundidad, necesitamos varias características para que un sistema sea considerado digno de confianza digital. Como por ejemplo el mantenimiento en el tiempo de la integridad de los documentos firmados digitalmente, la inalterabilidad de ellos una vez firmados digitalmente, hecho que impide que sean modificados o alterados por terceros. Esta es una de las principales características de la firma digital en la Argentina y de su consiguiente ecosistema digital.

Estos y muchos ítems que desarrollaremos más adelante nos dan la seguridad jurídica necesaria para la promoción de la utilización en el mercado digital y las posibilidades que este puede dar.

En este panorama, nuestro país integra el MERCOSUR, el cual tiene como objetivo principal generar oportunidades comerciales e inversiones a través de la integración competitiva de las economías nacionales al mercado internacional. Por lo tanto, si hablamos de un mercado digital en el MERCOSUR, la confianza digital proporcionada por la firma digital y su exponencial implementación aportará una seguridad jurídica y todos los beneficios que nos otorga.

III. Legislación en materia de firma digital en MERCOSUR

En materia de firma digital, actualmente todos los países del MERCOSUR cuentan con legislación nacional propia en la materia. Aclaramos que solo mencionaremos a los estados parte del MERCOSUR y sus estados asociados, los cuales veremos en los siguientes capítulos, no así al resto de los estados de Latinoamérica debido a que no aportaría significativamente a nuestra investigación.

Comenzamos con la República Federativa del Brasil, país en el cual la firma digital se regula en base a la Norma 2.002-2 de 24 de agosto de 2001, con más de 20 años de antigüedad.

La República Oriental del Uruguay cuenta con la Ley 18.600, “del documento electrónico y firma electrónica” del año 2009.

La República del Paraguay, cuenta con la Ley Nº 6.822/2021 “De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos” siendo esta la más novedosa, moderna y completa de todo el MERCOSUR y Latinoamérica.

La República Bolivariana de Venezuela por su parte cuenta con la “Ley Sobre Mensajes de Datos y Firmas Electrónicas'' publicada en diciembre del 2000.

Desde ya, la legislación de la República Argentina y casi todas las legislaciones que mencionamos son herederas y conocen su origen en la Ley Modelo sobre Firmas Electrónicas de la CNUDMI, por lo que decimos que se trata del documento fundacional de muchas legislaciones en la materia. Por lo tanto, afirmamos que la Ley Modelo de la CNUDMI sobre Comercio Electrónico de 1996 y Ley Modelo de la CNUDMI sobre las Firmas Electrónicas del 2001, son materia de innegable tratamiento en el presente trabajo.

A través del Consejo del MERCOSUR se establece el Grupo Agenda Digital [GAD] del MERCOSUR a través de la Decisión 27/2017 en el año 2017 con el objetivo de *promover el desarrollo de un Mercosur Digital.* Dentro de las principales iniciativas de este, nace el Acuerdo de reconocimiento mutuo de firmas digitales en el MERCOSUR a través de la Decisión del Mercosur 11/2019 del 4 de diciembre del 2019 y el Acuerdo de comercio electrónico del MERCOSUR el 28 de enero del 2021.

Actualmente decimos que el MERCOSUR se encuentra realizando grandes adelantos en materia de armonización de legislación de firma digital, Decisiones que promueven las transacciones digitales y por consiguiente el avance del mercado digital del bloque regional que integra nuestro país.

IV. Marco legislativo de la Unión Europea en materia de identificación electrónica y servicios de confianza

La U.E cuenta con el Reglamento 910/2014 del 23 de julio de 2014, conocido como Reglamento eIDAS, el cual entró en vigencia el 1 de julio del año 2016 en todos los países de la U.E. La norma regula la identificación electrónica y establece unas pautas para los servicios de confianza relativos a las transacciones electrónicas que son comunes para todos los países miembros del bloque regional.

Llaneza González (2018) ha sostenido que

> Todo el sistema de firma electrónica y sus prestadores ha cambiado drásticamente con la publicación y entrada en vigor del Reglamento de la UE que modifica de modo radical el paradigma de la Directiva y la Ley de Firma Electrónica Española: establece la figura de los Prestadores de Servicios de Confianza sujetos a nuevos requisitos legales, normativos y de seguridad que se asocian directamente con la confiabilidad de los servicios que prestan, lo que lleva al Reglamento a establecer presunciones legales sobre la validez de la firma electrónica, el sello electrónico, el sellado de tiempos o la entrega electrónica de documentos y contenidos basados en estos complejos requisitos (p. 8).

El Reglamento eIDAS deroga y reemplaza la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, que trataba previamente las firmas electrónicas de manera regional, sin ofrecer un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas.

Merchán Murillo (2021) destaca que: “Entre los objetivos de este Reglamento está reforzar la confianza en las transacciones electrónicas dentro del marco de la Unión Europea, proporcionando las herramientas jurídicas necesarias para crear un clima de seguridad entre ciudadanos, empresas y la Administración Pública…” (p. 31).

Observamos como novedad y precursor en la materia, que el Reglamento eIDAS ya no habla solamente de firmas electrónicas, sino que va más allá, incluyendo a esta última dentro de los denominados “servicios de confianza” e incorporando dentro de sus artículos nuevas herramientas digitales.

El Reglamento eIDAS actualmente cuenta con una propuesta de modificación, la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento 910/2014 eIDAS también llamado eIDAS 2.0. Tal como mencionamos, el mismo se trata de una “propuesta” por parte de la Comisión Europea. por lo que el Reglamento eIDAS se mantiene vigente, mientras que la comisión comenzará a trabajar y negociar con los estados miembros de la U.E., algo que debería concluir como máximo en septiembre del año 2022.

En este panorama, seguimos a Quiroga (2020) el cual sostiene que el estado del arte, conlleva un procedimiento sistemático y riguroso para analizar información relevante en forma crítica, con objetivos bien definidos. Se trata de explicar a partir de otros estudios el objeto de estudio.

Concluimos de este modo que el estado del arte sobre nuestra área de investigación, que conoceremos, identificaremos, y determinaremos en los siguientes capítulos y que nos permitirá cumplir los objetivos generales y específicos. También nos permitirá llegar a las respuestas que se plantearon, a la realización de conclusiones y a las propuestas que ayuden el engrandecimiento del derecho informático y el derecho privado.

Capítulo II

Introito, evolución y avance en materia de firma electrónica

I. Introducción

Comenzamos estableciendo que este capítulo inicial tiene como objetivo principal, el de conocer el origen, la evolución y además un poco del futuro de la firma electrónica y por sobre todo de la firma electrónica avanzada.

Con posterioridad, trataremos la recepción que terminó teniendo y su evolución en el derecho comparado. También trataremos los aspectos técnico-legales de la firma digital en general, qué tan difíciles resultan para los que estudiamos el derecho, por lo que propongo una visión más pragmática de temas tan complejos como por ejemplo la criptografía.

Planteamos también la necesidad de incorporar en la presente tesis doctoral la historia y la consiguiente evolución de la firma electrónica, así como también la ubicación temporal de la misma, todo ello por cuanto trataremos las revoluciones industriales y sus implicancias con los avances de las tecnologías emergentes.

Además, necesitamos tratar el origen y el modelo que terminarían adoptando las normas y reglamentos de firma digital sobre todo en el MERCOSUR, como por ejemplo la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas.

Seguimos por lo tanto a Mason (2016) que establece que la legislación que prevé a las firmas electrónicas se ha dirigido, esencialmente a fin de establecer la autenticidad de la persona que usa tal firma, entre otras cosas, además de la integridad de una firma electrónica, mensaje o documento. La autenticación puede ser el proceso mediante el cual una persona busca verificar la validez o autenticidad.

¿Y cómo se logra esto último? Gracias a la criptografía, más específicamente la criptografía asimétrica, este sistema criptográfico moderno permite que la seguridad de las herramientas digitales proporcione una seguridad jurídica sin precedentes en la historia del derecho. Es esta última el fundamento principal de todas las

regulaciones en materia de firma digital que veremos, tal seguridad jurídica en los diferentes ecosistemas digitales, crearon las infraestructuras digitales, y por consiguiente la importantísima “confianza digital” para las transacciones electrónicas.

II. Las Revoluciones industriales

Actualmente nos encontramos en la cuarta revolución industrial y aun cuando los fundamentos tecnológicos de la firma electrónica se dieron en la anterior revolución industrial, decimos que con la irrupción de las nuevas tecnologías terminarían ratificando la importancia de las legislaciones en materia de firma electrónica.

Además, no debemos olvidar la pandemia ocasionada por el Covid-19, circunstancia que produjo una implementación exponencial de las herramientas digitales, convirtiendo la utilización de ellas la regla general y las herramientas de antaño, como el papel y la firma ológrafa una simple excepción.

Partimos de la premisa de que la ciencia y la tecnología acompañaron a la humanidad, a través del constante avance de la ciencia es que se nos permite hablar del estado del arte tecnológicamente hablando de nuestro objeto de estudio. Por ello hacemos un breve repaso de las grandes revoluciones industriales de la humanidad para ubicarnos en tiempo y lugar.

Schwab (2016) sostiene que las revoluciones se han producido a lo largo de la historia cuando nuevas tecnologías y formas novedosas de percibir el mundo desencadenan un cambio profundo en los sistemas económicos y las estructuras sociales.

Por lo tanto, atravesamos la cuarta revolución industrial y decimos que se trata efectivamente una de las más importantes y más grande de todas las revoluciones que se han verificado desde la primera. Ésta comenzó a principios de este siglo con una llamada revolución digital, que se caracteriza por una fusión de tecnologías que está difuminando las líneas entre lo físico, las esferas digitales y las biológicas. Esta cuarta etapa está marcada por avances tecnológicos emergentes en una serie de campos, incluyendo robótica, inteligencia artificial, cadena de bloques,

nanotecnología, computación cuántica, biotecnología, Internet de las cosas, impresión 3D y vehículos autónomos (Schwab, 2016).

Para comenzar, afirmamos que el papel, tal como lo conocemos, responde también a una tecnología y al estado del arte de un momento determinado de la humanidad. Agregamos a grandes rasgos que para poder fabricar industrialmente el papel, el proceso comienza cuando las fibras de celulosa se mezclan con agua en un gran recipiente, esta mezcla pasa a la máquina papelera, paso siguiente esta mezcla de agua y fibras se coloca sobre una larga banda conducida por rodillos, donde por último se va retirando el agua por varios procedimientos: gravedad, vacío, presión y secado donde permite la obtención de una enorme hoja de papel, que se enrolla para formar una bobina la cual se transforma eventualmente en una hoja que servirá de documento.

Lo que acabamos de explicar son los procesos, tecnologías y demás circunstancias para que llegue a nuestras manos una simple hoja de papel, y que podremos firmar con un bolígrafo para manifestar nuestra voluntad de manera ológrafa, no obstante, la tecnología es también empleada para realizar un bolígrafo, o una lapicera de pluma.

Decimos que para empezar a hablar de la firma digital hablaremos un poco de informática, para después continuar nuestro viaje por la criptografía, madre de la tecnología que da origen a la firma digital de nuestra legislación, para llegar al súmmum en materia tecnológica que trataremos al final del capítulo, la tecnología de cadena de bloques o de *blockchain*.

A. La actual revolución industrial

Afirmamos que la historia de la humanidad y la historia del derecho es una historia de evolución constante acompañada por las ciencias y la tecnología.

Desde los orígenes de la humanidad se ha manipulado a la naturaleza a través de técnicas y métodos que permitieron que el ser humano evolucionara como conjunto, como por ejemplo con la creación de diferentes invenciones, por ejemplo, la imprenta, la máquina de vapor, la electricidad, etc.

En ese orden de ideas, la primera revolución industrial nació también con la implementación de tecnología ya sea de la máquina de vapor, el ferrocarril, el acero, etc. que hicieron avanzar a pasos agigantados a la humanidad. La segunda de las revoluciones también significó un gran paso para la humanidad con sus correspondientes invenciones y avances.

No obstante, las Tecnologías de la Información y la Comunicación [TIC], nacen en la tercera revolución industrial, trayéndonos la mayoría de los avances necesarios para la existencia de las firmas digitales, ya sea sistemas informáticos, sistemas criptográficos que se implementan en nuestro objeto de estudio. Más allá de eso, el concepto tercera revolución industrial o revolución de la inteligencia, términos acuñados por Rifkin (2011), en donde se destacan las nuevas tecnologías, así como también los nuevos mecanismos de obtención de energía, y en consecuencia de empresas líderes en energías renovables.

Según el autor recién mencionado, existen cinco ejes principales o pilares en esta tercera revolución industrial.

De la misma forma que en el siglo XX, la tercera revolución industrial, se desarrolla fuertemente el campo de la electrónica, las comunicaciones, el desarrollo de la informática, las redes telemáticas y de la comunicación. El siglo XX, nos permitió hablar de tecnologías que surgen de la utilización de la electricidad, los procesadores, semiconductores, transistores, y todos los procedimientos técnicos cada vez más avanzados en materia de informática, que terminaron de consagrarse como moneda corriente en la vida de las personas.

Podemos decir que toda tecnología influye en la sociedad y por consiguiente lo hace en el derecho, pilar fundamental de la paz social, así como hoy en día la utilización de Internet y de la informática se convirtieron en tecnologías fundamentales para los temas que tratamos en el presente trabajo.

En ese orden de ideas, nos encontramos atravesando la cuarta de las revoluciones industriales. Esta revolución trajo consigo tecnologías emergentes que van a cambiar la vida de las personas, ya sea económica, social o culturalmente, y son situaciones que ya podemos apreciar a simple vista. Tal como ya mencionamos, la firma digital actualmente es una tecnología gestada hace varias décadas, aun así,

esta encuentra su apogeo en la actualidad, donde la digitalización se produce de manera exponencial.

Schwab (2016) nos aclara

> Las tecnologías digitales que en su núcleo poseen hardware para computación, software y redes no son nuevas, pero, a diferencia de la tercera revolución industrial, son cada vez más sofisticadas e integradas y están, de resultas de ello, transformando las sociedades y la economía mundial (p.13).

Se habló por primera vez de esta revolución durante el debate sobre la “Industria 4.0”, un término acuñado en la feria alemana de Hannover del año 2011 para describir cómo esta revolucionará la organización de las cadenas de valor globales.

En lo que a nuestro tema principal respecta, la firma digital responde a una tecnología del siglo XX, pero sin embargo esta se suma a las nuevas tecnologías del siglo XXI. Todas las legislaciones en materia de firma digital, e incluso el Reglamento eIDAS de la U.E. sirven de pilar para los grandes descubrimientos y los grandes avances de la última revolución industrial.

Por ejemplo, no podríamos hablar de una regulación en materia de inteligencia artificial [I.A] tema tan de moda en la actualidad, sin la existencia como base de la legislación en materia de firma digital. No podríamos hablar primero del marco jurídico sobre la I.A. de la historia propuesto por la Comisión europea sin las bases del Reglamento eIDAS eje de nuestra investigación o el Reglamento de Protección de datos personales europeo [RPGD].

Tampoco de una de las tecnologías emergentes más disruptivas de la cuarta revolución industrial, la tecnología de *blockchain* (en español conocida como cadena de bloques), y que trataremos más adelante en este capítulo.

III. Avance de la informática

Dentro de este orden de ideas, hablaremos de la informática, la base tecnológica sobre la que se asienta la firma digital, el derecho informático y, por consiguiente, de nuestra tesis doctoral, la cual tendrá una más que importante relación con la informática.

Decimos que para nosotros no hay duda que la computadora, el ordenador o computador representa tal vez entre los hitos más importantes creados por la raza humana, más en la actualidad, donde casi la totalidad de los habitantes de la tierra cuentan con una computadora o con una computadora en el bolsillo, o mejor dicho un teléfono del tipo Smartphone. También decimos que la computadora está a la altura de invenciones como la rueda, el ferrocarril o el motor a vapor que permitieron que la humanidad avance nuevos estadios.

A. Derecho informático e informática jurídica

Para nosotros el derecho informático es el conjunto de principios y normas que regulan los efectos jurídicos entre el derecho y la informática.

Por su parte la palabra informática según la Real Academia Española [RAE] (2021) es definida como: “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras”.

Esta definición poco tiene que ver con el derecho, pero de la definición inferimos el uso de computadoras, del medio informático que en la actualidad forma parte de la vida de las personas.

Por su parte, Fernández Delpech (2014) define al derecho informático dándonos un concepto enriquecedor como

> El conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. La informática es una ciencia que estudia métodos, proceso y técnicas, con el fin de almacenar, procesar y transmitir informaciones y datos en formato digital (p. 1).

Como ya tratamos, con las conquistas científicas de las revoluciones industriales y el avance en el campo de la informática, el mundo pudo alcanzar el logro de firmar digitalmente sin necesidad de los trazos del puño y letra, un logro impensado en otra época.

La firma digital, la electrónica, el documento digital y el ecosistema digital integran la rama específica del derecho informático, lo que vuelve tema ineludible a tratar la misma en la presente investigación.

Camps (2015) nos enseña que

> Según puede observarse, la informática vendrá en adecuado auxilio al aportar sus reglas y mecanismos que permitan un rápido, ágil y sencillo procesamiento de la información, lo que incluye tanto la recolección de la misma como el tratamiento de los datos, su transmisión, almacenamiento y recuperación —evitando o limitando el soporte papel—, encriptación para preservar la seguridad, etc. (p.16).

Tal como menciona el autor, la informática aporta sus reglas y beneficios al derecho, y estos beneficios siempre crecen a diario al implementarse en la labor de los operadores de derecho, como se hace actualmente en la Informática Jurídica. Debido a ello, podemos hablar hoy en día de la firma a través de medios digitales y las consecuencias legales que ello implica.

Ahora bien, luego de lo que desarrollamos anteriormente, consideramos importante destacar a la informática jurídica.

“La informática jurídica, a diferencia del derecho informático, consiste en una ciencia constituida por los medios y herramientas tecnológicas puestos al servicio del derecho, para la recuperación, almacenaje y tratamiento aplicadas por ordenadores y programas al campo jurídico” (Clara, 2001, p.25).

Actualmente en casi todos los expedientes electrónicos y procesos electrónicos ya sean administrativos o judiciales de la República Argentina, hacen uso de manera exponencial de todo lo que acabamos de mencionar, más aún después de la pandemia ocasionada por el Covid 19.

IV. Evolución de la firma electrónica

Continuamos hablando del origen de la firma digital, para ello vamos a tener que tratar el origen y el desarrollo que tuvo el proceso de firma, autoría y de la manifestación de la voluntad.

Otra cuestión vital que debe incluirse en presente trabajo y que analizaremos en los próximos capítulos, es la legislación en materia de firma digital que se utiliza en Argentina, en el MERCOSUR y en la U.E, siendo esta última la más fecunda en el tema.

Para que fuese posible la actual forma de firma por medios digitales, fueron necesarios cientos de años de evolución. Necesitamos ver el camino histórico que tuvo que realizar la firma digital en nuestro país para llegar al estado del arte tecnológico que tenemos actualmente en nuestros días. Esta fue atravesando diferentes estadios, donde para comenzar pasaremos por pueblos de la antigüedad, la antigua Roma con la *manufirmatio*, después la firma ológrafa, por último, la firmas electrónicas o firmas digitales actuales con criptografía asimétrica y hasta identificación con tecnologías más punteras.

A. La firma en el derecho argentino

A través de la historia la firma ológrafa ha sido el medio permanente a través del cual las personas han manifestado la voluntad expresa del firmante y su vinculación a un documento, estableciendo de manera intrínseca, que quien firma un documento está de acuerdo con los términos expresados en el mismo, y que se adquieran los derechos o asuman las obligaciones que de éste se deriven. Por ello, no podemos dejar de hablar del tratamiento que tuvo en nuestro país la firma manuscrita.

Durante muchos años, en nuestro país la firma se encontraba regulada en el Título V, De los instrumentos privados. En tal código se afirmaba lo siguiente: “La firma de las partes es una condición esencial para la existencia de todo acto bajo

forma privada. Ella no puede ser reemplazada por signos ni por iniciales de los nombres o apellidos" (Código Civil Nación [CCN], 2015, art. 1012).

El autor de la misma fue el jurista argentino Dalmacio Vélez Sarsfield, el cual reconoce la fuente del jurisconsulto brasileño Augusto Teixeira de Freitas conforme al art. 740 del Código Civil *Esboco* o Esbozo de Código Civil para Brasil.

Aclaramos más sobre el tema, con la brillante nota del art. 3639 del CCN (2015) de Vélez Sarsfield que decía que "La firma no es la simple escritura que una persona hace de su nombre o apellido: es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad".

En la nota que contenía el antiguo art. 916 del CCN (2015) de Vélez establecía lo siguiente en materia de firma

> Desde la Edad Media, la declaración escrita se hace poniendo el nombre propio debajo de un acto escrito, y la firma establece que el acto expresa el pensamiento y la voluntad del que lo firma. El acto no valdría por el derecho moderno aunque estuviese escrito por la parte, si no estuviese también firmado. Esta forma era extraña a los romanos, y cuando muy tarde la aceptaron, fue para muy pocas aplicaciones.

Vélez Sarsfield nos enseñaba así el efecto jurídico de la firma en el derecho en general y en el derecho argentino en particular. Dejamos por sentado que los preceptos y conceptos de firma fueron los que se mantuvieron de manera ininterrumpida hasta la irrupción de las TIC y de las nuevas tecnologías siendo el actual art. 288 del CCyCN el que regula la manifestación de la voluntad de las personas ya sea de manera digital o no.

B. La firma por medios electrónicos

El diccionario de la RAE (2021) define a la firma electrónica como al conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. Por su parte, define a la firma digital a la serie de datos, generados por un método criptográfico, que garantiza la autenticidad de un mensaje o pedido comercial. Estas definiciones resultan complejas para personas ajenas y no tan ajenas al derecho muchas veces,

por lo que se hace necesario desenmarañar el terreno de este tema que tratamos y conocer la evolución, historia y demás problemas que tuvo hasta llegar a nuestros días.

Tal como podemos apreciar, para el antiguo art. 1012 del CCN de Vélez, la firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada.

Seguimos a Altmark y Molina Quiroga (2012), en cuanto a que este criterio del codificador resultaba anacrónico, en atención a la realidad de la irrupción de la informática en las relaciones comerciales, máxime en nuestros días de transacciones remotas y digitalización de casi la mayoría de los aspectos de estas.

Inferimos que la firma electrónica no es obra del azar, sino la suma de mucha evolución tecnológica y también de mucho trabajo por parte también del derecho. Cabe aclarar que nuestro enfoque es más práctico y con el fin de comprender mejor el tema, veremos la parte técnica que permitió la firma electrónica de nuestros días. Además, agregamos que para la existencia de esta herramienta digital, fue necesario una ardua tarea técnica y científica en materia de criptografía que nos permitió hablar de la firma digital de nuestros días.

Comenzaremos por Diffie y Hellman (1976), que describieron por primera vez la idea de un esquema de firma digital, pero solo teorizaron que tales esquemas existían. Ellos son los responsables del célebre sistema de intercambio de clave pública que lleva sus nombres y publicaron un artículo que ha sentado las bases de los sistemas de envío seguro de documentos actuales.

Pero el verdadero origen se remonta a la década del setenta, cuando finalmente Diffie y Hellman en el mismo año publicaron un artículo llamado *New directions in Criptography* [Nuevas direcciones en criptografía], en la que discutieron sobre un nuevo método de distribución de claves criptográficas y que serán vitales para los fundamentos y seguridad de la firma digital, la criptografía asimétrica.

Diffie y Hellman (1976) en *New directions in Criptography* establecen que (traducción propia)

> Se examinan dos tipos de desarrollos en criptografía contemporánea. La ampliación de las aplicaciones del teleprocesamiento ha dado lugar a la necesidad de contar con canales de distribución de claves seguros y

> suministrar el equivalente a una firma escrita. Este documento sugiere formas de resolver estos problemas actualmente abiertos. También se analiza cómo las teorías de la comunicación y la computación están comenzando a proporcionar las herramientas para resolver problemas criptográficos de larga data (p.1).

Más adelante, Ronald Rivest, Adi Shamir y Len Adleman inventaron el algoritmo RSA, que podría usarse para producir una especie de firma digital primitiva. Este artículo estimuló el desarrollo de un nuevo y efectivo asimétrico siendo éste un algoritmo de cifrado. Dieron la idea de esquemas de firma digital. Rivest et al. (1977) idearon el concepto del algoritmo RSA. Para un método más seguro, se aplicó una función hash criptográfica al mensaje original antes de seguir el algoritmo RSA. Goldwasser et al. (1984) fueron los primeros en definir la seguridad y los requisitos de la firma electrónica.

La CNUDMI (1996) desarrolló la Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el derecho mercantil internacional. Debemos prestar muchísima atención a esta Ley modelo, que establecía lo siguiente

> Firma 1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente (art. 7).

A estas alturas ya podemos observar la intención de la CNUDMI de promover la función de la firma en el ámbito electrónico.

Con posterioridad en el año 1999 se estableció la posibilidad de incrustar firmas digitales en documentos con formato *portable document format* [PDF] que en español se traduce como formato de documento portátil, Este tipo de documento es ahora un estándar abierto, reconocido por la Organización Internacional para la Estandarización y uno de los más utilizados no solo en la gestión de documentos electrónicos, sino para la firma digital de instrumentos electrónicos de todo tipo. Los documentos PDF pueden contener vínculos, campos de formulario, audio, vídeo e imágenes. En consecuencia, podemos firmar electrónicamente y puedes ver con

facilidad los archivos PDF en diferentes sistemas operativos como por ejemplo en Android, Linux, Windows o Mac OS utilizando el software gratuito Acrobat Reader DC.

En esta misma época (finales del siglo XX), la U.E establece la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo el 13 de diciembre de 1999. En ella se establece un marco comunitario para la firma electrónica, la cual fue publicada en el diario oficial de las comunidades europeas de 19 de enero del 2000. A grandes rasgos podemos decir que esta directiva armoniza las firmas digitales de los países integrantes del bloque europeo, estableciendo así un marco comunitario.

En el año 2000, solo que esta vez en los Estados Unidos de América, se establece la ley de firmas electrónicas en el comercio mundial y nacional, la ley *ESIGN* hace que las firmas digitales sean legalmente vinculantes y en el 2002 se funda *SIGNiX*.

Volviendo a la década de los noventa, las transacciones en línea comenzaron a convertirse en una norma en los Estados Unidos, surgiendo la necesidad de hacer que las firmas electrónicas tengan validez legal y jurídica. Tomó alrededor de cinco años hasta que, en el año 1999, la Conferencia Nacional de Comisionados introdujo la Ley Uniforme de Transacciones Electrónicas. Esta última sólo adquiere autoridad mediante la promulgación de legisladores estatales, por lo tanto, su legitimidad depende de los estados.

Después de eso, el congreso de los Estados Unidos adoptó la Ley de Firmas Electrónicas en el Comercio Global y Nacional en el año 2000. Este hito reconoció la importancia de las transacciones electrónicas y actualizó muchas regulaciones relacionadas con el comercio.

En 1996 la CNUDMI comienza su labor en materia de firma electrónica, cuando en la Ley Modelo sobre Comercio Electrónico, más precisamente en el art. 7, nos da una temprana y sencilla definición de firma electrónica, la cual ya pudimos ver, y que sentó las bases para que con posterioridad en el año 2001 la CNUDMI/UNCITRAL desarrollara la Ley Modelo sobre Firma Electrónicas.

La Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la guía para su incorporación al derecho interno 2001 establece en el capítulo I, introducción a la

Ley Modelo de la CNUDMI, más precisamente en la finalidad y origen de la Ley Modelo que dice así

> El creciente empleo de técnicas de autenticación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación ha planteado la necesidad de crear un marco jurídico específico para reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de dichas técnicas modernas (a las que puede denominarse en general “firmas electrónicas”). El riesgo de que distintos países adopten criterios legislativos diferentes en relación con las firmas electrónicas exige disposiciones legislativas uniformes que establezcan las normas básicas de lo que constituye en esencia un fenómeno internacional, en el que es fundamental la armonía jurídica y la interoperabilidad técnica.

Así nuevamente la CNUDMI establece como su objetivo principal la armonía jurídica y la interoperabilidad técnica de las legislaciones en materia de firma electrónica.

La Ley Modelo sobre Firma Electrónica, define en uno de sus artículos

> 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 (art. 2).

La Ley Modelo sobre Comercio Electrónico y La Ley Modelo sobre Firma Electrónica, establecen por lo tanto que la principal razón de ser de la firma electrónica es su capacidad para identificar a la persona que realiza la firma.

En Argentina la implementación oficial de la firma digital se da en el año 2001, en parte gracias a la CNUDMI que había aportado sus leyes modelos, que ayudaron al legislador argentino en dar origen a la legislación nacional.

> Para completar la definición dada por la Ley Modelo sobre Firma Electrónica debemos acudir al art 6, que, en su párrafo segundo, nos dice acerca de la identificación del sujeto, como persona que parte con la intención de vincularse o autentificar un documento, es esencial su identificación como parte, para diferenciarlo de otra persona que pueda utilizar su nombre u otros datos (Merchán Murillo, 2015, p.109).

Así las cosas, llegamos a la LFD Argentina, establecida en nuestra legislación con el objeto de facilitar, agilizar, efectivizar, de manera segura e inmediata la firma

de documentos electrónicos como prueba de la autoría de la declaración de voluntad del autor.

Sin embargo, decimos que el avance de estado del arte en materia de firma electrónica se produjo en Europa el 23 de julio de 2014, con el Reglamento 910/2014 del Parlamento Europeo y el Consejo, que introdujo novedades importantísimas en materia no solo de firma electrónica, sino también en el tratamiento de identificación electrónica, autenticación y servicios de confianza.

La importancia de este reglamento nos da la fundamentación de los objetivos de esta tesis doctoral y que trataremos más adelante en su capítulo correspondiente.

C. La firma electrónica en el derecho comparado

Establecemos que, en todo el mundo, las firmas electrónicas o digitales ya cuentan con legislaciones y la aceptación de ellas es unánime, además son el andamiaje sobre el que se asientan los ecosistemas digitales de todos los países incluso el de la República Argentina con más de dos décadas de implementación.

Por ello, consideramos necesario observar brevemente el derecho comparado en materia de firma electrónica y como termina de desenvolverse.

En los Estados Unidos de América, es conocida la decisiva influencia en la difusión de la necesidad del dictado de normas atinentes a la firma electrónica, la labor realizada por la *American Bar Association* [ABA], generalmente traducido al español como Colegio de Abogados de Estados Unidos, es la organización que nuclea a los principales colegios de abogados de ese país. Las *Digital Signature Guidelines* son materia de consulta y referencia permanentes en esta materia en todo el derecho anglosajón e inclusive del mundo.

La *ABA* (1996) en la guía de uso de la firma digital nos da una definición bastante interesante sobre la misma (traducción propia)

> La transformación de un mensaje usando el sistema de criptografía asimétrica y una función de hash tal que una persona teniendo el mensaje inicial y la clave pública del signatario puede precisamente determinar: 1. Ya sea la transformación creada usando una clave privada que corresponde a la clave pública del signatario, o 2. Ya sea que el mensaje inicial ha sido alterado desde que la transformación fue hecha (p. 35).

Las firmas digitales requieren un par de claves, las denominadas claves públicas y privadas. Así como las claves físicas que se utilizan para bloquear y desbloquear, en criptografía, las funciones equivalentes son el cifrado y el descifrado

En materia legislativa de los Estados Unidos de América, el estado de Utah fue el primero en tener su propia legislación sobre firma digital en el año 1996 (*Utah Digital Signature Act)*, basada fundamentalmente en sistemas criptográficos. California, el segundo estado que introdujo legislación en la materia, adoptó, en cambio, un criterio más amplio, respetando el principio de neutralidad tecnológica. Actualmente cuarenta y nueve estados de Estados Unidos y su gobierno federal han dictado su legislación en materia de firma digital.

Con posterioridad el congreso federal norteamericano aprobó la ley de firma electrónica de los Estados Unidos de América, la *Electronic Signature in Global and National Commerce Act* o también conocida como la *ESIGN*, el 30 de julio del año 2000. La *ESIGN*, se encarga de la validez de los documentos electrónicos y las firmas electrónicas para las transacciones que afecten al comercio interestatal e internacional del país.

Seguimos a Merchán Murillo (2015) al establecer que esta es una ley de superposición, con esto se refiere a que se trata de una ley que se superpone a las leyes federales y estatales del país, en lugar de establecer un protocolo tecnológico específico, por lo que las partes involucradas en la transacción deberán pactar la tecnología y la seguridad dándole así más libertad.

> La *E-Sign* se encuentra acompañado de la Ley Uniforme de Transacciones Electrónicas (*Uniform Electronic Transaction Act* – UETA), Ley modelo aprobada y recomendada a los Estados de la Unión para su aprobación por la Conferencia Nacional de Comisionados sobre Leyes Estatales Uniformes en julio de 1999, diseñada para proveer a cada Estado de estándares para el uso de y aceptación de la firma electrónica (Murillo Merchán, 2015, p. 47).

Por su parte La República Popular de China a través de la Asamblea Popular Nacional de China aprobó el 28 de agosto de 2004 la “Ley de Firmas Electrónicas de la República Popular de China”, la cual entro en vigencia el 1 de abril del 2005, y que regula los actos de firma electrónica, los efectos jurídicos de la firma electrónica y de los documentos electrónicos.

También seleccionamos algunos países europeos también dictaron su legislación en la materia y que veremos brevemente a continuación:

La República Federal de Alemania dictó el 1 de agosto de 1997 Ley para las firmas digitales, en alemán *Gesetz zur digitalen Signatur* [Ley de Firma Digital] o también conocida como *SigG* siendo uno de los primeros países del mundo en regular la firma digital e incluso antes de la Directiva 1999/93 sobre firma electrónica, e incluso a la propia Ley Modelo de Firma Electrónica UNCITRAL. Esta legislación aprobada por el parlamento alemán forma parte de otra legislación denominada Ley Multimedia, que regula con carácter general las condiciones de los servicios de información y comunicaciones en el territorio alemán.

La Ley para las Firmas Digitales de Alemania (1997) establece: "… crear condiciones generales para las firmas digitales bajo las cuales puedan considerarse seguras y puedan detectar con fiabilidad las falsificaciones e imitaciones de dichas firmas digitales" (art. 1.1).

Italia al igual que Alemania fueron de los primeros países en regular la firma electrónica. La Ley italiana de 11 de marzo de 1997, número 59, sobre "Delegación al Gobierno para la concesión de funciones y tareas a las regiones y a los entes locales, para la reforma de la Administración Pública y para la simplificación administrativa". A través del art. 15 va a tratar acerca de la validez jurídica de los documentos electrónicos elaborados tanto por entidades públicas como privadas. Con posterioridad al dictado de este artículo se aprobó, el 10 de noviembre del año 1997 un Reglamento que trata de aportar criterios y modalidades para la formación, el archivo y la transmisión de documentos con instrumentos informáticos y telemáticos.

El art. 15.2 de dicha norma establece en el año 1997 la validez de la firma electrónica

> … los actos, datos y documentos formados por la Administración Pública y por los particulares con instrumentos informáticos y telemáticos, los contratos estipulados en las mismas formas, así como su archivo y transmisión con instrumentos informáticos son válidos y relevantes a todos los efectos legales.

El 7 de marzo de 2005 es aprobado el Decreto Legislativo Nº 82, Código de la Administración Digital estableciendo el valor y la eficacia de la firma electrónica y la firma digital en el territorio italiano.

Francia cuenta con firmas electrónicas legalmente reconocidas desde 2000, desde la Ley N° 2000-230, después de la aprobación de la Directiva 1999/93/CE. También Francia introdujo diversas modificaciones a su Código Civil a través de la Ley 2000-230, de 13 de marzo de 2018.

El Reino de España obtuvo su legislación sobre firma electrónica a partir del Real Decreto-ley 14/1999, que se adelanta a la publicación de la Directiva 1999/93/CE, el 13 de diciembre de 1999, marco comunitario para la firma electrónica en la U. E. Aun así, el Real Decreto-Ley va a recoger la regulación establecida en la Directiva, además, concreta y desarrolla aspectos que corresponden, en base al principio de subsidiariedad, a cada uno de los estados miembros. Por último, la Ley 59/2003, de 19 de diciembre del 2003, de firma electrónica, deroga el Real Decreto-Ley, modificando e incorporando conceptos, tales como el de firma electrónica reconocida, siguiendo las pautas establecidas por la directiva, otorgándole equivalencia funcional con la firma manuscrita.

Reino Unido por su parte, aunque actualmente se haya producido el *Brexit* (esto es el abandono por parte del Reino Unido de su condición de estado miembro de la U.E*)*, había dictado el 26 de enero de 2000 la *Electronic Comunications Bill* la cual es la legislación que va a regular la firma digital en el territorio del Reino Unido, Inglaterra y Gales, Irlanda del Norte y Escocia. El primer borrador de un proyecto de ley, fue publicado en julio de 1999. *The Electronic Communications Act 2000* consta de tres partes, su primera parte trata sobre los proveedores de servicios de criptografía. La segunda parte trata la facilitación del comercio electrónico, almacenamiento de datos, etc. La última parte, trata los misceláneos y complementos de la ley.

La U.E, por su parte tiene una fecunda labor en la materia y que le dedicaremos gran parte de la obra por lo que en este punto solo veremos un brevísimo repaso. El Parlamento y el Consejo de la U.E aprobaron el 13 de diciembre de 1999 la

Directiva 1999/93/CE que establece un marco comunitario para la firma electrónica en la U.E.

La Directiva 1999/93/CE, fue la primera de las normas que regulan los servicios de firma electrónica en la U.E. Esta reconocía la validez de las firmas electrónicas, considerándose equivalentes a las firmas ológrafas estableciendo el principio de equivalencia funcional de esta herramienta digital. La mencionada directiva se encuentra derogada por un nuevo marco legal en la materia, el Reglamento de la Unión Europea Nº 910/2014, el Reglamento eIDAS, que establece un marco legal común para las firmas electrónicas en la U.E.

Señalamos que el fundamental problema que tenía la directiva 1999/93/CE era que cada estado miembro de la U.E la interpretaba a su manera. Situación que suponía una complicación para el reconocimiento y la validez de las firmas electrónicas entre estados miembros de la U.E. Esta problemática, iba en contra de la propia intención de la firma electrónica a nivel europeo (incluso en el bloque del MERCOSUR) que pretende agilizar procesos, y fomentar las transacciones electrónicas en favor de un Mercado Único Digital.

Por ejemplo, existía una laguna en el área de identificación de usuarios en los servicios electrónicos, puesto que cada país disponía de su propia forma de reconocerlos. Y cada una de estas formas de reconocimiento de identidades no siempre coincidía con las formas o mecanismos establecidos en otros países de la U.E.

De este modo, igual que ha sucedido con otras normas que regulan algunos aspectos del mundo digital, como la Directiva de privacidad o la de comercio electrónico de la U.E, la Directiva 1999/93/CE también quedó desfasada, circunstancia que decimos, se plantea en el problema principal de esta tesis.

Debido a lo que mencionamos, el actual y vigente Reglamento N° 910/2014, eIDAS, entra en vigor el 1 de julio de 2016 en toda la U.E. El Reglamento eIDAS regula la identificación electrónica y establece unas pautas para los servicios de confianza relativos a las transacciones electrónicas que son comunes para todos los países de la U.E.

Actualmente bajo la Resolución 2021/0136 del día 3 de junio del 2021, la Comisión Europea presentó una propuesta de Reglamento europeo regulador de una identidad digital [ID] segura y de confianza para todos los europeos, que propone modificar el Reglamento eIDAS.

V. Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho internacional

En este capítulo trataremos nuevamente, esta vez con mayor profundidad, un marco legal fundamental y fundacional para muchísimas legislaciones en materia de firma electrónica. Vamos a tratar en este punto los instrumentos elaborados por el Grupo de Trabajo de Comercio Electrónico en la CNUDMI: la Ley Modelo sobre Comercio Electrónico de la CNUDMI y la Ley Modelo sobre Firmas Electrónicas de la CNUDMI.

Esta se tuvo en cuenta para la confección de la LFD Argentina, y agregamos, casi todas las de las legislaciones en materia de firma electrónica del MERCOSUR. Por eso podemos afirmar que estas han tenido una importantísima influencia sobre las legislaciones en la materia digital en todo el mundo, pero por su parte la primera no se limita a la regulación de la firma digital, sino que abarca un espectro más amplio de aspectos vinculados al comercio electrónico y la segunda si impacta de lleno en nuestra temática.

Ambas leyes Modelo están destinadas a proporcionar ayuda y actuar como modelo para que los países puedan valerse de ella en la elaboración de la legislación de su ordenamiento positivo interno.

A. Ley Modelo sobre Comercio Electrónico de la CNUDMI

La Ley Modelo sobre Comercio Electrónico de la CNUDMI fue aprobada por la Resolución 51/162 de la Asamblea General el 16 de diciembre de 1996, a la cual se le realizó una adición en 1998, incorporando el art. 5 bis. La Asamblea General

de la ONU, aprobó la Ley Modelo sobre Comercio Electrónico mediante Resolución 51/162, la cual consta de 16 artículos y se encuentra dividida en dos partes.

El trabajo fue realizado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional a través del Grupo de Trabajo de Comercio Electrónico. Destacamos que la propuesta presentada a los países miembros, a fin de que adopten una legislación con rasgos comunes en Latinoamérica sobre el comercio electrónico y particularmente sobre la firma electrónica, fue paulatinamente incorporada por estos países.

Los objetivos de la Ley Modelo de Comercio Electrónico se encuentran en la Introducción: En principio, la finalidad de la misma es la de ofrecer un conjunto de reglas aceptables en el ámbito internacional que permitan eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que permita un desarrollo más seguro del comercio electrónico.

Se formula la Ley Modelo debido a que la legislación vigente en ese momento era por lo poco anticuada, e imponía restricciones al empleo de los modernos medios de comunicación.

Ayudar a remediar los inconvenientes del hecho de que un régimen legal interno era inadecuado llegando obstaculizar el comercio internacional.

Este sería un instrumento, en el ámbito internacional, para interpretar ciertos convenios y otros instrumentos internacionales existentes que impongan de hecho algunos obstáculos al empleo del comercio electrónico

También tuvo como objetivo los de permitir o facilitar el empleo del comercio electrónico y el de conceder igualdad de trato a los usuarios de mensajes consignados sobre un soporte informático que, a los usuarios de la documentación en papel, son esenciales para promover la economía y la eficiencia.

La primera parte de esta ley, nos habla sobre comercio electrónico en general y comprende básicamente el ámbito de aplicación, las definiciones, interpretación, reconocimiento jurídico de los mensajes de datos, la firma, el original, la admisibilidad y la fuerza probatoria de los mensajes de datos, la conservación de los mismos, la formación y validez de los contratos, el reconocimiento por las partes

de los mensajes de datos, su atribución, el acuse de recibo, el lugar y tiempo del envío y la recepción de un mensaje de datos.

La segunda parte de esta ley, va a tratar en cambio sobre el comercio electrónico sobre materias específicas y hace referencia a cuestiones sobre transporte de mercancías y los documentos de transporte.

Destacamos de vital importancia el art. 7, Firma dentro de la Ley Modelo

> 1. Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a. Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b. Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Este artículo será el fundamento de la Ley Modelo sobre Firmas Electrónicas que trataremos a continuación.

B. Ley Modelo sobre Firmas Electrónicas de la CNUDMI

El texto de la Ley Modelo sobre Firmas electrónicas de la UNCITRAL fue adoptado el 5 de Julio de 2001, el cual se basó en el informe de la CNUDMI sobre la labor de su trigésimo cuarto período de sesiones, celebrado en Viena, desde el 25 de junio al 13 de julio de 2001.

La Asamblea General de la Organización de las Naciones Unidas aprobó la Ley Modelo sobre Comercio Electrónico mediante la Resolución 56/80 con fecha 24 de enero de 2002, la cual se encontraba acompañada de una guía para su incorporación en el derecho interno de cada país.

Afirmamos, que la Ley Modelo para las Firmas Electrónicas no es ningún instrumento de obligatorio cumplimiento para los países, sin embargo, fue la primera iniciativa para armonizar las legislaciones a nivel internacional, la cual cobra mayor importancia cuando se refiere a las transacciones comerciales derivadas de las relaciones internacionales, que en un mundo globalizado se convierten en más frecuentes, como por ejemplo en el MERCOSUR, en el cual muchos países, a la salida de la ley no contaban con legislación en materia de firma electrónica.

Por consiguiente, en esta guía de Incorporación de la Ley Modelo se presentan las ventajas de que se trate como una ley modelo y no como una Convención, señalando entre ellas que los estados parte van a tener la posibilidad de hacer modificaciones al texto uniforme y no requiere de la notificación a las Naciones Unidas y a los otros estados parte cuando la adopten.

Esta Ley Modelo se basa en los principios en los que se basa el art. 7 de la Ley Modelo sobre Comercio Electrónico, y tiene como objetivo ayudar a los estados a establecer un marco legal para la firma electrónica.

Algo que no podemos dejar de mencionar en la Ley Modelo, es que se establece el principio de equidad entre la firma electrónica y la firma ológrafa, llegando a considerarlas de similar valor jurídico, lo que incorpora uno de los principios que rigen el documento electrónico resultante de la aplicación de la firma electrónica, tal principio es el de no discriminación, este principio lo encontramos en nuestra LFD y en nuestro CCyCN termina siendo recogido por el art. 288.

Los objetivos de la Ley Modelo incluyen el fomento de facilitar el uso de firmas electrónicas y proporcionar igualdad de trato para todos los documentos, ya sean en formato electrónico o almacenados en un portador físico.

Incluye, además, una serie de normas tendientes a regular las obligaciones de cada una de las partes que intervienen en el proceso de la firma electrónica, incluyendo a las entidades de certificación que tan decisivo papel cumplen en el mismo. La guía para la incorporación al derecho interno de la Ley Modelo, representa un régimen uniforme con la idea de facilitar a los legisladores la difícil tarea de incluir este tipo de normativa tan moderna. Sin embargo, es decisión de cada país adoptar e interiorizar la figura jurídica de la firma electrónica, es por esta razón que se ha optado por la promulgación de una ley especial o por la reforma de los diferentes cuerpos legales, tal como hemos apuntado con antelación.

La Ley Modelo sobre Firmas Electrónicas buscaba habilitar y facilitar el uso de las firmas electrónicas estableciendo un criterio de fiabilidad técnica para la equivalencia entre las firmas escritas y las electrónicas. De este modo, esta legislación puede ayudar a los Estados a establecer un marco legislativo moderno,

abordar de manera efectiva el trato jurídico de las firmas electrónicas, y permitir así la armonización.

Respecto a esto destacamos la armonización de los principios básicos nivel internacional lograda por esta ley.

Seguimos a Merchán Murillo (2015) cuando establece que a través de esta Ley Modelo se intentó recomendar los Estados para su incorporación al derecho interno, con unos principios básicos, que han de ser respetados para obtener una armonización a nivel internacional (p. 26).

La CNUDMI desarrolló Leyes Modelo sobre el Comercio Electrónico y Firmas Electrónicas para proporcionar a los legisladores nacionales un conjunto de normas internacionales aceptables encaminadas a eliminar los obstáculos jurídicos y a incrementar la previsibilidad legal del comercio electrónico y a facilitar el uso de la firma.

La Ley Modelo se basa en principios fundamentales, comunes como los textos de la CNUDMI relacionados con el comercio electrónico, especialmente, la no discriminación, la neutralidad tecnológica y la equivalencia funcional. Esta Ley establece criterios de confiabilidad técnica para la equivalencia entre las firmas electrónicas y estrictas, así como entre normas de conducta básicas que pueden servir como directrices para evaluar los deberes y responsabilidades de los signatarios, y los terceros de confianza.

Por último, la ley mencionada contiene disposiciones que favorecen el reconocimiento de certificados extranjeros y firmas electrónicas basadas en un principio de equivalencia sustantiva que no toma en cuenta el lugar de origen de una firma extranjera. Además, se acompaña una guía para la incorporación, que proporciona antecedentes e información exploratoria para ayudar a los Estados a preparar las disposiciones legislativas necesarias y guiar a otros usuarios del texto.

VI. Aspectos generales sobre la Firma electrónica avanzada

Afirmamos que la firma electrónica avanzada, que en países como Argentina ha terminado denominándose como firma digital, ha ganado muchísimo terreno, igual a lo que sucede a nivel mundial, y esto es gracias a sus múltiples beneficios, lo que suma razones más que lógicas para su difusión y sus usos. La firma digital, nos transporta remotamente a todos los escenarios posibles, a los asequibles y a los inaccesibles y a lo largo y ancho del país o del mundo, de manera instantánea y nos da seguridad, real y sobre todo seguridad jurídica.

Ordoñez (2020) afirma lo siguiente en materia de incorporación de esta herramienta digital: "Ya nada volvió a ser como antes, la irrupción de esta poderosa herramienta de expresión de voluntad y de identificación mutó las reglas de juego" (p.100).

El método más común para asegurar las transacciones electrónicas modernas son las tecnologías basadas en la criptografía, como la codificación y la firma electrónica. Una firma electrónica es a grandes rasgos una cadena de datos que se anexan a un mensaje electrónico a fin de garantizar su autenticidad, identificar al firmante y enlazar el contenido a ese firmante. La firma electrónica provee un medio eficaz para garantizar la autenticidad y la integridad de cualquier documento durante su vida útil.

En este punto necesitamos adentrarnos un poco más en las cuestiones que hacen a la firma digital en sí como por ejemplo la infraestructura.

A. Infraestructura de Firma electrónica avanzada o digital

Continuamos hablando de temas que casi escapan temas de derecho, pero aun así siguen teniendo relación. Por ejemplo, para entender la firma digital y la transmisión de esos datos en el terreno digital tendremos que hablar de la Infraestructura de clave pública o también conocida por sus siglas en inglés *PKI* de *Public Key Infraestructure.*

Establecemos que este es uno de los principales elementos que sostienen el sistema de firma digital en general esta Infraestructura de clave pública, que regula cómo se emiten y distribuyen las claves. La infraestructura de implementación, requiere que cada usuario tenga un par de claves públicas y privadas donde la clave pública sea disponible para todos, mientras que la clave privada solo la conozca el usuario.

También decimos que uno de los principales propósitos de la Infraestructura de clave pública es facilitar la transferencia electrónica segura de información de diferentes actividades de la red, como por ejemplo el comercio electrónico.

Hablamos de este tema ya que esta tecnología es la que permite a los usuarios de la red autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes a través de algoritmos de criptografía que veremos más adelante.

Por su parte, Argentina la denomina en la Ley como Infraestructura de Firma Digital lo que es conocido en el resto del mundo *PKI*. Esta infraestructura de firma digital podríamos decir que, para la LFD, se trata de conjunto de leyes, normas, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades se identifiquen entre sí de manera segura al realizar transacciones en redes.

Irigoitia (2016) establece que

> Una infraestructura *PKI* es una infraestructura de seguridad, basada en criptografía de clave pública, que permite la gestión de certificados digitales. La meta de una infraestructura de clave pública es cumplir las necesidades del control de acceso, de la identificación automatizada y de la autentificación de manera determinista (p. 71).

Está conformada por un conjunto de componentes que interactúan entre sí, permitiendo la emisión de certificados digitales en los dispositivos criptográficos o vía software para verificar firmas digitales en condiciones seguras, tanto desde el punto de vista técnico como legal.

Básicamente, la estructura está constituida por un certificador licenciado, dependiente de una autoridad de aplicación, y sometido a un régimen de auditoría y sanciones establecidas en la LFD.

Los estándares tecnológicos mencionados requieren de especial cuidado y atención. Este cuidado se vincula fundamentalmente a la utilización de estándares tecnológicos basados en principios, normas y protocolos internacionalmente aceptados tales como los que vimos así que ahondaremos en el tema.

El modelo de clave pública más conocido y utilizado mundialmente es el denominado RSA por las siglas de los apellidos de los descubridores: Rivest, Shamir y Adelman. También, otro algoritmo de firma digital muy extendido es el *Digital Signature Algorithm* [algoritmo de firma digital] definido en el *Digital* Signature *Standard*, el cual fue propuesto por la *U.S. National Institute of Standards and Technology* para ser el estándar de autenticación digital del gobierno de los Estados Unidos.

Los estándares aprobados y mencionados en la infraestructura de firma digital, se encuentran descritos en la Decisión Administrativa Nº 6/2007.

Por un lado, en cuanto a la generación de las claves se utiliza RSA, DSA o ECDSA, la protección de las claves privadas de certificadores y suscriptores se utiliza FIPS 140, las políticas de certificación RFC 5280 y 3739 (estándar de seguridad de ordenadores para la acreditación de módulos criptográficos).

Dejamos aclarado nuevamente que con fines didácticos decidimos no ahondar con temas que más que al derecho corresponden a la informática, matemáticas o ingeniería, pero que debimos tratar como los estándares mencionados.

B. El certificado licenciado, el certificado digital y las autoridades de registro

Decimos que el certificador licenciado es la Persona Humana o Jurídica, según lo que se infiere del texto legal vigente, que está habilitada por el Estado Nacional, para otorgar los certificado digitales, a los fines y efectos de que dicha clave pública se corresponda con el firmante y dote al procedimiento de firma y autenticación de la suficiente confiabilidad y seguridad jurídica, de modo tal que el certificador licenciatario, se constituye en tercero de confianza y se transforma en la garantía sobre el que funciona y se desarrolla en sistema, creando la confianza digital la cual

trataremos larga y tendidamente en el próximo capítulo siendo el primer elemento sobre el cual se sostiene el sistema.

Es la ley en materia de firma electrónica la que otorgará a esta herramienta digital las presunciones jurídicas, en nuestro caso hablamos de la Ley 25.506, que es quien va a dotar al certificado digital, del carácter de único título habilitante, para que un usuario de firma digital pueda realizar documentos digitales firmados con la validez jurídica a los realizados de manera manuscrita.

Los certificados digitales son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. En general, para hacer más transparente esta función, intervienen terceros que cumplen la función de entidades certificantes y otras que se denominan autoridades u operadores de registro, que dan fe de la identidad o calidades que reviste el firmante, titular de un certificado digital.

Acerca de esto, De Luca (2015) establece que

> Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona. En algunos casos, puede ser necesario crear una cadena de certificados, cada uno certificando el previo, para que las partes involucradas confíen en la identidad en cuestión (p. 36).

Dicho certificado digital requiere necesariamente para cumplir su función, que esté emitido por un certificador licenciado por el Estado Nacional a través de autoridad, que en nuestro país podemos hablar de la Autoridad Certificante Raíz de la República Argentina, único habilitado en el caso, para aportar a los documentos digitales firmados digitalmente.

Los certificados digitales permiten efectuar comunicaciones electrónicas de documentos o datos electrónicos de manera segura, proporcionando y garantizando siempre:

La autenticación: Nos permite que la identidad del emisor y el receptor sean reconocidas y autorizadas, así como la información que de ellos proviene. El certificado digital asocia los datos del usuario a una clave pública, que permite a otros verificar que esa clave es válida.

Confidencialidad: Toda información transmitida mediante el uso de algoritmos de cifrado, con el propósito de que sólo el destinatario del documento pueda acceder a su contenido

No repudio: Nos permite que probemos la participación de las partes en una comunicación, existiendo dos posibilidades: no repudio en origen y no repudio en destino: el primero es cuando el emisor no puede negar que envió porque el destinatario tiene pruebas del envío; en cambio el segundo, no repudio en destino es cuando el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

Integridad: Garantiza que la información que se transfiere no ha sido manipulada o alterada en algún dato digital ya que en el ecosistema digital siempre dejaría un rastro de esa manipulación.

Por último y más arriba en la pirámide de la Infraestructura de Clave Pública, tenemos a las Autoridades de Registro. Estas son las entidades públicas o privadas que se encuentran habilitados por el Ente Licenciante o la Autoridad Certificante para emitir certificados digitales, es decir quienes otorgan concretamente la habilitación para firmar.

C. Tipos de certificados digitales

Existen varios tipos de certificados digitales, lo que nos va a permitir firmar documentos electrónicos de dos maneras:

La primera es la local, vía hardware o token, en la que se descarga e instala en un dispositivo electrónico y la firma solo podrá realizarse desde donde el certificado se encuentre instalado.

Tiene dependencia del dispositivo de hardware, por lo que, si se extravía, se rompe, es robado, etc. Se deberá solicitar la revocación o cancelación del certificado incorporado en el mismo, y luego solicitar la generación de un nuevo certificado digital. Este tipo de firma se implementa con el dispositivo criptográfico, y a modo de ejemplo se puede decir que se podrá firmar mediante programas gestores de

documentos en PDF como por ejemplo Adobe Reader o Foxit Reader o en portales web que permitan esta funcionalidad.

En segundo es el que se realiza en la nube, firma digital *cloud* también llamada sin token (se accede a través de Internet). Este novedoso método fue incorporado en nuestro país por el Decreto 892/17 el 02 de noviembre del 2017, en el cual todas las personas pueden tener su firma digital y se encuentra almacenado en la nube en un servidor criptográfico.

Permite al firmante acceder desde cualquier ordenador o dispositivo móvil, limitando los riesgos a nivel de seguridad, porque requiere credenciales para poder utilizarse y además elimina la dependencia de un dispositivo de hardware.

Por ejemplo, en la República Argentina, para firmar un documento electrónico a través de este tipo de firma digital, lo podemos hacer desde la Plataforma de Firma Digital Remota Argentina.

VII. Documento electrónico

El documento electrónico es otro gran protagonista de las transacciones digitales y del ecosistema digital, pero generalmente se les otorga poca prominencia a estos.

Rolero (2001), hace más de dos décadas acertadamente decía: “EL DOCUMENTO ELECTRÓNICO. La evolución tecnológica de los últimos tiempos ha provocado una verdadera conmoción que afecta todos los ámbitos de la actividad jurídica y comercial, surgiendo nuevas modalidades de contratación y de actos jurídicos”.

Para la RAE (2021) el documento significa: “1. Diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos. 2. Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo”. Pero en nuestro ámbito de estudio, la segunda definición es la que más se acerca. En sentido amplio entendemos que el documento es un instrumento u objeto que contiene información. Sin embargo, en un sentido restringido solo serían reconocidos aquellos que están escritos en soporte y firmados conforme al ordenamiento de fondo del país.

Generalmente documento se suele pensar como un soporte, y actualmente casi todo tiene soporte digital, por lo que en la actualidad el soporte electrónico o digital es casi el rey indiscutido dejando al papel en un rol secundario. Más allá de eso cualquier medio sirve para el envío de datos y por consiguiente de estos documentos: En el caso de software, la nube, mails, mensajería instantánea y en el caso de hardware pendrives, CD, DVD, etc.

La LFD Argentina se toma el trabajo de definirlo, aun cuando en la Ley Modelo de la CNUDMI que sirve de modelo, no se define el documento electrónico.

Para la ley modelo 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” (art. 6).

“El contenido del artículo que analizamos es sumamente importante ya que forma parte de la arquitectura normativa adoptada por la ley 25.506 a los fines de incorporar un moderno concepto sustancial de documento en nuestra legislación civil” (Altmark y Molina Quiroga, 2012, p. 593).

Queda más que claro así que cuando para determinada transacción necesita de un escrito, que en antaño se confeccionaba en papel, puede ser realizado con el documento digital de manera equivalente.

La acepción digital, en documento digital, debe ser considerada de manera similar a la que se utiliza en otras legislaciones como documento electrónico para evitar confusión en este punto.

Otra situación que debemos tener en cuenta con respecto a los documentos digitales, son los “originales”, ya que como todos sabemos las copias de los mismos pueden ser realizadas de manera simple mediante medios informáticos y realizar así varias reproducciones infinitas de un mismo documento digital.

Seguimos a Altmark y Molina Quiroga en cuanto entienden que esta es una norma sustancial en la medida en que resalta la eficacia jurídica de los documentos digitales, incorporando el requisito de que esta haya sido firmado digitalmente (2012, p. 358).

Por lo tanto, afirmamos que un documento original es exactamente igual a sus copias. El art.11 de la Ley 25.506 es el que va a hablar del Original dando por sentado lo siguiente: Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

De Luca (2015) acerca de ese tema menciona: “Relacionado a este artículo la ley define la originalidad de los documentos. Debe recordarse que en el mundo digital un documento original es exactamente igual a sus copias” (p. 31).

Demuestra la importancia del documento electrónico también el Reglamento eIDAS, la definición de documento electrónico: “documento electrónico, todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual” (art. 3, punto 35).

Asimismo, el Reglamento incluso le dedica el capítulo 4 para tratar en especial para sus Efectos jurídicos y el considerando 63 que establece: “Los documentos electrónicos son importantes para que sigan desarrollándose las transacciones electrónicas transfronterizas en el mercado interior”.

VIII. Criptografía

Sin el avance de la informática no tendríamos a la firma digital, y de la misma manera que sin el sistema moderno de criptografía asimétrica tampoco tendríamos a la firma digital. Debido a ello necesitamos conocer más de estos sistemas de encriptación y de por qué permiten los niveles de seguridad que nos permiten hablar de la confianza digital y por consiguiente de la seguridad jurídica.

Según Núñez Miller (2017) la criptografía es el arte de convertir un mensaje legible en otro ilegible, a este proceso se le llama cifrado y por el contrario, la recomposición a un mensaje legible, toma el nombre de descifrado (p. 203).

Comenzamos estableciendo que la palabra criptografía proviene del griego de la conjunción de *kriptos*, que significa escondido u oculto y *graphos* que significa

grafía o escritura. Para la RAE (2021), este es el arte de escribir con clave secreta o de un modo enigmático. Nosotros consideramos más que un arte es un sistema de técnicas que permiten cifrar y descifrar mensajes, y en nuestro ámbito se traduce a datos digitales.

Podemos decir que la criptografía moderna nace con el estadounidense Claude Shannon, tal vez el fundador de la criptografía matemática. Con sus publicaciones *Communication Theory of Secrecy Systems* [Teoría de la comunicación de los sistemas secretos] en la *Bell System Technical Journal* [Diario de Sistemas Técnicos Bell], y el libro *Mathematical Theory of Communication* [Teoría Matemática de la Comunicación].

La criptografía es la encargada de estudiar el modo de transformar un texto original, en un texto cifrado o criptograma mediante una operación que dificulte a los terceros conocer el contenido del texto sin descubrir u obtener, en primer término, la clave que permite descifrarlo. Cuanto mayor sea el grado de dificultad que el método de cifrado opone a quienes intentan quebrarlo, mayor seguridad ofrecerá a quienes lo utilicen. Por lo tanto, podemos decir que la criptografía utiliza técnicas matemáticas relacionadas con aspectos de seguridad de la información, tales como la confidencialidad, la integridad de datos, la autenticación de entidades y la autenticación del origen de datos.

Por lo tanto, la finalidad de la criptografía va a ser la de garantizar el secreto en la comunicación entre dos partes y, por otra parte, la criptografía va a asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado no haya sido modificado.

Sin embargo, nosotros haremos foco sobre la criptografía más actual y la implementada en la firma digital. Decimos técnicamente que la firma digital es un conjunto de tecnologías de cifrado y descifrado implementadas mediante la aplicación de algoritmos criptográficos, o sea, esto último se hace en a través de la utilización de sistemas de criptografía asimétrica o de clave pública.

Altmark y Quiroga (2012) han sostenido

> … debido al riesgo y a la necesidad de generar la nombrada confianza digital se desarrolló el sistema de la Criptografía de Clave Pública (CCP) que cuenta

> con dos llaves complementarias, denominadas públicas y privadas. Cada usuario debe generar su propio par de claves, por intermedio de un software confiable. La clave pública de cada persona se difunde mientras que la privada se mantiene en secreto, bajo exclusivo control del suscriptor (p. 537).

Para cifrar un texto o un dato pueden usarse claves simétricas o claves asimétricas. Cuando se utiliza el sistema de claves simétricas, el emisor y el receptor del texto de que se trate utilizan la misma clave para cifrar y descifrar; Este tipo de criptografía comparte una misma clave y en esto reside su mayor debilidad, pues la necesidad de comunicarse claves entre emisor y receptor les hace necesario encontrar, además, un canal seguro para hacerlo. Para crearla se utiliza una fórmula matemática compleja, aplicarla sobre un mismo documento o mensaje devuelve siempre el mismo hash.

Estos números, se llaman claves y si bien son distintos, están relacionados de modo tal, que lo que se encripta con una clave o número, sólo se puede desencriptar con la otra clave o número.

A este par de claves se los conoce como clave pública y clave privada. La clave pública se distribuye y la clave privada la conserva el propietario protegido por una o varias contraseñas que sólo él conoce.

El par de claves funciona siempre en conjunto: No es posible encriptar y desencriptar un documento electrónico con una misma clave. Cuando se aplica la clave privada sobre un documento electrónico en su totalidad, este queda cifrado o encriptado. Es decir, se vuelve ilegible para cualquiera que no posea la clave pública con que descifrarlo.

A. Tipo de sistemas de criptografía

A lo largo de la historia, se han utilizado cientos de sistemas de criptografía diferentes, pero a grandes rasgos estos pueden dividirse en dos tipos:

Sistemas de criptografía de clave privada: utilizan la misma clave para cifrar y descifrar el mensaje. La clave secreta es compartida con el emisor y el receptor del mensaje. Este tipo también se conoce como criptografía simétrica.

Sistema de criptografía de clave pública: utilizan una clave pública para cifrar el mensaje y una clave privada para descifrarlo o viceversa. La clave privada debe mantenerse en secreto y la clave pública debe ser conocida por todas las restantes entidades que van a comunicarse con ella. Los sistemas de clave pública se conocen también como criptografía asimétrica.

Los sistemas de criptografía simétricos, o llamados también de clave secreta, privada o también clásicos, se caracterizan por que en ellos se usa la misma clave para cifrar y para descifrar.

La seguridad del cifrado simétrico depende de la privacidad de la clave, no de la privacidad del algoritmo. Es decir, se asume que no es práctico descifrar un mensaje teniendo el texto cifrado y conociendo el algoritmo de cifrado/descifrado. En otras palabras, no es necesario que el algoritmo sea secreto; lo único que hay que mantener en secreto es la clave. Esta característica del cifrado simétrico es la causa de su uso tan extendido.

La criptografía asimétrica o de clave pública utiliza un par de claves, una clave pública y una clave privada, para el envío del mensaje, una para cifrar y otra para descifrar el mensaje; lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. De este modo, estas claves tienen la propiedad de que, cada una de ellas, invierte la acción de la otra, pero, y aquí está el punto más relevante, a partir de una no se puede obtener la otra.

La criptografía asimétrica es muy usada, siendo sus principales servicios la confidencialidad, la integridad y la autenticación del origen de los datos, además del uso del mecanismo de firma electrónica avanzada o firma digital.

Por todo lo antes mencionado de manera unánime a nivel mundial, considera a la criptografía asimétrica o de clave pública, como la más segura y la única que se puede implementar de manera que cumpla con las características de la firma ológrafa hoy en día.

Los creadores de este sistema tal como ya adelantamos, fueron Diffie y Hellman, (1976) imaginaron un futuro en el que las personas se comunicarían regularmente a través de redes y sus mensajes podían ser robados o alterados, situación que sucede actualmente en internet. En noviembre de ese año, publicaron el artículo

denominado *New directions in crhyptography* [Nuevas direcciones en criptografía], que vino a introducir las ideas del cifrado y de las firmas digitales de clave pública, base para los protocolos de seguridad que utilizamos hoy en día.

Estos dos desarrollaron un algoritmo que mostraba que la criptografía asimétrica o de clave pública era posible. Actualmente, conocemos a la infraestructura fundada sobre las ideas de Diffie y Hellman como infraestructura de clave pública o por su sigla: *PKI.* A estos dos visionarios en el año 2015 se les otorgó el Premio Turing, considerado el más prestigioso a los aportes más brillantes en el campo de la ciencia informática y conocido como el Nobel de este campo, y que sin su aporte no existiría seguridad en materia de firma digital tal como la conocemos.

B. La función Hash

Establecemos ahora el sistema y el funcionamiento de este sistema criptográfico asimétrico. Al mensaje o documento que se quiere enviar de manera encriptada se le aplica una función hash, sobre este mensaje se aplica la clave privada, encriptando y obteniéndose así la firma electrónica avanzada o en nuestra legislación conocida como firma digital.

Luego se envía al destinatario el documento y el resumen hash encriptado o documento firmado digitalmente. Así mismo transmite su clave pública para ser utilizada en el proceso de verificación.

El receptor aplica la función hash al documento y desencripta el resumen encriptado, con la clave pública del emisor. Generalmente en el intercambio de información lo que se cifra no es el mensaje original, sino un resumen o hash o digesto seguro del mismo.

Un mensaje resumido mediante la función hash y encriptado con una llave privada es lo que en la vida real se denomina firma digital, dado que los sistemas de clave pública son muy lentos en vez de firmar digitalmente el texto completo se realiza sobre el hash.

La función hash [hasheo] es una función matemática o algoritmo criptográfico que transforma un documento digital en una secuencia de bits de longitud fija,

transforma al documento que contiene palabras y eventualmente números, en un resumen numérico llamado extracto o digesto de mensaje o resumen hash.

A partir de un mensaje en texto plano, se obtiene su resumen al aplicar una función hash determinada. Este resumen se firma con la clave privada del emisor y se envía al receptor. Simultáneamente se envía el mensaje original al receptor. Éste descifra el resumen mediante la clave pública del emisor, y aplica la misma función hash que él al mensaje recibido para obtener un resumen. Compara el resumen recién obtenido y el enviado por el emisor, si son iguales el mensaje es el inicial.

IX. Blockchain y firma electrónica

Decimos que el sistema de seguridad implementado en la autentificación de la manifestación de la voluntad actualmente se realiza a través de la tecnología de criptografía asimétrica y esta es una técnica bastante confiable.

Nos preguntamos entonces: qué sucedería si surge una tecnología más avanzada y qué sucedería si irrumpe en el escenario una nueva tecnología con un sistema más seguro. Para nosotros esta tecnología emergente es el *blockchain* [cadena de bloques], una de las nuevas tecnologías surgidas en la mencionada cuarta revolución industrial.

Seguimos Monroy (2020) cuando menciona que hemos oído hablar este término asociado a las famosas criptomonedas, pero lo que puede ofrecer blockchain es mucho más pues los procesos comerciales, jurídicos, de producción y muchos más comenzarán cada vez a utilizar esta tecnología o por lo menos, el futuro se basará en tecnologías similares que permitan dar seguridad y confianza, desarrolladas y mejoradas tomando como base inicial esta nueva herramienta (p. 56).

Asimismo, esta tecnología está diseñada para administrar un registro de datos online, caracterizada por ser transparente y prácticamente incorruptible. Además, incorpora otras tecnologías como lo son el *pier to pier* (o también conocía en español como red de pares), la prueba de trabajo y el hash, lo que nos lleva a afirmar, sin ningún lugar a dudas que el *blockchain* es una tecnología superior en todo sentido a la empleada por la firma digital, aun cuando comparte un poco de la tecnología.

Tales características, hacen al *blockchain* capaz de realizar muchísimas funcionalidades, entre ellas mencionamos a grandes rasgos, las criptomonedas, los contratos inteligentes, los tokens no fungibles, etc.

“Blockchain es un libro digital incorruptible de transacciones económicas que puede programarse para registrar no solo transacciones financieras, sino virtualmente todo lo que tiene valor” (García Mexía P.,2018, p. 42).

Así pues, la tecnología de *blockchain* también puede hacer posible la identificación del usuario y la consiguiente manifestación de la voluntad, basados en el consenso de los usuarios de la red de *blockchain*.

A. El Blockchain en Argentina

El CCyCN reformado por la Ley 26.994 establece en su segunda parte, al ocuparse de la forma y prueba del acto jurídico, que: “… para los instrumentos obtenidos por medios electrónicos, el requisito de la firma, satisfecho con la utilización de una firma digital, asegurando así la autoría e integridad del instrumento” (art. 288).

Después de la lectura del segundo párrafo de este artículo concluimos que la utilización de una firma digital es requisito de la firma de los instrumentos obtenidos por medios electrónicos, para asegurar su autoría e integridad.

Caramelo (2015) explica con respecto a este artículo tan importante para nosotros que

> La última parte del artículo se refiere a la firma en los instrumentos generados por medios electrónicos; para esos casos establece que el requisito de la firma queda satisfecho si se utiliza la firma digital en los términos que establece la ley 25.506 (p. 469).

Ahora bien, el artículo no especifica la modalidad de materialización de dicha firma, por lo que en concordancia con la normativa establecida por la LFD y tratándose de una norma general debe observarse lo dicho por esta última.

La Ley 25.506 establece que

> 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 (art. 2).

En este artículo concluimos que, para la existencia de la firma digital, el procedimiento matemático requiere información de exclusivo conocimiento del firmante (clave privada), encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes (clave pública). Hasta acá no habría ningún problema, pero la LFD se asienta sobre la infraestructura de clave pública argentina para la emisión de los certificados digitales y no otro tipo de red.

No debemos olvidar tampoco el Decreto 182, decreto reglamentario de la Ley 25.506, la Resolución Nº 399/2016 del Ministerio de Modernización que reemplaza la Decisión Administrativa Nº 927/2014 y la Disposición SSTG Nº 7/2015. Todas las normas mencionadas establecen los procedimientos y condiciones para la emisión de certificados digitales en el ámbito de la Infraestructura de Firma Digital de la República Argentina. Que nada dicen de la tecnología de *blockchain*.

Después de analizar los artículos concluimos que la tecnología de *blockchain* aún no se encuentra habilitada con los alcances de firma digital, por nuestro marco legal nacional, más allá de que sea utilizado como una firma electrónica.

Además de la definición del art. 2 de la LFD, tenemos los requisitos consagrados en el art. 9 del mismo cuerpo legal, el cual establece que la firma digital debe haber sido creada durante el período de vigencia del certificado digital válido del firmante, ser verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado y que el certificado haya sido emitido o reconocido por un certificador licenciado. Este último también responde a la Infraestructura de Firma Digital de la República Argentina, por lo que no menciona que esta comprenda participantes que autoricen o se encuentren con la tecnología de *blockchain*.

Analizados los artículos podemos llegar a la conclusión de que otro tipo de tecnología no se encuentra habilitada, por el art. 288 del CCyCN, para la utilización de la *blockchain*. No permitiéndonos la posibilidad de la inclusión de otra tecnología aún más segura y aún más práctica que la mencionada. Vemos que el *blockchain* no se puede incluir en el art. 288 del CCyCN, no porque el *blockchain* no permita

todo lo que la firma digital hace, sino porque el *blockchain* es una tecnología y un proceso más avanzado aún no enmarcado en el ordenamiento positivo nacional.

Por eso concluimos que el código de fondo argentino expresamente nos aclara que debe ser una firma digital, con los alcances y limitaciones que contiene la definición de esta, por lo que sí realizamos una manifestación de la voluntad por medios digitales y la plasmamos con la tecnología de *blockchain*, solo firmaremos electrónicamente.

Afirmamos a estas alturas que el *blockchain* es una de las tecnologías informáticas más seguras para almacenar información por medios electrónicos, por lo que con el avance del tiempo y el estado del arte tecnológico, lo podremos usar como medio de identificación. Prescindiremos de un usuario y una contraseña para acceder a webs como medio de identificación, sustituyéndolo por ID propia creada por nosotros para acceder a webs, firmar documentos electrónicos y plasmar la manifestación de la voluntad de la autoría a través de la tecnología del *blockchain*, y que muy posiblemente sea la nueva regla a la hora de firmar con medios electrónicos.

X. Conclusión

A través del presente capítulo analizamos cómo la firma electrónica se ha desarrollado hasta la que finalmente conocemos en nuestros días. Conocimos también la parte histórica de esta tecnología aplicada al derecho, que nos permitió identificar sus aspectos básicos para gradualmente llegar a los aspectos generales de la firma por medios electrónicos. Por ello hicimos necesario desarrollar una introducción, evolución y avance en materia de firma electrónica, y su impacto como parte del derecho informático en la historia. Establecimos también la revolución que significó la implementación de la firma electrónica en la historia del derecho produciendo un cambio de paradigma entre lo físico y lo digital.

Conocimos además la Ley Modelo sobre Firmas Electrónicas de la CNUDMI, una mirada a la recepción que la misma termino teniendo en el derecho comparado, y

aspectos generales que hacen a la firma electrónica y que terminaron por incluirse en casi todas las legislaciones del mundo, MERCOSUR y de la U.E.

Desarrollamos un tema bastante técnico, la criptografía, lo cual nos permite entender mejor el sistema sobre el que descansa la seguridad jurídica que tanto se necesita en la firma digital y por consiguiente en las transacciones electrónicas de los mercados actuales.

Por último, tocamos un tema muy actual e interesante como es el de la tecnología de *blockchain*, y su interrelación en el derecho argentino, situación que más que seguro se traerá a discusión en materia legislativa en cualquier momento.

Capítulo III

La firma digital en Argentina

I. Introducción

Decimos que el presente capítulo tiene como objetivo conocer la legislación argentina de firma digital, por un lado, la LFD y por el otro el CCyCN en el apartado correspondiente a la firma digital. Para ello establecemos que a través del análisis, relevamiento y comparación de distintas fuentes de información llegar a generalidades, antecedentes, conceptualizaciones, diferenciaciones, naturaleza jurídica, exclusiones, presunciones y todos los demás fundamentos teóricos de esta legislación en el marco nacional argentino. Gracias a lo mencionado, identificaremos los elementos fundamentales del tema en nuestro país.

Conoceremos la implementación de la misma desde el sector público nacional, situación que terminaría reemplazando la administración y la gestión de los servicios públicos por medios tradicionales por los medios electrónicos.

Destacamos que este capítulo reviste de vital importancia para introducirnos en la firma digital argentina y poder determinar el grado de implementación en derecho argentino para poder avanzar a los esquemas regionales e internacionales de esta temática.

II. Generalidades

A. Principios generales

La LFD ha sido establecida en nuestra legislación con el objeto de facilitar, agilizar, efectivizar, de manera segura e inmediata la firma de documentos electrónicos como prueba de la autoría de la declaración de voluntad expresada en el texto al cual corresponde.

“La irrupción de las nuevas tecnologías de la información y las comunicaciones han puesto en crisis varios paradigmas con los que nos manejamos tradicionalmente en el derecho” (Altmark y Molina Quiroga, 2012, p. 519).

Ahora bien, la LFD Argentina 25.506, establece y regula la firma digital y la firma electrónica en Argentina, considerándola equivalente a la firma ológrafa otorgándole su validez legal y todos sus efectos jurídicos que ello conlleva.

“La base tecnológica para otorgarles la validez jurídica estará dada por el establecimiento de la infraestructura de firma digital que ofrece autentificación y garantía de integridad de los documentos digitales y/o electrónicos” (Bibiana, 2006, p. 30).

Al entrar en el concepto de firma digital estamos aludiendo a una variedad de conceptualizaciones relativas al mismo. Elementos como el certificado digital, el documento electrónico, la criptografía, claves públicas y privadas, etc. Conceptos que jamás hemos escuchado o de haberlo hecho, fue en contadas y específicas ocasiones.

Para la LFD la firma electrónica es el conjunto de algoritmos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación que carezca de algunos de los requisitos legales para ser considerada firma digital.

De tal modo, podemos decir que la firma electrónica es un conjunto genérico y con relación a la firma digital (firma electrónica avanzada) tiene un carácter residual. La principal consecuencia radica en el valor probatorio atribuido a cada uno de ellos, dado que, en el caso de la firma digital, como veremos más adelante, existe una presunción iuris tantum en su favor, gracias a unas presunciones que se le otorgan al utilizar un sistema criptográfico más severo, mientras una firma electrónica, en caso de ser desconocida por su titular corresponde a quien invoca acreditar su validez”.

La ley 25.506 incorpora la firma digital como herramienta de aplicación cuasi obligatoria al derecho positivo vigente, en todas sus ramas, focalizándose en el CCN (vigente en aquella época de su sanción) y al CCyCN (siendo que, en este cuerpo

normativo, se encuentra expresamente integrada) como también toda ley especial que regule instrumentos públicos o privados.

Los principios normativos que debería contemplar toda legislación referida a la firma electrónica están contemplados en nuestra ley y pueden resumirse de la siguiente manera:

a) Compatibilidad con el marco jurídico internacional: Se refiere a la visión internacional de la legislación referente a la firma electrónica desde el punto de vista legislativo y tecnológico, a fin de permitir la inserción del país en el mercado mundial del comercio electrónico, en este trabajo es algo primordial.

b) Neutralidad tecnológica: Se hace referencia aquí a la no discriminación entre distintas tecnologías y, en consecuencia, la necesidad de producir normas que regulen los diversos entornos tecnológicos. Este principio refiere a la flexibilidad que deben tener las normas, es decir, que las mismas no estén condicionadas a un formato, una tecnología, un lenguaje o un medio de transmisión específico. No se debe favorecer a una determinada tecnología para las firmas y certificados electrónicos.

c) Establecer la equivalencia de la firma digital a la firma ológrafa: Se considera que la misma satisface el requerimiento de firma respecto de los datos consignados en forma electrónica y que tiene los mismos efectos jurídicos que la firma ológrafa con relación a los datos consignados en papel.

d) Establecer la libre competencia: Referida a todos los servicios relacionados con la certificación de las firmas electrónicas.

e) Respeto a las formas documentales existentes: Significa no obligar a la utilización de la firma electrónica en lugar de la firma ológrafa, sino que su utilización es voluntaria.

f) Libertad contractual: Permite a las partes convenir la modalidad de sus transacciones, es decir, si aceptan o no las firmas electrónicas.

III. Antecedentes legislativos argentinos

La LFD Argentina N° 25.506 se sancionó el 14 de noviembre del año 2001 en base al Proyecto de los diputados Pablo A. Fontdevila, Irma F. Parentella y Norberto R. Nicotra (Expte. 3534-D-00), y fue precedida de numerosos otros proyectos sobre el tema, provenientes tanto del propio parlamento como del Poder Ejecutivo argentino: Proyecto de los diputados Alfredo N. Atanasof y Graciela Camaño (Expte. 7331-D-00); Proyecto de los Diputados José M. Corchuelo Blasco, Mario A. Cafiero y Ricardo A. Patterson (Expte. 4175-D-00); Proyecto de la Diputada Adriana V. Puiggrós (Expte. 5460-D-00), Proyecto de los Diputados Enrique G. Cardesa, Marcela Bordenave y Margarita R. Stolbizer (Expte. 7099-D-00); Proyecto de los Senadores Pedro Del Piero y Luis Molinari Romero (Expte. S-1155/00); Anteproyecto de Ley Formato Digital de los Actos Jurídicos de la Jefatura de Gabinete de Ministros. En el Informe de las Comisiones de Comunicaciones e Informática y de Legislación General, que acompaña el proyecto sancionado, se reconocen a estos proyectos como antecedentes de la ley.

El 19 de febrero de 1985, se firmó el Decreto 333 relativo a “Normas para la elaboración, redacción y diligenciamiento de los proyectos de actos y documentación administrativa”. Después en el año 1987, la secretaría de justicia de la nación encargó la redacción de un anteproyecto de ley en la que se le otorgaría valor jurídico y probatorio al documento electrónico. Más adelante el 16 de abril de 1998, mediante el Decreto 427 se abrió el camino de la firma digital en la Administración Pública (APN). Poco tiempo después, el 27 de noviembre de 1998 la Resolución 194, permitió establecer los estándares sobre tecnología de firma digital para la APN, hasta que el Decreto 78 del 10 de enero del 2002, definió sobre en quiénes recaerá estos temas. Finalmente, la LFD, que como ya mencionamos fue sancionada el 14 de noviembre del 2001, pero hasta la aparición del Decreto 2628 el 19 de diciembre del 2002, que reglamenta la LFD Argentina y que fue firmado en, no podía hacerse mucho.

Listado de los antecedentes legales nacionales de la firma digital argentina:

• Decreto N° 283/03- Autorizase a la ONTI - Oficina Nacional de Tecnología Informática a emitir certificados digitales.

• Decreto N° 2.628/02 - Reglamentación de la Ley 25.506.

• Decreto N° 658/02 - Obligaciones Tributarias: Declaraciones por Medios Electrónicos.

• Decreto Presidencial Nº 1023/01. Régimen de Contrataciones de la Administración Pública Nacional - Art. 21: Contrataciones en formato digital.

• Administración Pública Nacional. Decisión Administrativa Nº 102/2000. Prórroga del Decreto Nº 427/98 de Firmas Digitales para la Administración Pública.

• Decreto Presidencial Nº 427/98. Firmas Digitales para la Administración Pública Nacional.

• Administración Pública Nacional. Decisión Administrativa Nº 118/2001. Proyecto de Simplificación e Informatización de Procedimientos Administrativos (PRO-SIPA).

• Resolución N° 176/02 Jefatura de Gabinete de Ministros. Sistema de tramitación electrónica para la recepción, emisión y archivo de documentación en formato digital firmada digitalmente de la Subsecretaría de la Gestión Pública.

• Resolución General CNV N° 345/99 Comisión Nacional de Valores. Remisión y Publicación de Información Financiera de Emisoras de Títulos Valores y Calificadoras de Riesgo por la Autopista de la Información Financiera en Internet Web.

• Resolución MTSS N° 555/97 Ministerio de Trabajo y Seguridad Social. Normas y procedimientos para la incorporación de Documentos y Firma Digital.

• Resolución SAFJP Nº 293/97 Superintendencia de Administradoras de Fondos de Jubilación y Pensiones. Incorporación del Correo Electrónico con Firma Digital.

• Resolución SFP Nº 45/97 Secretaría de la Función Pública. Incorporación de Tecnología de Firma Digital a los Procesos de Información del Sector Público

• Resolución SFP Nº 194/98 Secretaría de la Función Pública. Estándares Aplicables a la Infraestructura de Firma Digital para el Sector Público Nacional del Decreto Nº 427/98

• Resolución SFP Nº 212/98 Secretaría de la Función Pública. Políticas de Certificación para el Licenciamiento de Autoridades Certificantes

• Resolución AFIP Nº 474/99 Administración Federal de Ingresos Públicos. Régimen de Declaraciones Juradas Impositivas y Provisionales por Internet.

• Proyecto de Ley de Nuevo Código Civil, Artículos (con fundamentos) relevantes a la Digitalización (LIBRO II - De la Parte General, TÍTULO IV - De los Hechos y Actos Jurídicos, Capítulo III - Forma y Prueba de los Actos Jurídicos, Artículos 260-69, 277, 289, 290, 294, 296, 303, 311 y 315.).

• La Provincia de Buenos Aires adhirió a la Ley 25.506 a través de la Ley 13.666 del año 2007. Dicha ley provincial fue reglamentada por el Decreto Nro. 305 del año 2012.

IV. Ley de Firma Digital Argentina 25.506

Tal como mencionamos, en el año 2001 se sancionó la ley 25.506, que regularía la firma digital, la firma electrónica y los documentos electrónicos, que fue reglamentada originalmente por el Decreto 2628/2002, modificada por el Decreto 724/2006 y que finalmente la decisión administrativa del jefe de gabinete de ministros 6/2007 estableció los requisitos para los certificadores licenciados. Esta ley reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital, su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina.

A. Estructura de la Ley de Firma digital argentina

El art. 1 de la LFD expresa que se reconoce el empleo de la firma digital y su eficacia jurídica en las condiciones que establece la normativa. Los artículos siguientes determinan cuáles son los requisitos para que la firma digital tenga la plena eficacia que la ley reconoce.

A pesar del ámbito de alcance que parecería derivar de este artículo introductorio, la ley avanza sobre algunas cuestiones no incluidas en este objetivo, tal como el reconocimiento de la validez del documento digital no firmado tal como se establece en el art. 6 de la LFD.

El artículo va en línea con el objetivo reconocido a la firma digital de reducir los riesgos e inseguridades derivados de la utilización de mensajes digitales a través de la red. Las comunicaciones por redes abiertas están sujetas a ciertos riesgos: que el autor y fuente del mensaje haya sido suplantado, la alteración provocada o accidental, del mensaje trasmitido, el repudio del mensaje, tanto por parte del emisor cuando por parte del receptor, la intercepción del mensaje por persona no autorizada.

Es necesario, entonces, implementar herramientas tecnológicas que nos permitan asegurar que el mensaje proviene de quien dice enviarlo, que no ha sido alterado desde su envío, el no repudio o rechazo respecto al envío y a la recepción del mensaje y la confidencialidad. A estos fines la ley determina los requisitos para que la firma digital cumpla con algunas o todas las funciones mencionadas.

“Uno de los aspectos más trascendentes es la equiparación entre firma manuscrita y firma digital” (Altmark y Molina Quiroga, 2012, p. 589).

El art. 3 dice: “cuando la ley requiera una firma manuscrita esa exigencia también queda satisfecha por a una firma digital. Este principio es aplicable a los casos en los que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia”.

B. Conceptualizaciones

Conceptualizamos en un primer lugar el significado de firma digital y firma electrónica. Donde bajo el nombre genérico de firma electrónica, o firma digital que en otras legislaciones se trataría de firmas electrónicas avanzadas donde existen diferentes grados de seguridad. En el grupo de trabajo de comercio electrónico de UNCITRAL existen tres niveles de firmas electrónicas, la firma, firma electrónica y firma electrónica segura.

Decimos que una firma digital es una cantidad determinada de algoritmos matemáticos (que se genera a través de un certificado digital emitido por una autoridad certificante licenciada por un órgano público) y que fue creada utilizando para ello una clave privada originada a través de un método de cifrado denominado

criptografía asimétrica, donde es utilizada una clave pública para verificar que dicha firma digital fue realmente generada utilizando la clave privada correspondiente a la persona titular del certificado digital, siendo la misma plasmada a un documento digital (donde queda plasmada la voluntad del signatario) revistiendo de la correspondiente validez jurídica. El algoritmo a utilizar para generar la firma debe funcionar de manera tal que sin conocer la clave privada del titular del certificado sea posible verificar su validez. A tal fin, la Ley 25.506 concibe una Infraestructura de Firma Digital, bajo la órbita de la Jefatura de Gabinete de Ministros.

Es así que la LFD nos otorga un concepto de firma digital, manifestando que

> 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 (art. 2).

Aplicar a un documento digital: de acuerdo con la definición de firma digital no existe un documento digital si no es con los requisitos de la misma ley.

Un procedimiento matemático: la firma digital es un procedimiento matemático (código binario) realizado automáticamente por una computadora, generando un par de claves como luego explicaremos.

Información de exclusivo conocimiento del firmante: requiere información que en la en la mayoría de los casos supone sólo pertenece a la esfera del exclusivo conocimiento de quien quiere firmar. Según la definición de la Ley 25.506, debe ser de conocimiento exclusivo del que firma, pero el que lo comparta al conocimiento no le quita ese carácter.

Encontrándose ésta bajo su absoluto control: aquí sucede el mismo inconveniente que en el punto examinado arriba; esto se trata más que nada de una recomendación, pero no integra la definición ni la naturaleza de la norma. Debe ser de su conocimiento exclusivo y estar ‘bajo su absoluto control’. Esto supone tener en todo momento la posibilidad de su utilización, sin depender de terceras personas, pero el que el firmante resuelva compartirlo, nuevamente no quita el carácter de firma digital.

Susceptible de verificación: ésta es una de las más importantes características de la ley, de una importancia tal que si ello no se verifica por las entidades certificadoras no estaríamos frente a una firma digital sino frente a una firma electrónica.

Posibilidad de identificar al firmante: la firma digital debe permitir la identificación del firmante de manera indubitable. Por lo tanto, estamos aquí ante una ventaja sobre la simple firma ológrafa, ya que esta no identifica necesariamente al firmante.

No alteración del documento digital: finalmente la firma digital debe proteger la inalterabilidad del documento digital con lo cual ya que sería imposible de que el firmante niegue o repudie el documento digital. En otras palabras, está introduciendo el concepto del 'no repudio' que requieren otras legislaciones. En esto la ley de firma digital es superior a la firma ológrafa tradicional, que no garantiza la inalterabilidad del documento, una ventaja más sobre la firma ológrafa o manuscrita.

Por su parte Bielli y Nizzo (2017) han definido la misma de la siguiente manera

> Una Firma Digital es una cantidad determinada de algoritmos matemáticos y que fue creada utilizando para ello una clave privada originada a través de un método de cifrado denominado criptografía asimétrica, donde es utilizada una clave pública para verificar que dicha Firma Digital fue realmente generada utilizando la clave privada correspondiente a la persona titular del certificado digital, siendo la misma plasmada a un documento digital revistiéndolo de la correspondiente validez jurídica. El algoritmo a utilizar para generar la firma debe funcionar de manera tal que sin conocer la clave privada del titular del certificado sea posible verificar su validez (p.48).

En el art. 9 establece tres requisitos para otorgarle validez a la firma digital: el primero es que haya sido creado durante el periodo de vigencia del certificado digital; ser debidamente verificado por la referencia a los datos de verificación de firma digital indicados en dicho certificado; y último que dicho certificado haya sido emitido o reconocido por un certificador licenciado.

Por lo tanto, la LFD Argentina establece con respecto a su validez lo siguiente

> Una firma digital es válida si cumple con los siguientes requisitos: a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante; b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado (art. 9).

Este sería el dique de contención que diferenciara y filtra así la firma digital de la firma electrónica. Los procedimientos de firma y verificación van a ser determinados por la autoridad de aplicación.

La firma electrónica en nuestra legislación es un concepto mucho más abarcativo que el de firma digital, resultando una relación de género y especie entre ambas nociones. La firma electrónica concibe un marco normativo que le otorga validez jurídica a la firma digital. Es en sí, un conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, pero que carece de algunos de los requisitos legales esenciales para ser considerada Firma Digital.

La LFD Argentina nos da una definición de firma electrónica

> Se entiende por 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 para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien le invoca acreditar su validez (art. 5).

Aquí debemos decir que autores como Altmark y Molina Quiroga (2012) no consideran conveniente incorporar definiciones de este tipo en nuestra LFD ya que en materias como las ligadas a las tecnologías en las cuales podrían a corto plazo transformar también en obsoleta la definición.

“En efecto, en primer lugar, consideramos que no es conveniente ni de sana técnica legislativa incorporar legislaciones en una norma jurídica sobre todo en materias como las ligadas a la irrupción las tecnologías de la información, en las cuales la rápida obsolescencia, podría a corto plazo transformar también en obsoleto un concepto determinado” (Altmark y Molina Quiroga, 2012, p. 587).

Además de lo mencionado estos autores consideran que las definiciones de firma electrónica o firma digital no requiere ser definidas para su comprensión: “ya que basta con el concepto general de que ambas son formas que la tecnología pone a disposición de la sociedad para identificar adecuadamente al emisor y al receptor de una declaración de voluntad” (Altmark y Molina Quiroga, 2012, p. 587).

Se consideran ejemplos claros de su empleo: la clave que utilizamos para operar un cajero automático, como así también cuando se utiliza cualquier tipo de

verificación de seguridad que efectivamente no sea la firma digital, ya sea la identificación mediante el iris, mediante la huella digital, y desde la inserción de una clave de validación en las operaciones con débito, hasta la contraseña que utilizamos para desbloquear nuestro celular. Todos estos procesos pueden ser considerados firma electrónica.

En este concepto amplio y tecnológicamente indefinido de firma, tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (por ej. la firma manual digitalizada) incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de valor probatorio a efectos de autenticación, aparte de su nula aportación respecto a la integridad del mensaje.

C. Diferenciación entre firma electrónica y firma digital

Ahondando en el tema, la diferencia fundamental que posee una firma digital frente a una firma electrónica son las exigencias necesarias para su implementación, siendo las mismas mucho más severas en la firma digital. Esta diferenciación es importantísima para nuestro trabajo puesto que los efectos legales en materia de presunciones y de carga probatoria difieren en nuestra legislación, según se trate de una firma digital o una firma electrónica.

La primera cuenta a su favor con las presunciones de integridad y de autoría, según lo dispuesto por los arts. 7 y 8, y por ende parten de la condición de no repudio. Por su parte la firma electrónica según el art. 5 carece de ellas, y de allí que conforme la ley, en caso de ser desconocida corresponde a quien la invoca acreditar su validez, algo que no sucede en la digital puesto que consta de presunciones va de suyo que se obtienen sólo a través de los requisitos para ser una firma digital.

Pero de todas formas la firma electrónica fue incluida en el entramado normativo de la ley argentina, dada la proyección que hizo el legislador de los posibles y continuos avances tecnológicos que se suceden ininterrumpidamente con el paso del tiempo, ya que, como dijimos, el concepto de firma electrónica es mucho más amplio que el de firma digital.

Sostenemos entonces que la firma digital es en un génesis, un procedimiento matemático cifrado por medio de dos claves (una pública y una privada), y que, mediante su incorporación, reviste de validez jurídica un documento digital al cumplimentar el requisito de firma. La clave privada es de solo acceso y conocimiento por el titular firmante y la clave pública es la que otorga al acto validez jurídica frente a los terceros.

Cuando hablamos de firma digital decimos que con la misma se asegura de manera categórica y concluyente la identidad del firmante mediante su vinculación con el certificado digital propio, como así también la inalterabilidad del documento digital en el cual se ve incluida la voluntad del signatario y, en consecuencia, la fecha y la hora de la firma, logrando de esta forma ser considerada de manera análoga con una firma ológrafa y sus requisitos de fondo. Está configurada por métodos matemáticos cifrados que son propios y únicos del titular de la misma, logrando un marco de seguridad inviolable.

En los procesos electrónicos legales y judiciales, es necesario revestir de efectividad, privacidad, seguridad y potestad jurídica al método aplicado para la elaboración de escritos o presentaciones electrónicas como así también para las notificaciones electrónicas, siendo que es condición sine qua non constatar de manera acabada y determinante la identidad del sujeto firmante y consecuentemente la veracidad, integridad y correspondencia del documento digital al que se le aplicó la firma digital, que es donde consta la voluntad que se quiso plasmar a través de su contenido.

A raíz del nexo que se produce al emplear tanto la clave privada para cifrar el contenido íntegro del documento digital remitido, como así también la clave pública que utiliza el destinatario para acceder al mismo y constatar que efectivamente fue firmado por el titular de la certificado digital generado del documento electrónico, es que se logra crear un ecosistema de seguridad extremadamente efectivo, dentro del cual y en lo que a la praxis legal, se lleva a cabo la digitalización de un procedimiento judicial.

La jurisprudencia argentina no se ha mantenido al margen al respecto del tema. En el año 2008 con el fallo “Bieniauskas, Carlos c/ Banco de la Ciudad de Buenos

Aires", y de nuevo el fallo más actual "Banco de la Provincia de Buenos Aires c/ Spindola Sabrina Lorena s/ cobro ejecutivo" diferenciando en ambos casos a la firma digital con los alcances de los arts. 7 y 8 de la ley 25.506; y los art. 287 y 288 del CCyCN en contraposición con la firma electrónica.

D. Naturaleza Jurídica

Podemos inferir que la naturaleza jurídica de la firma digital es la de un medio que vincula al titular con los actos jurídicos que declara al firmar el documento y, a su vez, un medio de certificación de los mensajes que se envían.

En resumen, se trata de un medio de prueba de la manifestación de la voluntad, de la autoría y de la integridad de un documento digital. Esta circunstancia es la que le va a otorgar seguridad jurídica.

En conclusión, la naturaleza jurídica de la firma digital es la de un medio de seguridad, cuya funcionalidad probatoria permite la identificación de una persona y de la autoría del mensaje, además de asegurar la integridad del mismo.

E. Documento digital en la Ley de Firma Digital argentina

No podemos continuar hablando de la LFD Argentina sin referirnos al documento digital, cómo es conceptualizado y tratado en la misma.

El art. 6 de la Ley 25.506 nos da el concepto de documento digital, donde a grandes rasgos 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.

Para ésta es la representación digital de actos y hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Es relevante que la norma que disponga que un documento digital también satisface el requerimiento de escritura, es decir cualquier soporte de una declaración de una voluntad electrónica reúne los requisitos a los fines de adquirir valor y eficacia jurídica que

la ley le otorga a los documentos digitales. Concebimos al documento, en sentido amplio, como todo objeto susceptible de representar una manifestación del pensamiento, con prescindencia de la forma en que esa representación se exterioriza.

Pasaremos entonces a hablar del valor probatorio del documento electrónico, de los públicos o privados y sus efectos.

La temática de la autenticidad de los documentos electrónicos es indiscutida, dado que como ya mencionamos, a través de los elementos que conforman su génesis, se puede garantizar su objetividad, autoría, fidelidad y seguridad. Se hace necesaria una enorme infraestructura para falsificar un documento electrónico si nos basamos en los recaudos de seguridad que incorporan de por sí hoy en día. Consecuentemente se considera al mismo como una alternativa eficaz y de confianza que el documento papel suscrito mediante firma ológrafa. En lo que respecta a la relación documento electrónico y documento digital, sucede lo mismo que ocurre con la firma electrónica y la firma digital, siendo esta una relación de género y especie. Documento electrónico es el género siendo mayormente abarcativo y comprensivo de varios conceptos asimilables, mientras que documento digital es la especie, una forma específica de documento electrónico.

La LFD Argentina define al documento digital en el art. 6: “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.”

El documento digital es el instrumento donde queda plasmada la voluntad de su creador, al que se le aplica la firma digital, dotándolo del carácter de integridad, inalterabilidad y de conexidad consecuente con el titular signatario, a través de la presunción de autoría.

De esta manera, y a través de un conjunto de presunciones legales, se produce el principal efecto jurídico de la firma digital que es la instrumentación de la manifestación de voluntad respecto al contenido del documento digital.

A lo largo de innumerables años, hemos habituado nuestro raciocinio a vincular automáticamente una firma ológrafa a un escrito en papel. Esto se ha mantenido

inalterable a través del tiempo y el impacto que produce la ley nacional de firma digital en la materia, no es de menor consideración. Implica un cambio de paradigma trascendental en favor de las nuevas tecnologías.

Un documento digital firmado digitalmente es intangible, no se puede sentir a través del sentido del tacto tal como lo hacemos con el papel, no se puede oler, no se puede arrugar, no se puede percibir al tacto. Pero, sin embargo, se encuentra ahí y tiene el mismo valor legal y probatorio que el papel firmado ológrafamente.

El Decreto Reglamentario 182 del año 2019 de la LFD dice: La Autoridad Certificante Raíz es la Autoridad Certificante administrada por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS…" (art. 5).

Entendemos que dicho organismo tendrá a su cargo la facultad de establecer los procedimientos y el marco regulatorio requerido para producir, conservar y transmitir un documento digital.

Si concebimos la generación de un documento digital, a partir de las numerosas medidas de seguridad implícitas que se encuentran impregnadas en él, como asimismo los diferentes grados de validación y verificación de autoría que conlleva, nos encontramos en un pie de igualdad del instrumento en soporte papel, y es íntegramente verificable a través de la utilización de un método u otro, su correspondencia de autoría, la voluntad plasmada del firmante y la validez jurídica y probatoria del acto configurado.

Para clarificar, conceptualizaremos y clasificaremos los diversos tipos de documentos electrónicos que rigen el entramado normativo del derecho positivo argentino, públicos y privados. Varios doctrinarios han sostenido que, en el derecho positivo nacional, los documentos electrónicos pueden ser divididos en dos grandes grupos.

En primer orden se consideran documentos públicos los que emanan de un funcionario público en el ejercicio de su función, confeccionados con las formas establecidas por la normativa vigente. Por otro lado, concebimos a los documentos privados (bajo un régimen de exclusión) a todos aquellos que no revisten las cualidades requeridas para ser considerados documentos públicos. Los

instrumentos privados se encuentran caracterizados por dos pilares fundamentales, que son ni más ni menos que el requerimiento de firma y el doble ejemplar.

En relación a la existencia de la firma impregnada en el documento, no hay discusión doctrinaria que sostenga la imposibilidad de cumplir con ese requisito a través del empleo de la firma digital, siendo que, a través de un certificado digital, vincula de manera certera e inequívoca la autoría del titular signatario, y en forma derivada, logra revestir de validez jurídica al documento electrónico donde quedó plasmada su voluntad.

Aclarado lo anterior, podemos manifestar que en la Argentina se cuenta en la actualidad con la tecnología requerida para conceder valor probatorio al documento electrónico.

Solo es necesario adaptar la normativa de fondo e incluir este tipo de concepciones y categorizaciones con el objeto de cumplimentar los requisitos necesarios para que el documento electrónico posea valor probatorio indiscutido, dejando de lado todas las discusiones doctrinarias existentes al respecto y armonizar nuestra legislación con la internacional, como bien se hizo con la firma digital en el CCyCN.

F. De los certificados digitales y el certificador licenciado

La LFD va a establecer lo que se entiende por certificado digital: “Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular” (art. 13).

Por lo tanto, decimos que para la ley el certificado digital habilita a su titular a la elaboración de documentos digitales firmados digitalmente. Además, el certificado digital es firmado digitalmente por un certificador. Por ello es un elemento necesario para firmar digitalmente que debe ser emitido por un certificador licenciado por el estado.

En resumen, es necesario para la emisión de certificados digitales contar con una infraestructura soportada por un sistema de criptografía asimétrica.

“El certificador licenciado se constituye en el tercero de confianza (*Trusted Third Party*) y se transforma en la garantía sobre la que se desarrolla el sistema” (Bibiana, 2006, p. 73).

La LFD argentina incorpora lo que se llama entidad certificante, es decir, aquella que cuenta con la tecnología de criptografía asimétrica adoptada por nuestra legislación nacional que es la que va a permitir emitir los certificados de firma digital. La estructura adoptada por nuestra legislación hace necesario entidades que cuenten con licencia concedida por el estado a través de la autoridad de aplicación tal como se establece en el art. 17: “se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismos públicos que expide certificados, presta a otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

El certificador licenciado es el encargado de las actividades establecidas en el art. 19 de la LFD: a) Emitir certificados digitales; b) Definir sus políticas de certificación; c) Identificar los certificados; d) Mantener copia de los certificados; e) Revocar los certificados emitidos. Y este se constituye en un tercero de confianza y en la garantía sobre la que se desarrolla el sistema, razón por la cual se establece un mecanismo de supervisión de sus actividades y se les imponen obligaciones a cumplir en el desempeño de las mismas, así como también serán responsables por sus incumplimientos y negligencias en el desarrollo de sus tareas y se les podrán imponer sanciones conforme el art. 41.

G. Valor probatorio de la Firma Digital

Aclarado lo anterior podemos afirmar que la firma digital es una firma electrónica avalada por una Autoridad Certificante, que a través de los requisitos de verificación necesarios permite establecer la conexidad entre la titularidad de quien suscribe el documento digital, su voluntad plasmada en el mismo y la integridad propia de dicho documento, logrando de esta forma producir una analogía entre la firma ológrafa y la firma digital conforme lo determina hoy por hoy el CCyCN.

La LFD establece la validez jurídica que se le otorga al documento digital, manifestando expresamente que este es la representación digital de actos o hechos, más allá del soporte utilizado para su fijación, almacenamiento o archivo. Asimismo, el art. 11 agrega, que las reproducciones que se hagan del documento electrónico serán consideradas originales y poseen, como consecuencia de ello, valor probatorio como tales equiparando al suscripto primario.

En el mismo orden, decimos que "un documento digital también satisface el requerimiento de escritura. Siendo que, de esta manera, la dualidad existente entre el formato papel y el formato electrónico pasa a ser un equivalente en sentido estricto, revistiendo ambos del mismo valor probatorio legal en un proceso judicial. Podemos agregar que el documento digital tiene un marco regulatorio propio cuyos cimientos son la Infraestructura de Firma Digital Argentina.

La normativa establece expresamente una presunción de autoría en lo que respecta a la relación vinculante con la identidad del signatario como asimismo una presunción de integridad acerca de la voluntad plasmada dentro del documento y su validez jurídica implícita. Estas dos presunciones conjuntamente con la de inalterabilidad, invierten la carga probatoria al tener que demostrar aquel que niega la autenticidad de la firma digital o la integridad del documento, que el mismo posee algún defecto legal de fondo o de forma.

Por ende, decimos que quien desconozca en juicio la validez de una firma digital, es quien debe producir la prueba necesaria para sostener su posición, dado que en este caso la carga probatoria se invierte como sucede al negar la autenticidad de todo instrumento público.

H. La confianza digital

La Ley 25.506 nos va a traer el concepto de confianza digital como uno de los pilares fundamentales del sistema, la seguridad.

Sostenemos que es necesario para una correcta aplicación de la firma digital, que la interfaz elaborada por la autoridad de aplicación, nos brinde la confianza necesaria para lograr adoptarlo como nuestro medio de uso habitual para promover, gestionar y compulsar un proceso judicial en forma íntegra. Generar la confianza digital, era la única manera de lograr que el sistema se apruebe masivamente en lo que respecta a su utilización.

Varias son las características necesarias para que un sistema se considere digno de confianza digital, siendo que entre ellas podemos encontrar: el mantenimiento en el tiempo de la integridad de los documentos que firmamos digitalmente, como así también inalterabilidad e invulnerabilidad de estos instrumentos donde se encuentra la voluntad que queda plasmada por el titular del certificado digital, impidiendo que sea modificado o alterado por un tercero. Esta es una de las principales características de la firma digital en la Argentina.

Bielli y Nizzo (2017) han sostenido que

> Es necesario para una correcta aplicación de la Firma Digital, que la interfaz elaborada por la autoridad de aplicación, nos brinde la confianza necesaria para lograr adoptarlo como nuestro medio de uso habitual para promover, gestionar y compulsar un proceso judicial en forma íntegra. Generar la confianza digital, era la única manera de lograr que el sistema se apruebe masivamente en lo que respecta a su utilización (p.52).

Un documento digital, una vez que es firmado se torna inalterable. No puede ser modificado por terceros bajo ningún punto de vista gracias al enorme grado de encriptación mediante el cual se encuentra revestido.

La firma digital debe proteger la inalterabilidad del documento digital con lo cual es asegurada la identidad de quien la firma y la autenticidad del documento digital, y sería imposible que el firmante niegue o repudie el documento digital. En otras palabras, está introduciendo el concepto del no repudio que requieren otras legislaciones.

Así, un documento electrónico de la especie inalterable presentaría, en un comienzo, una mayor idoneidad al momento de oficiar como documento de registro, toda vez que podría asegurar la intangibilidad de los datos.

Otra característica que posee el sistema es la autenticidad a través de la vinculación, o sea, que el documento haya sido efectivamente firmado por el creador del mismo, quien solamente puede ser el titular del certificado digital autorizado por la autoridad certificante. Es así, y como ya mencionamos, que la autenticación se establece mediante la utilización de la clave privada que posee cada sujeto usuario del sistema en particular logrando de esta forma cifrar el documento; siendo que dicho instrumento será eventualmente descifrado por el destinatario mediante la clave pública que posee el remitente, para poder dar con el contenido del mismo y establecer la conexidad necesaria con el firmante y el contenido de dicho documento.

Se puede manifestar con un enorme grado de certeza, que estos instrumentos poseen una mayor protección que los documentos en soporte papel firmados ológrafamente a los que estamos acostumbrados y habituados en tantos años de ejercicio profesional. Todo esto fundamentándose en el complejo cifrado aplicado y la cantidad de validaciones requeridas para lograr suscribir mediante la firma digital un documento digital; y a razón de lo dicho, han sido adoptados como medios de gestión del proceso y expediente electrónico en nuestro país y en varias naciones alrededor del mundo como por ejemplo Chile, Brasil, Uruguay, Paraguay, etc.

Las medidas de seguridad que el mismo posee, como así también la celeridad que brinda en el impulso procesal de un expediente y su utilización de forma remota, sumado a las nuevas funcionalidades y ventajas que se vayan incorporando con el tiempo, contribuirán a que un número mayor de profesionales se sumerjan en la gestión judicial informática de un expediente.

I. Firma Digital y Confidencialidad

En ocasiones, además de garantizar la procedencia de los mensajes electrónicos que se intercambian a través de medios informáticos y la autenticidad o integridad de los mismos, puede ser conveniente garantizar también su confidencialidad. Ello implica tener la certeza de que el mensaje enviado por A (emisor) únicamente será leído por B (receptor) y no por terceras personas ajenas a la relación que mantienen A y B.

En tales casos, también se acude al cifrado del mensaje con el par de claves, pero de manera diferente al mecanismo propio y característico de la firma digital. Para garantizar la confidencialidad del mensaje, el cuerpo del mismo (no el hash o resumen) se cifra utilizando la clave pública de B (receptor), quien al recibir el mensaje lo descifrará utilizando para ello su clave privada (la clave privada de B). De esta manera se garantiza que únicamente B pueda descifrar el cuerpo del mensaje y conocer su contenido.

J. Exclusiones. Marco interpretativo

La LFD realizaba una serie de exclusiones taxativas establecidas en el artículo 4 del régimen de este cuerpo legal, actualmente derogado, que establecía los casos y los que no eran aplicable la firma digital.

Establecía que: Las disposiciones de esta ley no eran aplicables:

a) A las disposiciones por causa de muerte;

b) A los actos jurídicos del derecho de familia;

c) A los actos personalísimos en general;

d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

Las disposiciones de causa de muerte: en sí hace referencia a las disposiciones de última voluntad, siendo el ejemplo más invocado, el testamento. Al ser actos de

carácter estrictamente personalísimos, la ley no da lugar a la utilización de la firma digital como formato de suscripción de los mismos.

A los actos jurídicos del derecho de familia: hace referencia principalmente a ciertos actos, también de carácter personalísimos, como pueden ser la celebración de un matrimonio, la adopción, el reconocimiento de un hijo, etc. Es muy importante aclarar que este artículo no se refiere al aspecto procesal jurídico aplicado a las derivaciones de las consecuencias legales que produzcan dichos actos. Por ende, al día de la fecha, la firma digital y las notificaciones y presentaciones electrónicas son utilizadas de manera habitual en todos los procesos de familia de la Provincia de Buenos Aires como del Poder Judicial de la Nación.

A los actos personalísimos en general: ampliando el marco generalizado de los incisos anteriores, podemos mencionar actos tales como la donación de órganos, disposición de cadáver, etc. No pudiendo aplicarse en estos casos la utilización de la firma digital, conforme la voluntad del legislador al redactar la presente norma.

A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes: por último, hace mención a aquellos actos que queden excluidos de aplicación de la firma digital ya sea por consecuencia de disposiciones legales posteriores o por la libre voluntad contractual entre las partes.

En este punto remarcamos que el DNU N° 27/2018 derogó el art. 4 de la LFD, en el que se enumeraban las exclusiones a la aplicación de la misma. Las disposiciones que mencionamos y todos los actos que debían ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes actualmente han sido readecuados para la implementación a través de medios digitales.

Dicho lo anterior, la LFD excluía de su aplicación a los actos mencionados arriba, situación que no sucedía en la mayoría de las legislaciones como por ejemplo las de Europa y las de Latinoamérica. Tampoco figura esta exclusión en la Ley Modelo

sobre Firmas Electrónicas de UNCITRAL por lo que su derogación es un avance bastante acertado en favor de lo digital.

K. La presunción de autoría

El art. 7 de la ley 25.506 nos brinda un carácter esencial del sistema normativo argentino de firma digital, una presunción de autoría, y establece: “Se presume, salvo prueba en contrario, que toda Firma Digital pertenece al titular del certificado digital que permite la verificación de dicha firma”.

Este artículo introduce el concepto del certificado digital de donde resulta que no hay firma digital sin un certificado digital. Esta norma viene a restringir el concepto general del art. 1, que recordemos este le otorga plena eficacia jurídica a la firma electrónica y a la firma digital.

Es así que existe una presunción, que admite prueba en contrario (presunción iuris tantum), de que toda firma digital está vinculada y pertenece a la persona titular del certificado digital mediante el cual se suscribió el documento electrónico. Por ello consideramos uno de los artículos de mayor importancia en el entramado de la ley.

Esto es así dado que se origina el “principio de autoría” que surge de la redacción. Es decir que cuando un documento digital es generado y suscripto digitalmente, hay que presumir que la firma digital plasmada pertenece al titular del certificado digital por la cual se generó la misma, consagrándose de esta forma la autenticidad, integridad correspondencia, e inalterabilidad todo el acto (salvo prueba en contrario). Consecuentemente, el documento digital producirá plenos efectos jurídicos, y en caso de que se negare la autoría del mismo, será la parte que desconozca esa firma digital quien deberá probar que la misma fue adulterada o falsificada. No hay firma digital sin la correspondiente existencia necesaria de un certificado digital.

L. Presunción de integridad

Por otro lado, en LFD Argentina, encontramos la denominada presunción de integridad: “Si el resultado de un procedimiento de verificación de una Firma Digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma” (art. 8).

Como ya mencionamos, el documento digital es el instrumento donde queda plasmada la voluntad de su creador, al que se le aplica la firma digital, dotándolo del carácter de inalterabilidad y de conexidad consecuente con el titular signatario, con efecto vinculante.

En esta ley una de las características principales del documento digital es que la declaración de la voluntad recibido no haya sido modificada de manera alguna por el emisor, estableciendo así una de las presunciones más importantes privilegiando la integridad del documento firmado digitalmente que se presume válido e íntegro y aquel que impugne la validez e integridad del mismo debe probarla.

Esta presunción establece que, si a través de un proceso de verificación de una firma digital es verdadero, consecuentemente se determina que el documento digital no se ha modificado desde el momento en el cual se integró y quedó plasmada esa firma digital, salvo prueba en contrario.

Todo converge en demarcar claramente que la voluntad del signatario se ha mantenido inalterable en el recorrido que realiza el documento digital hasta llegar a su destinatario.

Todo esto mencionado nos lleva a hablar de la garantía de no repudio ya que la firma digital goza de una doble presunción *Iuris Tantum*: La firma digital argentina cuenta con presunción de autoría es decir que la firma digital pertenece al titular del certificado digital, tiene la presunción de integridad, se presume salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

V. Actualidad en materia de Firma Digital argentina

Hablaremos de la actualidad en la materia de firma digital nacional, con el dictado del Decreto de Necesidad y Urgencia N° 27/2018, que modificó la regulación de la LFD.

Entre otras cosas este decreto derogó el art. 4 de la LFD, en el que se enumeraban las exclusiones a la aplicación de dicha ley, circunstancia que no encontramos en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, y que responde a la gran recepción que tuvo el empleo de este tipo de firma.

Por otro lado, se deroga el art. 18 de la Ley, que regulaba los certificados por profesión, y los arts. 28, 35 y 36 que hacían referencia a la Comisión Asesora para la Infraestructura de firma digital y su funcionamiento.

También, el DNU modifica el art. 10 de la Ley, el cual establecía que cuando un documento digital fuera enviado en forma automática por un dispositivo programado y llevase la firma digital del remitente, se presumiría, salvo prueba en contrario, que el documento firmado provenía del remitente. El nuevo artículo 10 dispone que todo documento electrónico firmado por un certificado de aplicación se presumirá, salvo prueba en contrario, que proviene de la persona titular del certificado digital.

Otra novedad es que el Ministerio de Modernización pasa a ser la autoridad de aplicación, en lugar de la Jefatura de Gabinete de Ministros, y la Sindicatura General de la Nación fue designada como la nueva encargada de realizar las auditorías previstas por la Ley.

Por último, en su art. 128, establece que los documentos oficiales electrónicos firmados digitalmente, los expedientes electrónicos, las comunicaciones oficiales, las notificaciones electrónicas y el domicilio especial electrónico constituido en la plataforma de trámites a distancia, en los sistemas de gestión documental electrónica que utilizan los organismos públicos en procedimientos administrativos y procesos judiciales tienen para el sector público nacional idéntica eficacia y valor probatorio que sus equivalentes en soporte papel o en cualquier otro soporte que se utilice.

El Decreto N° 892/17 (publicado en el B.O el 02/11/2017) creó la Plataforma de Firma Digital Remota, que incluyó la firma digital remota como una de las firmas digitales admitidas en el Sistema de Gestión Documental Electrónica, modificando el art. 13 del Decreto N° 1063/16.

La plataforma de Firma Digital Remota incorporó la posibilidad de firmar vía software sin necesidad de hardware. Se le llama también firma en la nube, o firma digital *cloud*, permitiendo esta última al firmante acceder desde cualquier ordenador o dispositivo móvil.

Este novedoso método incorporado por el decreto 892/17 en el cual todas las personas pueden tener su firma digital de manera remota, limita los riesgos a nivel de seguridad, porque requiere credenciales para poder utilizarse y elimina la dependencia de un dispositivo electrónico.

El 11 de enero de 2018, se publicó en el B.O el Decreto 27/2018, con el objetivo de desregular, desburocratizar y simplificar los trámites en el Estado. En los considerandos del Decreto, se estableció la necesidad de la incorporación de nuevas plataformas tecnológicas que faciliten la vinculación y las transformaciones entre los distintos organismos del Estado, y principalmente con los ciudadanos.

Bajo tal premisa, el Capítulo XI del Decreto amplió el alcance de la Ley 25.506 de Firma Digital Argentina a los fines de extender el uso del documento electrónico, la firma electrónica y la firma digital a la totalidad de los actos jurídicos y administrativos, actualizando su contenido en función de los avances tecnológicos y la experiencia de implementación de la Infraestructura de Firma Digital de la República Argentina.

El Ministerio de Modernización pasó a ser la autoridad de aplicación de la LFD, en lugar de la Jefatura de Gabinete de Ministros, y la Sindicatura General de la Nación fue designada a realizar las auditorías previstas por la Ley. Previamente recaía en universidades y organismos científicos y/o tecnológicos nacionales o provinciales, o los colegios y consejos profesionales que acrediten experiencia profesional acorde en la materia.

Por último, el art. 128 del Decreto, estableció que los documentos oficiales electrónicos firmados digitalmente, los expedientes electrónicos, las

comunicaciones oficiales, notificaciones electrónicas y el domicilio electrónico constituido en la plataforma TAD y en los sistemas de gestión documental electrónica que utilizan los organismos públicos, tienen para el sector público nacional la misma eficacia y valor probatorio que en papel.

A su vez, otra actualización importante sucede el 12 de marzo de 2019, cuando se publicó en el B.O el Decreto Nº 182/2019 que reglamenta la LFD.

De acuerdo a lo expuesto por este último Decreto resulta necesario llevar adelante una adecuación de la reglamentación de la LFD y su modificatoria Ley Nº 27.446 (Ley de Simplificación y Desburocratización de la Administración Pública Nacional) actualizando su contenido en función a los nuevos avances tecnológicos y la experiencia previa en la implementación de la Infraestructura de firma digital.

En función de lo que exponemos, el Decreto regula determinados aspectos vinculados al empleo del documento electrónico, de la firma electrónica y de la firma digital y su eficacia jurídica en el marco de la Infraestructura de la Ley de Firma Digital.

En particular, el decreto regula los poderes para la actuación ante organismos públicos. Así, se dispone que cuando una norma requiera la formalidad de escritura pública para otorgar poderes generales o particulares, para diligenciar actuaciones, interponer recursos administrativos, realizar trámites, formular peticiones o solicitar inscripciones, dicho requisito se considera satisfecho mediante el apoderamiento realizado por el interesado en la plataforma de TAD del sistema de Gestión Documental Electrónica [GDE], salvo disposición legal en contrario.

Este punto generó preocupación entre los notarios argentinos quienes entendieron que el art. 4 del Decreto y el art. 2 de su anexo, equipara la firma digital a la firma ológrafa certificada ante notario, y que ello según su punto de vista resulta incompatible con lo dispuesto por la propia LFD y por el CCyCN.

A tal extremo se agraviaron los escribanos que interpusieron una medida cautelar sobre los preceptos del Decreto mencionado, que equipararía los efectos de la firma digital a los de la firma ológrafa certificada por escribano público. La medida cautelar fue presentada ante el Juzgado Civil y Comercial Federal 5, Incidente Nº 1, y que tuvo como actor al Colegio de Escribanos de la Ciudad de

Buenos Aires y como demandado al Estado nacional Jefatura de Gabinete de Ministros.

El Decreto indica que la firma digital de un documento electrónico satisface el requisito de certificación de firma establecido para la firma ológrafa, tal como lo dispone el art. 2 del Decreto. Por ello los escribanos dicen que se equiparaba la firma digital con la firma certificada ante un escribano público, lo cual resulta incompatible, según ellos, con lo dispuesto por la LFD y supone una modificación por vía reglamentaria y por lo tanto se presenta la inconstitucionalidad, ya que va más allá del art. 314 del CCyCN, indicando que mientras la norma legal dispone para un determinado antecedente jurídico (firma digital) una consecuencia concreta de presunción de autenticidad e integridad, salvo prueba en contrario, el Decreto reglamentario prevé para ese mismo antecedente jurídico una consecuencia distinta a la equiparación con la firma certificada por escribano y, por lo tanto, la eliminación de la posibilidad de prueba en contrario.

En resumen, los escribanos argumentan que mientras que la firma digital da sólo una presunción de autoría equiparable a la firma ológrafa, la certificación de firmas por parte de un notario representa otro procedimiento de verificación de identidad, en donde interviene una persona a la que el Estado delega la fe pública el notario- que da real certeza de autoría a quien firma un documento. Y por ello los notarios afirman que el Decreto del Poder Ejecutivo es inconstitucional, pues va más allá de lo que el CCyCN y la LFD dicen, otorgándole a la firma digital efectos distintos a los que la ley y el código le otorgan.

Por ello, se solicitó el dictado de una medida cautelar, 4451/2019 Incidente Nº 1-Actor: Colegio de Escribanos de la Ciudad de Buenos Aires-Demandado: Estado Nacional Jefatura de Gabinete de Ministros s/Incidente de medida cautelar, la cual suspendió los efectos de dichas disposiciones, con el objeto de evitar que por vía reglamentaria se otorgue plena fe y carácter de instrumento público a un mecanismo informático al cual el legislador dotó de presunción *Iuris Tantun* que, según ellos, consideran está lejos de poder brindar una seguridad similar a la firma certificada por escribano.

En consecuencia, el gobierno nacional modificó el Decreto 182/19 reglamentario de la LFD y resolvió circunscribir en forma expresa al ámbito de su interoperabilidad administrativa a través del Decreto 774/2019, sustituyendo el art. 2 del anexo del Decreto 182/19.

El nuevo texto del Decreto 182 (2019) dispone: “La firma digital de un documento electrónico satisface el requisito de certificación de firma establecido para la firma ológrafa en todo trámite efectuado por el interesado ante la Administración Pública Nacional, centralizada y descentralizada” (art. 2).

Sostenemos que para que un sistema se considere digno de confianza digital es necesario el mantenimiento en el tiempo de la integridad de los documentos que remitimos digitalmente, como así también inalterabilidad e invulnerabilidad de estos instrumentos donde se encuentra la voluntad que queda plasmada por el titular del certificado digital, impidiendo que sea modificado o alterado por un tercero. Esta es una de las principales características de la firma digital, y la modificación entendible y efectuada en el art. 2 del Decreto 182/19 no ayuda en nada todos los previos pasos que venían siendo llevados a cabo positivamente en la materia, pero que tampoco son un impedimento para que más adelante sean concretados debidamente.

Un documento digital una vez que es firmado se torna inalterable. No puede ser modificado por terceros bajo ningún punto de vista gracias al enorme grado de encriptación mediante el cual se encuentra revestido dando las mismas características o tal vez mejores que las otorgadas a la firma ológrafa, certificar como se dispone en el art. 2 es el paso evolutivo ineludible en cuanto a firma digital, por lo cual solo se puede retrasar, pero no evitarse tal como sucede por ejemplo en otros países.

La firma digital debe proteger la inalterabilidad del documento digital con lo cual es asegurada la identidad de quien la firma y la autenticidad del documento digital, y sería imposible que el firmante niegue o repudie el documento digital. En otras palabras, está introduciendo el concepto del no repudio que requieren otras incontables legislaciones internacionales en materia de firma digital.

Del análisis concluimos que para los escribanos la LFD en ninguna de sus disposiciones permite sostener que la firma digital quede equiparada a una firma debidamente autenticada o certificada notarialmente y que, conforme dicha norma, todo documento firmado digitalmente queda equiparado a un instrumento privado firmado de modo ológrafo o manuscrito y que ello no puede ser asimilado al instrumento privado firmado ante notario, quien auténtica la signatura y mucho menos, equipararse a un instrumento público.

Por lo que, para ser justos, decimos que la LFD no establece en sus disposiciones la posibilidad de sostener que la firma digital quede equiparada a una firma debidamente autenticada o certificada notarialmente, situación que es más que posible y más que práctica.

Pero lo único seguro es que este parate evolutivo solo servirá para reforzar el empuje que va a lograr la firma digital en nuestro país en la materia cuando se arbitren las vías correctas para implementar (tal como se pensó originalmente) el art. 2 del anexo del Decreto 182/19.

A. Reglamentación de la Firma Digital en Argentina, Decreto Nº 182/2019

En este punto trataremos el reglamento, que se publicó el 12 de marzo del año 2019 en el B.O mediante el Decreto 182/2019 que ya pudimos ver. Vale decir que por los motivos que expusimos más arriba, la misma necesitó una aclaración expresa a través del Decreto Nº 774/2019 publicado el 19 de noviembre del 2019 en el B.O.

Tal como ya tratamos el tema de confianza digital, el mismo se encuentra mencionado en el considerando como punto principal, al igual que la LFD.

El Decreto Reglamentario 182/2019 se expide de manera inmejorable sobre el tema

> Que la creación de un clima de confianza en el entorno digital es esencial para el desarrollo económico y social, por lo que resulta conveniente reforzar la confianza en las transacciones electrónicas en nuestro país, para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y la Administración Pública e incrementar, en consecuencia, la economía digital,

> la prestación de servicios en línea públicos y privados y el comercio electrónico (considerando).

De acuerdo a lo expuesto, decimos que resultó necesario llevar adelante una adecuación de la reglamentación de la Ley Nº 25.506, con casi dos décadas de andar y su modificatoria, la Ley Nº 27.446 (Ley de Simplificación y Desburocratización de la Administración Pública Nacional), actualiza así su contenido en función a los nuevos avances tecnológicos y la experiencia previa en la implementación de la Infraestructura de Firma Digital Argentina.

Con anterioridad el Decreto 283/03 autorizó con carácter transitorio y hasta tanto no estuviese implementada la Infraestructura de Firma Digital, a la entonces Oficina Nacional de Tecnologías Informáticas dependiente de la ex Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros a proveer certificados digitales en el ámbito de la Administración Pública Nacional.

B. Aspectos principales del Decreto Nº 182/2019

Trataremos un poco más los principales artículos del decreto que nos permitirá vislumbrar el desenvolvimiento del ecosistema digital actual en nuestro país.

Comenzaremos con uno de los principales puntos del decreto, el art. 2, dónde se va a tratar la certificación de firmas y los poderes para actuación ante organismos públicos, por el cual se dispone que cuando una norma requiera la formalidad de escritura pública para otorgar poderes generales o particulares, para diligenciar actuaciones, interponer recursos administrativos, realizar trámites, formular peticiones o solicitar inscripciones, dicho requisito se considera satisfecho mediante el apoderamiento realizado por el interesado en la plataforma de TAD del sistema GDE, salvo disposición legal en contrario. Este tema se trató en profundidad en el punto anterior y debió ser modificado en su texto original a través del Decreto 774/2019.

Por su parte el art 4. del decreto va a establecer la composición de la Infraestructura de firma digital y la integración de esta suerte de escalafón digital.

En ese orden de ideas tenemos al art. 5 donde se establece la Autoridad Certificante Raíz. Este organismo es la autoridad certificante administrada por la Secretaría de Gobierno de Modernización y la Secretaría de Modernización Administrativa (dependiente de la primera). Reviste la mayor jerarquía de la Infraestructura de Firma Digital establecida por la Ley 25.506, sus modificatorias y es la encargada de emitir los certificados digitales.

El Ente Licenciante conformado por la Secretaría de Gobierno de Modernización, los certificadores licenciados, las autoridades de sello de tiempo, los suscriptores de los certificados, los terceros usuarios, los certificadores reconocidos por la Autoridad de Aplicación, el Organismo Auditante, y los prestadores de servicios de confianza.

La Autoridad Certificante Raíz es la autoridad certificante administrada la cual constituye la única instalación de su tipo y reviste la mayor jerarquía de la infraestructura de firma digital establecida por la Ley 25.506 y sus modificatorias. Emite certificados digitales a las Autoridades Certificantes de los certificadores licenciados, una vez aprobados los requisitos de licenciamiento.

Por su parte el art. 7 establece el llamado Informe de auditoría. El informe de auditoría es el que evaluará los sistemas utilizados por el certificador de acuerdo con los requerimientos de la LFD Argentina y su modificatoria, el presente Decreto y las normas complementarias. El Organismo Auditante, previa consulta con el Ente Licenciante, determinará los objetivos de control.

El art. 8 que establece el “Deber de confidencialidad”, por el cual las entidades que componen la Infraestructura de firma digital están obligadas a mantener la confidencialidad sobre la información que no sea pública. Dicha obligación subsistirá aun cuando se hayan desvinculado de la entidad o la entidad deje de ser parte de la Infraestructura de Firma Digital Argentina.

El art. 16 del reglamento va a tratar el tema del reconocimiento de certificados extranjeros. Por el cual se faculta a la Secretaría de Gobierno de Modernización para suscribir acuerdos de reciprocidad con países extranjeros a los efectos de lograr el reconocimiento de certificados de firma digital emitidos en otros países.

Por su parte el art. 17 establece la llamada “Política Única de Certificación”. Por la cual la Secretaría de Gobierno de Modernización establece la Política Única de Certificación de acuerdo a los estándares nacionales e internacionales vigentes, la que será de cumplimiento obligatorio para todos los certificadores licenciados. Dicha política deberá contener determinada información para que pueda ser considerada firma digital.

El art. 21 por su parte, va a establecer cuáles son las obligaciones del Certificador licenciado. En este artículo se establece que el certificador licenciado deberá cumplir con todas las obligaciones estipuladas por el Decreto, adicionales a las establecidas por la LFD y modificatoria.

Con respecto de los servicios de terceros, se establecen los recaudos que deberán cumplir los certificadores licenciados en caso de que requieran o utilicen los servicios de infraestructura tecnológica prestados por un tercero. En particular, se dispone que deberán prever dentro su Plan de Contingencia los procedimientos a seguir en caso de interrupción de los servicios, de modo tal que permitan continuar la prestación de los servicios sin perjuicio para los suscriptores.

Con respecto a la Autoridad de Aplicación y Ente Licenciante, se fijan las funciones de la Secretaría de Gobierno de Modernización y la Secretaría de Modernización Administrativa en su calidad de Autoridad de Aplicación y Ente Licenciante, respectivamente.

Por su parte el art. 27 del Decreto establece quiénes serán las Autoridades de Registro. En éste se establecen las funciones, responsabilidades y roles que deberán cumplir. Se estipula que los certificadores licenciados podrán delegar en las Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas.

Por último, tenemos el art. 36 del Decreto, donde se trata a los prestadores de Servicios de Confianza. El Decreto define que debe entenderse por Servicio de Confianza al establecer que se refiere al servicio electrónico prestado por un tercero de confianza. El decreto establece que los Prestadores de Servicios de Confianza podrán brindar servicios de confianza ya sea a personas humanas, jurídicas,

consorcios, entes públicos, entes públicos no estatales, de acuerdo a los procedimientos que determine a estos efectos la Secretaría de Modernización Administrativa.

Por lo tanto, conforme al Decreto reglamentario 182 del 2019 la Infraestructura de Firma Digital Argentina quedaría compuesta por:

1. La Autoridad Certificante Raíz de la República Argentina.
2. El Ente Licenciante está conformado por la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros y la Secretaría de Modernización Administrativa dependiente de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros.
3. Los certificadores licenciados, incluyendo sus autoridades certificantes y sus autoridades de registro, según los servicios que presten.
4. Las autoridades de sello de tiempo.
5. Los suscriptores de los certificados.
6. Los terceros usuarios.
7. Los certificadores reconocidos por la Autoridad de Aplicación.
8. El Organismo Auditante del art. 34 de la Ley 25.506 y su modificatoria.
9. y por último los prestadores de servicios de confianza.

VI. Firma digital en el Código Civil y Comercial de la Nación

A. Incorporación de nuevas tecnologías a la normativa de fondo

El CCyCN, reformado por la Ley 26.994, en su art. 288, establece todo lo que respecta al concepto de firma en general y firma digital en particular conjuntamente con su entramado normativo en el derecho positivo argentino recientemente sancionado, podemos establecer que la misma hace las veces de requisito esencial para la configuración de cualquier acto jurídico, especialmente cuando hablamos de instrumento privado.

“Este criterio resulta anacrónico, en atención a la realidad de la irrupción de la informática en las relaciones comerciales” (Altmark y Molina Quiroga, 2012, p. 531).

El Código Civil de Vélez establecía que: “La firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos” (art. 1012).

En las transacciones que cotidianamente se llevan a cabo, las firmas en el sentido clásico de las ológrafas ya se encuentran ausentes. Por ello consideramos que el requisito esencial de la firma de las partes establecido antigua e históricamente en el código civil para la existencia de todo acto bajo forma privada se volvió incorrecto.

Vélez Sarsfield, sostenía en la nota al art. 3639, que “la firma no es la simple escritura que una persona hace de su nombre o apellido; es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad. Regularmente la firma lleva el apellido de la familia; pero esto no es de rigor si el hábito constante de la persona no era firmar de esta manera”. Y en la primera nota al art. 916, Vélez Sarsfield con cita de Friedrich Karl Von Savigny decía que “la firma establece que el acto expresa el pensamiento y la voluntad del que lo firma”.

La vital importancia de este elemento, radica en que una vez plasmada la firma digital en un documento, deja en manifiesto la expresión de voluntad del firmante, en lo que respecta al contenido del mismo procurando su adhesión. La firma digital se encuentra firmemente unida al objetivo que el acto jurídico pretende producir.

El CCyCN procura un concepto más completo de firma que su antecesor (por razones obvias dado que al momento de la sanción de la Ley 340, no existían estos avances) al integrar las nuevas tecnologías que hoy por hoy son parte fundamental de la sociedad.

Es así que, al introducir la firma digital al relativamente nuevo CCyCN, se la equipara con el efecto propio de la firma ológrafa. Todo en consonancia con lo establecido por la Ley 25.506 que dice: “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” (art. 3).

En consecuencia, se reviste formalmente de validez jurídica a los documentos electrónicos firmados digitalmente conforme los requisitos establecidos en la Ley

25.506, siendo que de esta manera se lo equipara análogamente a un documento en formato papel suscripto ológrafamente.

En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho sólo si se utiliza firma digital, que asegure indubitablemente la autoría e integridad del instrumento. En efecto, como se ha expresado, la Ley 25.506 ya regulaba la categoría de documento digital al que define en su Artículo 6° y al que le extiende la característica de documento escrito; y lo propio respecto de la firma digital y su equivalencia a la firma ológrafa (arts. 2 y 3) y la firma electrónica en el art. 5.

En el nuevo CCyCN, el documento electrónico aparece ahora en el art. 286, y la firma digital en el art. 288, sobre el que más adelante nos detendremos a analizar. Respecto del documento digital o electrónico, el Código se manifiesta en sentido muy similar a la LFD argentina.

> Expresión escrita. La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados; excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos (art. 286).

Pero, al momento de receptar el instituto de la firma digital, lo hace con una redacción que tendremos que analizar.

> Firma. La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento (art. 288).

Esta fórmula ha planteado un problema de interpretación que genera dos conclusiones diferentes respecto de si el Código otorgó la categoría de “firma” exclusivamente a la “firma digital” o si ello también alcanzaría a la “firma electrónica”.

Muchos especialistas en materia de Derecho informático entienden que no cabe sino interpretar del texto del artículo que el requisito de firma en un documento generado por medios electrónicos se cumple sólo si se utiliza una firma “digital” y por ende únicamente en tales casos se equiparan sus efectos a la firma ológrafa, mientras que no sucede lo propio con la firma electrónica.

Esta interpretación tiene además un sustento extra cuando lo comparamos el Anteproyecto de Unificación, el que preveía

> Firma. La firma prueba la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza un método que asegure razonablemente la autoría e inalterabilidad del instrumento (art. 288).

B. Problemas interpretativos derivados del uso de firma electrónica

Ahondando sobre los problemas existentes con respecto a la Firma Digital Nacional, con la sanción del CCyCN surgieron opiniones encontradas en la doctrina, respecto de las implicancias del mismo sobre la firma electrónica consagrada en la LFD.

Hay quienes se pronuncian en contra de la vigencia actual de la firma electrónica siendo esta una tesis restrictiva, desmereciéndola como firma y, por otro lado, hay quienes sostienen su validez y plena independencia de las disposiciones del Código Civil y Comercial siendo esta una tesis amplia y avalando su uso por completo.

Tesis restrictiva:

Quienes desmerecen a la firma electrónica como tal, son contestes en que el actual art. 288 del CCyCN, el cual reconoce como antecedente el proyecto de reforma de 1998 también mencionado up supra. Entre ambos textos, existe una diferencia sustancial, habiéndose reemplazado la referencia a un método por la alusión a una firma digital y el razonablemente por el indubitablemente. En sintonía con ello, sostienen que la firma electrónica, ya no puede ser considerada una firma y consecuentemente, aquellos documentos electrónicos que carezcan de firma digital, deben ser considerados como documentos sin firmar en los términos del art. 287 del CCyCN.

Argumentan que no parecería coherente que el legislador, al utilizar el término firma digital, haya procurado incorporar otras modalidades distintas de aquellas admitidas dentro de tal concepto y que los primeros comentaristas del flamante código (Ricardo Luis Lorenzetti, Julio César Rivera, Marisa Herrera, Gustavo Caramelo y Sebastián Picasso), en ninguno de sus comentarios hacen alusión a

que el citado art. 288 no habría modificado el criterio adoptado hasta este momento: o sea la existencia de dos sistemas aceptados (firma digital y firma electrónica).

En cuanto a cuál sería la situación actual de la firma electrónica en el ordenamiento jurídico, existen a grandes rasgos dos corrientes.

Algunos, sostienen que los artículos referidos a la firma electrónica y que se encuentran contenidos en la LFD, parecerían haber quedado elípticamente derogados, no en forma expresa. Otros prefieren hablar de complementación, no de sustitución o derogación.

Refieren que el CCyCN modificó la aplicación de la LFD, al referir que el requisito de la firma de un documento electrónico queda satisfecho sólo si se utiliza exclusivamente una firma digital, que asegure indubitablemente la autoría e integridad del instrumento, negando tal carácter a los documentos que no cuentan con ella.

Tesis amplia:

Desde un punto de vista mucho más amplio, hay quienes sostienen que lejos de ser una modificación impensada, los términos utilizados en la redacción actual del CCyCN nos permiten afirmar dos circunstancias: por un lado, que la recepción legislativa de la firma digital ha llegado ahora a la norma fundamental que rige el derecho privado de los particulares; por el otro, que al momento del empleo de la firma digital en concreto será de aplicación la legislación especial que la regula. De esta manera, al momento de analizar tanto los efectos como los requisitos de la firma digital en nuestro país, deberemos observar las disposiciones contenidas en la Ley 25.506.

También se ha dicho que la interpretación propuesta por la otra tesis, implica vaciar de contenido al marco normativo fijado por la LFD, se opone al principio de neutralidad tecnológica y al de licenciamiento voluntario. Desde un plano lingüístico, llegaron a preguntarse. Qué sentido tiene utilizar la palabra “una” precediendo a la expresión firma digital. Arribando a la conclusión que aludir a una firma digital estaría reconociendo que hay, conceptualmente hablando, más de un tipo de firma digital. Lo cual se puede completar al apreciar el agregado que el texto del artículo hace a continuación de la coma, cuanto expresa, “(…) que asegure indubitablemente la

autoría e integridad del instrumento". Si, como se afirma en la primera interpretación, no hay dudas que el Código se refiere a la firma digital prevista en los arts. 2 y 6 de la Ley 25.506, ¿qué sentido tiene sobreabundar en características, asegurar autoría e integridad, que son inherentes a la definición de firma digital según la Ley.

Otra corriente, destacó que la terminología utilizada en la norma deberá interpretarse inclusiva de cualquier procedimiento que se desarrolle en el futuro que asegure autoría e integridad del documento aun cuando sus características técnicas sean diferentes a la firma digital conocida en la actualidad.

El cambio de expresión en el art. 288 actual ha obedecido a una intención deliberada de especificar concretamente qué mecanismo electrónico puede equipararse a la firma manuscrita, inclinándose el CCyCN, por la firma digital.

Entonces sostenemos, que esa diferenciación no la encontraremos de la misma manera por ejemplo en otras legislaciones, ni mucho menos en la Ley Modelo sobre Firmas Electrónicas de la UNCITRAL, que hablan en plural de firmas electrónicas. Lo que hacen estas legislaciones es distinguir de la firma electrónica avanzada, que es aquella que además de la manifestación de la voluntad puede probar la integridad del documento electrónico.

VII. La firma digital en el Sector Público Nacional

A. La firma digital en el Sector Público Nacional

La Ley 25.506 y su modificatoria establecieron en los arts. 47 y 48, el uso obligatorio de la firma digital para las transacciones de la Administración Pública Nacional, además esta invitó a las provincias del país a adherir a la utilización de la misma. El art. 48 de la ley establecía que, en el plazo máximo de 5 años a contar desde su entrada en vigencia, los organismos del Estado Nacional deberían aplicar sistemas informáticos con firma digital con el objetivo de promover la despapelización de todos los organismos públicos nacionales.

Thill (2011) menciona

> En Argentina, en 1998 la Administración Pública Nacional introdujo la primera norma a nivel nacional, y quinta en el escenario internacional, tendiente a

> otorgar validez jurídica a la Firma Digital, de modo de facilitar los procesos de despapelizacion. En efecto, el Decreto N° 427 de abril de 1998 creó la Infraestructura de Firma Digital en el ámbito del Estado Nacional (p.13).

Pero nosotros comenzamos con el mismo año que se dictaba la LFD, mediante el dictado del Decreto Nacional 103/2001, por el cual se aprobó un nuevo Plan de Modernización para la Administración pública nacional, para las empresas y sociedades del Estado, que se denominó el *Plan de Modernización del Estado*.

Este plan de modernización planteó como objetivo principal generar un cambio de paradigma en la gestión de la Administración Pública Nacional. Es decir, superar el modelo que hasta entonces era el preponderante, con organismos autónomos, independientes, que implementaban papel, transformarlo en los modelos implementados en los países escandinavos o similar al modelo de Estonia y así lograr transformar todo el servicio público de la Nación en uno, moderno, simplificado y sobre todo electrónico.

Después de muchos años de avances tecnológicos, no así de implementación de ellos en la administración pública en nuestro país, se produjo este cambio tan deseado. La Subsecretaría de Gestión Pública dio el último paso para la instrumentación de la firma digital, el documento digital, y el expediente digital en el sector. En el año 2016 se comenzó a verificar una suerte de revolución en la administración pública, con una serie de decretos que involucran el paso de la gestión administrativa en soporte papel a la aplicación de la estrategia de gobierno electrónico.

De todos modos, al menos en un principio, la firma digital no estuvo disponible para todos sino sólo para algunos usuarios de los organismos certificadores, funcionarios, beneficiarios de la seguridad social, entidades bancarias y las mutuales.

Por todo lo que mencionamos y como consecuencia de este cambio de paradigma, empezó una nueva era en la administración pública, la del gobierno electrónico y gobierno abierto en nuestro país. El gobierno electrónico en el Sector Público nacional, tuvo y sigue teniendo su pilar y base en la implementación del sistema de GDE.

Mediante el Decreto 561/2016 se aprobó la implementación del sistema de GDE y lo define como

> Sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional. Entre sus objetivos se encuentra facilitar el acceso de los ciudadanos a la administración en forma remota, posibilitar la integración e interoperabilidad de los sistemas de información, dotar a los organismos de mayores niveles de eficiencia y accesibilidad, promover la transparencia, tender a la despapelización de la administración pública y brindar seguridad a las tramitaciones (Decretos 434/16 y 561/16).

Desde el vamos, los beneficios en nuestro país fueron, son y siguen siendo innegables, solo por dar unos ejemplos, podemos mencionar en materia de acceso a la información pública, transparencia, agilidad, economía y desburocratización en la administración pública en contraposición a los medios tradicionales de administración siempre tan criticados en la ciudadanía.

Además, por último, no podemos dejar de hacer hincapié en la presente tesis doctoral, al gobierno abierto y su incorporación en la administración pública. Tratándose este gobierno que se fundamenta en los principios de transparencia informativa, fomento, apertura a la participación ciudadana y la acción colaborativa, además de la tecnología y la innovación en el sector público. Además cuenta con una agenda y un plan que parecen tener cada vez más fuerza en nuestro país, y que desarrollaremos en el presente trabajo.

“El gobierno abierto se basa en los siguientes principios fundantes: la participación ciudadana y la colaboración, la Transparencia y rendición de cuentas, tecnología e innovación” (Ritto, 2019, p.2).

Como decimos, con la sanción de la Ley 25.506, y la consiguiente incorporación de los medios digitales, se establecía entre otras circunstancias, la implementación de la firma digital en el sector público con artículos especialmente diseñados con ese objetivo. Además, se buscaba que la administración pública hiciera uso de las Tecnologías de la Información y la Comunicación tal como se venía implementando en otros sectores, como por ejemplo en el sector privado, donde se obtenían muchísimos beneficios.

Encontramos estos fundamentos en la LFD, el cual establece lo siguiente

> Implementación: El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.
> En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156 (art. 48).

Debido a esto, entendemos que Ley 25.506 disponía que el Estado Nacional, dentro de las jurisdicciones y de todas las entidades comprendidas en la Ley 24.156: “La Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social” (art. 8).

Las empresas y sociedades del estado que abarca empresas del estado, las sociedades del estado, las sociedades anónimas con participación estatal mayoritaria, las sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde el estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.

Los entes públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones.

Por último, los fondos fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional.

Como consecuencia, se promovió el uso masivo de la firma digital de tal forma que posibilita el trámite de los expedientes por vías simultáneas, las búsquedas automáticas de información, el seguimiento y control por parte de las personas interesadas, promoviendo la progresiva desaplicación del papel en todas estas entidades nacionales.

De la misma forma, teníamos a la Ley 27.446 de Simplificación y Desburocratización de la administración Pública Nacional, donde aparece la modificación a la LFD y la interoperabilidad documental que fue clave en el avance hacia la gestación del gobierno electrónico en nuestro país.

En nuestro país el plan de gobierno electrónico comienza su camino con la sanción el 27 de abril del 2005 del Decreto Reglamentario 378/2005. En este plan se establece la estrategia, a la vez que se logran definir los principios rectores, los instrumentos, las acciones a llevar a cabo y las responsabilidades de la subsecretaría de la función pública como de todos los organismos de la administración pública nacional.

Entre los lineamientos estratégicos del Plan Nacional de Gobierno, resaltamos un mejor servicio al ciudadano unificando y facilitando el vínculo de los ciudadanos mediante el uso de las TIC, reduciendo así tiempos y costos. También se busca mejorar la gestión pública, buscando aumentar la calidad de los procedimientos y sistemas de información de cada organismo y, además, facilitar el acceso de la ciudadanía a la información pública para lograr una administración pública eficiente y transparente

En esa orden de ideas, teníamos por ejemplo a la Resolución 25/2011, que ya en esos años, previos a la implementación del sistema de GDE, por el cual se establecía que los comprobantes de gestión y ejecución presupuestaria o contable de recursos y gastos, así como otros documentos de información que requieran los órganos dependientes de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerio de Economía y Finanzas Públicas, puedan ser firmados de manera digital, de manera efectiva y en la práctica.

A manera de colofón, en el año 2016 se dicta el Decreto 434/16, estableció el Plan de Modernización del Estado, cuyo objetivo principal era lograr una administración pública simplificada y eficaz en la prestación de servicios públicos, contemplando como uno de sus ejes el desarrollo, con una mejora continua y la integración de los sistemas de gestión.

Dates y Maqueda (2018) acertadamente refieren: “… la modernización del procedimiento administrativo (y, más generalmente, de la actuación estatal) es sin

dudas un objetivo esencial para las exigencias de la sociedad contemporánea y para que el Estado regulatorio funcione lo más eficientemente posible".

Decimos que lo que produjo un cambio más revolucionario en la administración pública, comenzó con la aprobación de este Plan de Modernización nacional, y que venía desarrollándose tímidamente alcanzando su madurez con la implementación del sistema GDE, además estableciendo en el mismo que su ámbito de aplicación abarca a todas las entidades que componen el Sector Público Nacional Argentino, ya mencionado.

Es por ello, que el Decreto 434/16 incluyó el objetivo de implementar una plataforma informática o mejor dicho un portal informático de generación de documentos y expedientes electrónicos que sería utilizada por toda la administración pública nacional para facilitar la gestión documental, el acceso, la reducción de los plazos y el seguimiento de cada expediente en este caso ya casi en su totalidad digital.

En tal sentido, el Plan de Modernización del Estado, conforme al Decreto 434/2016, reconoce expresamente que

> …Plan de Modernización tiene entre sus objetivos constituir una Administración Pública al servicio del ciudadano en un marco de eficiencia, eficacia y calidad en la prestación de servicios, a partir del diseño de organizaciones flexibles orientadas a la gestión por resultados. Esto supone promover una gestión ética y transparente, articulando la acción del sector público con el sector privado y las organizaciones no gubernamentales. La modernización del Estado es un proceso continuo en el tiempo que presenta acciones concretas y específicas que buscan mejorar el funcionamiento de las organizaciones públicas (anexo único).

La implementación del sistema de GDE, se logra materializar con el Decreto 561 del 2016. Con la implementación del sistema de GDE, se logró cumplir con objetivo de modernización del estado y así finalmente cumplir con el traspaso del gobierno tradicional, hacia la implementación del gobierno electrónico que, si bien este admite muchas definiciones, alude a un gobierno a través de la utilización de las TIC para la transformación y mejora de la gestión de gobierno.

Por otro lado, a través del Decreto 1063/16 se establece la implementación de la Plataforma de TAD del sistema GDE, como vía de acceso e interoperabilidad entre la ciudadanía y los organismos del Sector Público Nacional, que actualmente creció

de manera exponencial en cuanto a su implementación con la crisis sanitaria ocasionada por el Covid 19.

En ese orden de ideas resaltamos el Decreto 1273/16, el cual logra un gran avance en materia de interoperabilidad en el sector público, por el que las entidades y jurisdicciones enumeradas en el art. 8 de la Ley 24.156, deberán intercambiar la información pública que produzcan, obtengan, obre en su poder o se encuentre bajo su control con cualquier otro organismo público que así se lo solicite, facultando a la Secretaría de Modernización Administrativa del Ministerio de Modernización a dictar los protocolos de intercambio, pautas de interoperabilidad, normas complementarias, aclaratorias, técnicas y operativas necesarias para el cumplimiento de lo dispuesto. que forma parte integrante del Decreto reglamentario.

Por último, hablaremos del Decreto 182/2019 en el Sector Público, que deroga los decretos reglamentarios vigentes hasta entonces de la ley que reglamenta, para reemplazarlo con el Anexo.

El Decreto 182/2019 establece

> Que, asimismo, la sanción de la Ley N° 25.506 otorgó un decisivo impulso para la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información pública y posibilitar la realización de trámites por Internet en forma segura. Que, en tal sentido, y siendo la materia administrativa de carácter local, la Ley N° 25.506 y su modificatoria estableció en sus artículos 47 y 48 el uso obligatorio de la firma digital para las transacciones de la Administración Pública Nacional, e invitó a las provincias a adherir en cuanto a su uso (fundamentos).

B. El Gobierno Electrónico en el Sector Público Nacional

Seguimos a Nasser y Concha (2011) cuando afirman que el gobierno electrónico es la transformación de todo el gobierno como un cambio de paradigma en la gestión gubernamental, es un concepto de gestión que fusiona la utilización intensiva de las TIC, con modalidades de gestión, planificación y administración, como nueva forma de gobierno. (p.5).

Para la *E-Government Act*, la Ley de Gobierno Electrónico de los Estados Unidos (2002), el gobierno electrónico o *E-Goverment* como se conoce en los países anglosajones, se define en la misma norma de la siguiente manera:

> … el uso por parte del Gobierno de aplicaciones basadas en Internet y otras tecnologías de la información, combinado con el proceso que implementa estas tecnologías para desarrollar el acceso y envío de información gubernamental y servicios; o llevar a cabo mejoras en las operaciones gubernamentales (p. 2902).

La Carta Iberoamericana de Gobierno Electrónico nos da una definición de gobierno electrónico bastante completa

> A los efectos de la presente Carta Iberoamericana se entienden las expresiones de “Gobierno Electrónico” y de “Administración Electrónica” como sinónimas, ambas consideradas como el uso de las tecnologías de la información y de la comunicación, en los órganos de la Administración Pública, para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y la eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y de la activa participación de los ciudadanos (p. 6).

Con estas definiciones podemos afirmar con toda seguridad que vivimos un impacto y la implementación de las TIC en todos los ámbitos, y como estas transformaron la vida de todos los ciudadanos, y por consiguiente de sus sectores públicos.

El impacto que tienen las TIC tanto para ampliar y diversificar los canales y las formas de gestión como para abrir nuevas vías de expresión en las que se generen, circulen y consuman datos e información pública relevante para la ciudadanía.

El gobierno electrónico, en tanto estrategia para administrar el Estado mediante el uso de TIC, permite mejorar la eficiencia de las respuestas gubernamentales a los ciudadanos. En este sentido, las TIC pueden ser herramientas para que los gobiernos locales sean más participativos y para que logren mayores niveles de transparencia e interacción con sus ciudadanos.

“Se ha dado entonces una primera evolución de lo que por más de una década se había venido asumiendo como gobierno electrónico, al ampliarse la manera de entender la relación entre la administración y la ciudadanía” (Naser, 2017, p.11).

Por otra parte, la Carta Iberoamericana de Gobierno Electrónico del año 2007, establece siete principios que inspiran al Gobierno Electrónico a saber:

El primero de ellos es el principio de igualdad, el que establece que de ningún modo el uso de los medios electrónicos afecte la existencia de límites o

discriminaciones para los ciudadanos que se vinculen con las administraciones públicas por medios no electrónicos. Por lo que se fomenta la eliminación de los sesgos que ocasionan la utilización de las herramientas digitales.

El segundo principio es el principio de legalidad, el cual establece que las garantías previstas en los modos tradicionales en la relación del ciudadano con el gobierno y las administraciones públicas sean las mismas en los medios electrónicos. Este principio hace referencia a la implementación de las leyes de protección de datos personales de los países que adopten los gobiernos electrónicos.

El tercer principio es el principio de conservación, por el cual las comunicaciones y los documentos electrónicos deben ser mantenidos en las mismas condiciones que por los medios tradicionales, por lo que se pregona un principio de equivalencia funcional para el gobierno electrónico y sus usos, y el gobierno analógico.

El cuarto principio es el principio de transparencia y accesibilidad, por el cual tanto la información de parte de la administración pública, como el conocimiento de los servicios por medios electrónicos sean claros para los destinatarios, decimos que este principio es una suerte de lenguaje claro en la administración pública.

El quinto principio es el de proporcionalidad, el que establece que los requisitos de seguridad sean adecuados a la naturaleza de la relación establecida con la administración.

El sexto es el principio de responsabilidad, por el cual la administración pública y el gobierno deben responder por las acciones realizadas mediante los medios electrónicos de igual forma que de los realizados por medios tradicionales.

Por último, tenemos el principio de adecuación tecnológica, que indica que las administraciones escogen las tecnologías más convenientes para satisfacer sus necesidades y las de sus administrados.

C. Gestión Documental Electrónica

Como adelantamos, a través del Decreto 561 publicado en el B.O el 6 de abril del 2016, se aprobó la implementación del sistema GDE, el sistema informático del

sector público nacional de nuestro país, a través del cual se materializa efectivamente una plataforma que sirve para gestionar los trámites de la administración pública nacional. Este sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional, y así es como lo podemos encontrar definido en la página web argentina.gob.ar.

El GDE es el reemplazo del Sistema de Comunicaciones Documentales, el cual permitía la coexistencia del papel y el digital.

El sistema GDE se trata de una plataforma de gestión de expedientes electrónicos y que debe ser utilizado para la totalidad de las actuaciones administrativas por todas las entidades y jurisdicciones enumeradas en el artículo 8° de la ley 24.156.

El 21 de abril del 2016, la Secretaría de Modernización Administrativa del Ministerio de Modernización aprobó la implementación de los módulos denominados Comunicaciones Oficiales, Generador de Documentos Electrónicos Oficiales y Expediente Electrónico, todo parte del sistema GDE.

El módulo GEDO es el que contiene y administra todas las reglas, lo cual permite generar, registrar y archivar todos los documentos oficiales electrónicos, los que sustituyen a los documentos físicos, es decir, los tradicionales en papel. Éstos son guardados en el Repositorio Único de Documentos Oficiales. Los principales beneficios de la implementación de este módulo en la gestión de la Nación radican en establecer cualquier tipo de documento de manera controlada, separar la elaboración de documentos del flujo de trabajo del proceso, es decir del trámite, en que se usa a través del flujo de trabajo propio, posibilitar la constitución de un Repositorio Único de Documentos Oficiales, aligerar la producción de documentos, en especial en los de firma conjunta, al mismo tiempo que observar instantáneamente todos los intervinientes en la creación de estos, el gobierno trabaja al día, puesto que ya no puede “suponer” con ejercer las tareas en una fecha posterior a la establecida por las normas, evitar la falsificación de firmas.

Gracias al módulo de Expediente Electrónico, se administran las reglas que guían el uso de un expediente en la Nación, aceptando asociar documentos generados por GEDO y guardados en el repositorio único.

El módulo utilizado por los agentes y funcionarios dentro de DGE, es el de Comunicaciones Oficiales. Gracias a éste se puede solucionar la creación, numeración, firma, comunicación y archivo de las Notas y Memorandos de la Nación de una manera segura, controlada, automática, con soporte y registro digital. Sus principales funciones son la creación, envío y reenvío.

El último de los cuatro módulos principales es el de Escritorio único, el cual representa el medio por el que se puede navegar por todos los módulos que conforman el sistema de GDE.

Entre otros módulos de GDE, encontramos el de Portal Firmas, el cual permite administrar la firma de los documentos oficiales generados en el módulo GEDO. También, realizar la ejecución de tareas de firma pendientes sobre las que se puede trabajar de forma individual o de forma masiva. Por otra parte, se ofrece la posibilidad de visualizar el listado de todos los documentos firmados por el usuario, con un correspondiente filtro de clasificación, que facilita la conducta.

Asimismo, se cita el módulo Locación de Obras y Servicios, que permite la caratulación, vinculación de documentos, pases y consultas de EE qué tramiten la contratación de personal bajo los regímenes de locación.

El 4 de octubre del 2016, a través del Decreto 1063, se implementó la plataforma TAD como herramienta de acceso, presentación de documentación, seguimiento de trámites y notificaciones en el Sistema de GDE.

Este permite a los ciudadanos realizar trámites ante la APN durante las 24 horas del día desde cualquier computadora o Smartphone sin tener que acudir a una oficina pública.

Entre otros módulos que componen al GDE podemos decir que se encuentra el Sistema Integrado de Archivos, el Registro Legajo Multipropósito, el cual permite cargar y actualizar los registros administrados por los diferentes organismos de la APN. El Legajo Único Electrónico, que permite la creación, guarda y archivo de todos los documentos electrónicos correspondientes a los agentes del ámbito

Público; el Gestor Único de Proveedores; el Registro integral de destinatarios, el cual permite identificar a las personas que son o serán candidatos a percibir prestaciones, beneficios, subsidios, exenciones, entre otros; los Gestos de asistencias y Transferencias, a través de los cuales se puede realizar la tramitación y pago de las prestaciones, beneficios, subsidios, entre otros.

La última gran actualización en esta materia se produce con Decreto 182, la reglamentación de la ley 25.506 y que nos debemos detener a tratar nuevamente:

En cuanto al art. 1 del Decreto es el que aprueba la reglamentación de la Ley 25.506, el cual forma parte integrante del Decreto.

El art. 2 nos va a hablar de la interoperabilidad documental. La interoperabilidad documental prevista en el art. 7 de la Ley 27.446 se instrumentará mediante el módulo Interoperabilidad del sistema GDE administrado por la Secretaría de Modernización Administrativa de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros.

El Decreto reglamentario nos habla de los poderes. Decimos que fue un tema controvertido y que se resolvió mantenerlo solo para la administración pública, y que se trata en la presente tesis doctoral. Actualmente se encuentra redactado de la siguiente manera

> Cuando una norma requiera la formalidad de escritura pública para otorgar poderes generales o particulares, para diligenciar actuaciones, interponer recursos administrativos, realizar trámites, formular peticiones o solicitar inscripciones, dicho requisito se considera satisfecho mediante el apoderamiento realizado por el interesado en la plataforma de Trámites a Distancia (TAD) del sistema de Gestión Documental Electrónica – GDE, salvo disposición legal en contrario (art. 3).

Destacamos lo interesante de este artículo que deposita su confianza en la “confianza digital” y por el cual cuando se requiera la formalidad de escritura pública para otorgar poderes generales o particulares, dicho requisito se considera satisfecho mediante el apoderamiento realizado por el interesado en la plataforma T.A.D siempre con la utilización de la firma digital para ello.

El mismo sustituye el anterior art. 13 del Decreto 1063 del 4 de octubre de 2016, por el siguiente: “Artículo 13.- Firmas digitales del Sistema de Gestión Documental

Electrónica (GDE). a) Firma digital remota. b) Firma digital con dispositivo criptográfico externo. c) Firma digital con certificado del sistema" (art. 4).

Por lo que podemos observar cómo se introduce la firma digital vía software, nube o *cloud* en nuestro ordenamiento jurídico de manera definitiva, más allá de ser el sector público.

Por último, mediante el art. 5 del decreto antes mencionado, se derogan los Decretos 2628/02, 283/03 y 724/06 y los art. 8, 9 y 10 del Decreto 561/2016 actualizando así casi en su gran mayoría de preceptos la reglamentación de la LFD.

D. Marco legal del Sistema de Gestión Documental Electrónica

Para el marco legal de este sistema electrónico, mencionamos primero a la Ley 25.506, donde se establece por primera vez el valor jurídico de la firma electrónica, digital y del documento electrónico en el año 2001.

El Decreto Reglamentario 378/2005 y en él se establece la estrategia del "Plan Nacional de Gobierno electrónico".

El Decreto 434/2016 "Plan Nacional de Modernización del Estado".

El Decreto 561/2016 por el cual se establece la utilización obligatoria del sistema de GDE como único sistema para la tramitación electrónica de todas las actuaciones y expedientes del Sector Público Nacional, la baja definitiva del sistema COMDOC y demás sistemas similares en la administración pública nacional.

El Decreto 1273/2016, "Buenas prácticas en materia de simplificación – aprobación".

La Resolución SMA 19/2018, la Aprobación del Módulo de Interoperabilidad de GDE como plataforma de intercambio seguro de la información pública de sistemas y bases de datos del SPN, designación de la SMA como administrador y aprobación de las "Pautas Técnicas de Interoperabilidad de Sistemas".

El Decreto 27/2018. Desburocratización y simplificación de gestión de diversos organismos del sector público nacional.

La Ley 27.446, Simplificación y Desburocratización de la Administración Pública Nacional. Y por último el Decreto reglamentario 182/19 y sus modificatorias.

E. El Gobierno Abierto en el Sector Público Nacional

Afirmamos en este punto de la tesis doctoral, que las herramientas brindadas por la firma digital y su implantación en el sector público nacional, sentó las bases de la gobernanza digital. Ahora bien, en consonancia con el Gobierno Electrónico, surge un movimiento que acompañó y se entrelazo con esta nueva forma de gobernanza por medios electrónicos, este es el “Gobierno Abierto”.

Decimos que el Gobierno Abierto es una forma de desarrollar políticas públicas. Este concepto surge a finales del año 1970 en Inglaterra con el objetivo principal de reclamar la apertura y la participación ciudadana frente al secretismo imperante hasta entonces.

“La consolidación del gobierno abierto en la agenda internacional es el resultado del esfuerzo sostenido de los países, desde los inicios del siglo XXI, en el ámbito del gobierno electrónico” (Naser, 2017, p.10).

Veinte años después se continuó utilizando el término *open government* [gobierno abierto], entendiendo el mismo como el acceso libre a la información, protección de datos y al conocimiento de las actividades que realizaba el gobierno a través del sector público.

Por su parte el Centro Latinoamericano de Administración para el Desarrollo (CLAD) ha sumado a sus cartas precedentes la Carta Iberoamericana del Gobierno Abierto (CIGA) en la que afirma que el gobierno abierto lleva en su base un cambio cultural, una forma de gobierno por, para y con la ciudadanía.

En el capítulo Primero, Objetivos de la CLAD (2015), esta nos trae el concepto de gobierno abierto

> … se entenderá el gobierno abierto como el conjunto de mecanismos y estrategias que contribuye a la gobernanza pública y al buen gobierno, basado en los pilares de la transparencia, participación ciudadana, rendición de cuentas, colaboración e innovación, centrando e incluyendo a la ciudadanía en el proceso de toma de decisiones, así como en la formulación e implementación de políticas públicas, para fortalecer la democracia, la legitimidad de la acción pública y el bienestar colectivo (p.5.).

Por otra parte, tenemos a la Organización para la Cooperación y el Desarrollo Económico, una organización que agrupa a 35 países, entre los que se encuentran los más importantes centros económicos y financieros, como Estados Unidos, Reino Unido y la U.E. Ésta ha apoyado iniciativas para que los países, tanto miembros o no, adhieran, adopten e implementen estrategias e iniciativas de gobierno abierto. Nuestro país participa de la Organización para la Cooperación y el Desarrollo Económico, adhiriéndose a múltiples declaraciones y convenciones de la Organización, así como participando de órganos oficiales y el Centro del Desarrollo de organización.

Ahora bien, nuestra LFD, sentó las bases para poder desarrollar y materializar este tipo de proyectos dentro del gobierno nacional argentino. Decimos, que cuando hablamos de un gobierno abierto y de un gobierno electrónico como el que vimos, presumimos que se tratan de definiciones que se relacionan, pero no necesariamente un tipo de gobierno con el otro.

El gobierno abierto en nuestro país se encuentra desarrollado dentro del gobierno electrónico y por consiguiente en el empleo del ecosistema de firma digital argentina.

Actualmente a nivel internacional existe la llamada Alianza de Gobierno Abierto, una iniciativa multilateral que busca asegurar compromisos concretos de los gobiernos para avanzar en la promoción de esta forma de gobierno.

En nuestro país, siguiendo ese camino, contamos con la Dirección Nacional de Gobierno Abierto, la cual se encuentra trabajando en coordinar el desarrollo de los planes de acción nacionales de gobierno abierto presentados ante la Alianza para el Gobierno Abierto.

La Alianza para el Gobierno Abierto es una iniciativa multilateral que busca asegurar compromisos concretos de los gobiernos para promover la transparencia, luchar contra la corrupción y mejorar los servicios públicos. Argentina forma parte de OGP desde el año 2012. Desde entonces ha desarrollado cuatro planes de acción, resultado de procesos de creación conjunta junto a la sociedad civil. El enlace oficial o Punto de Contacto ante OGP se ubica en la Dirección Nacional de

Gobierno Abierto de la Subsecretaría de Gobierno Abierto y País Digital (Secretaría de Innovación Pública, Jefatura de Gabinete de Ministros).

Este ente promueve la participación ciudadana digital a través de la Plataforma de Consulta Pública, impulsa la colaboración mediante la Mesa Nacional de Gobierno Abierto y motiva conversaciones con la sociedad civil para generar políticas de transparencia dentro del Estado Nacional.

Nuestro país se encuentra comprometido a llevar adelante iniciativas que ponen en valor la transparencia, la participación ciudadana y la rendición de cuentas a través del plan de Acción de Gobierno Abierto. Estas acciones o compromisos de gobierno abierto son liderados por instituciones públicas, resultan de un proceso de participación junto a la ciudadanía y organizaciones de la sociedad civil, y se integran en Planes de Acción bianuales.

Durante el periodo de implementación de cada plan, las instituciones responsables de los compromisos reportan públicamente los avances y acciones desarrolladas, y esa información es relevada por el Mecanismo de Revisión Independiente de la OGP, encargado de la evaluación final.

El Primer Plan de Acción Nacional de Gobierno Abierto contó con 19 compromisos para el bienio (2013-2015).

El Segundo Plan (2015-2017) incluyó seis compromisos y estableció que se presenten otros de medio término en julio de 2016 (es decir, de un año de ejecución). Luego del trabajo con la sociedad civil, la Argentina incorporó nueve compromisos, sumando un total de 15 a cumplirse a julio de 2017.

El Tercer Plan de Acción Nacional de Gobierno Abierto (2017-2019) incluyó 44 compromisos adoptados por instituciones de los poderes Ejecutivo, Legislativo y Judicial, órganos de control externo y garantes de derechos, y gobiernos provinciales. Durante la implementación de este plan, los y las responsables de los compromisos reportaron sus avances en tableros de seguimiento públicos.

Actualmente nos encontramos en el Cuarto Plan de Acción de Gobierno Abierto (2019-2022). El mismo está conformado por 18 compromisos que buscan desarrollar políticas transformadoras para solucionar problemáticas concretas de agenda pública. Los compromisos son resultado de un proceso de creación conjunta

entre el gobierno y la sociedad civil, los cuales son implementados por instituciones nacionales en un plazo de 3 años, con prórrogas producto de la pandemia ocasionada por el Covid 19.

La Mesa Nacional de Gobierno Abierto se formalizó a partir de la Resolución 132/2018, que crea como instancia de coordinación de trabajo entre el gobierno y la sociedad civil para articular esfuerzos en la promoción de políticas de gobierno abierto, y además aprueba su reglamento interno de funcionamiento. El espacio respeta una conformación equilibrada de sectores: cuatro miembros de gobierno y cuatro de sociedad civil. En representación del Gobierno nacional participan la Subsecretaría de Gobierno Abierto y País Digital (Secretaría Innovación Pública, Jefatura de Gabinete de Ministros), la Secretaría de Asuntos Políticos (Ministerio del Interior), la Oficina Anticorrupción y la Agencia de Acceso a la Información Pública. Por otro lado, en representación de la sociedad civil participan en la Mesa Nacional: Acción Colectiva, Democracia en Red, Fundación Huésped y Fundación para el Desarrollo de Políticas Sustentables. La selección de estas organizaciones está a cargo de la Red de Organizaciones de la Sociedad Civil para un Estado Abierto en Argentina.

Tratamos así, el nacimiento de un nuevo ecosistema digital en la administración pública y un gran promotor de esta tesitura ha sido el sistema G.D.E que supuso también una revolución dentro de la administración pública nacional.

Concluimos en este punto, que notamos un cambio profundo en las conductas entre los organismos del sector público con los ciudadanos, por la implementación de las herramientas digitales, que modificaron la formas de relacionarse entre el gobierno y los ciudadanos para siempre.

VIII. Conclusión

Destacamos la acertada labor del legislador argentino que adoptó de manera relativamente temprana, el empleo de la firma digital y de los documentos electrónicos en la vida de los argentinos. También consideramos acertados los

últimos avances legislativos que incorporan novedades muy prácticas para las transacciones comerciales, diferentes procesos judiciales y administrativos del país.

El avance tecnológico de las nuevas tecnologías, la introducción del formato electrónico a la vida diaria, al derecho y la gran cantidad de hechos que realizamos a diario, máxime cuando los abogados argentinos que actualmente casi en su totalidad de las provincias se encuentran en transición o algunos en pleno auge, de procesos judiciales digitalizados. Todo ello nos obliga a replantearnos el concepto de firma que tradicionalmente conocimos y a comenzar a construir sus nuevos horizontes. El CCyCN con su última reforma, dio un paso de suma trascendencia al brindarnos un nuevo concepto de firma, mucho más actual y contemporáneo que el que preveía el CCN de Vélez Sarsfield.

A lo largo del capítulo referente a la implementación de la firma digital en el sector público nacional observamos los distintos avances logrados por el gobierno nacional de la mano de la Ley 25.506 y de cómo esta supuso una suerte de revolución en el sector. La administración pública, no ha sido ajena al cambio de paradigma que vive la sociedad argentina, y el mundo en materia digital. Ante este cambio de paradigma tan notorio, los modelos y conceptos de gobierno electrónico y de gobierno abierto, nacen con la misión de obtener mejores prácticas y procedimientos administrativos para ofrecer al gobierno alternativas de solución frente a los retos que se presentan actualmente en nuestro país.

No debemos olvidar el ecosistema creado por la LFD, el cual demostró su grandísimo acierto y su gran importancia durante la cuarentena y la pandemia ocasionada por el Covid 19. La implementación del mismo y de sus consiguientes herramientas digitales, permitieron trabajar de manera remota, y así proteger la salud e incluso a salvar la vida a incontables personas.

Si miramos por ejemplo los procesos de la justicia nacional, provinciales, así como también en la justicia bonaerense la regla general son los medios digitales y la excepción es el papel.

Le podremos reclamar a la legislación nacional la necesidad de avanzar sobre temas como el sello electrónico, sellos electrónicos del tiempo, o diferentes servicios de confianza que promueven la confianza digital en todas las transacciones

electrónicas inclusive tecnologías como las cadenas de bloque tan en boga en la actualidad.

Concluimos, que nuestra LFD gracias a su concepción, a sus características y su implementación, puede ser parte de un proyecto conjunto en el MERCOSUR, que promueva comercio electrónico transfronterizo del bloque y armonice de manera más profunda las herramientas digitales, promoviendo así el mercado digital.

Capítulo IV

La firma electrónica en el MERCOSUR

I. Introducción

Destacamos la gran importancia del presente capítulo, el cual nos permitirá conocer la legislación en el MERCOSUR, de los países que integran este bloque regional y de sus estados asociados. A través del análisis, identificaremos los elementos fundamentales en materia de firma digital en proceso de integración regional.

Proponemos también un repaso de la legislación de la organización del organismo, para que entendamos de mejor manera los objetivos fundacionales del MERCOSUR y de cómo este es un terreno fértil para la siembra de un mercado digital, y de la promoción de las transacciones por medios digitales.

Previo a adentrarnos en el análisis de los países, conoceremos los acuerdos en materia de firma electrónica Mercosureña. Acuerdos que decimos, que realizamos sobre la marcha de la presente tesis, no solo promoviendo la firma digital a nivel regional, sino que también fortaleciendo empíricamente que la pregunta de la tesis, termina siendo más que válida.

Por último, analizaremos las legislaciones en materia de firma electrónica y digital de los países que integran el MERCOSUR, así como también de los Estados asociados, circunstancia que nos permitirá determinar el grado de armonización existente, así como también la posibilidad de en caso de existir este último, avanzaremos en una mayor adopción de medidas en favor de armonizar dichos Acuerdos o Decisiones emanadas por el organismo.

II. El MERCOSUR

Establecemos que MERCOSUR, se constituye a partir de la firma del Tratado de Asunción, tratándose de la norma fundacional de ente supranacional. Podemos visualizar esto en su artículo 1º, como un proceso de "naturaleza intergubernamental", el cual va a estar compuesto por la República Argentina; la República Federativa del Brasil, la República del Paraguay, y la República Oriental del Uruguay.

El Mercado Común del Sur, en castellano, *Mercado Comum do Sul,* en portugués, y *Ñemby Ñemuha,* en guaraní, se trata de un proceso integrado tal como mencionamos inicialmente por los países de Argentina, Brasil, Paraguay y Uruguay.

El 26 de marzo de 1991, se firmó y se constituyó el Tratado de Asunción, donde se adoptó la denominación, su tratado fundacional y se establecieron sus principales lineamientos. Además, en esta norma se le dio una estructura institucional básica y estableció un área de libre comercio. Con posterioridad, en junio de 1992 se estableció el cronograma definitivo hacia la constitución del mercado común, el cual al día de la fecha sigue obteniendo grandes resultados.

En función del Tratado de Asunción, se encuentra abierta la adhesión de otros Estados latinoamericanos que deseen integrarse al grupo, como, por ejemplo, la República Bolivariana de Venezuela, país que se constituyó en el primer estado latinoamericano en adherir al tratado constitutivo en el año 2006. Señalamos que Venezuela se encuentra suspendida en el bloque desde el año 2016, y el motivo manifestado por miembros integrantes fue que Venezuela había violado la Carta Democrática de acuerdo al Protocolo de Ushuaia sobre Compromiso Democrático en el MERCOSUR, suscripto el 24 de julio de 1998, conforme a su situación política interna.

Por otro lado, tenemos el Protocolo de Adhesión de Bolivia al MERCOSUR, el cual ya fue firmado por la totalidad de los estados partes en el año 2015 y ahora se encuentra en vías de incorporación por los estados parte.

El estatus de “estado asociado” se establece por Acuerdos de Complementación Económica, firmados entre el MERCOSUR y cada país asociado. En tales acuerdos se establece un cronograma para la creación de una zona de libre comercio entre los países integrantes, la gradual reducción de las tarifas arancelarias entre el MERCOSUR y los países firmantes.

Sostenemos que del Tratado de Asunción y del Protocolo de Ouro Preto, no surge la figura de los “estados asociados”. Más bien, se trata de una creación posterior en el tiempo vinculada a la suscripción de Acuerdos de Alcance Parcial por parte de terceros países integrantes de la Asociación Latinoamericana de Integración [ALADI] con el MERCOSUR, y a partir de ello surge la regulación de su participación en las reuniones del MERCOSUR y en los acuerdos que se pudiesen celebrar en los ámbitos de negociación de este.

La República de Chile estableció su asociación al MERCOSUR el 25 de junio de 1996 durante la X Reunión de Cumbre del Mercosur celebrada en la Provincia de San Luis, Argentina, a través de la suscripción del Acuerdo de Complementación Económica Mercosur-Chile.

Por su parte Colombia, Ecuador y Venezuela formalizaron su asociación al MERCOSUR el 2004 mediante la suscripción del Acuerdo de Complementación Económica Mercosur-Colombia, Ecuador y Venezuela.

Afirmamos que el MERCOSUR tuvo desde sus orígenes como objetivo principal propiciar un espacio común que generará oportunidades comerciales y de inversiones a través de la integración competitiva de las economías nacionales al mercado internacional de sus países integrantes. Como resultado se fueron estableciendo múltiples acuerdos con países o grupos de países. Si esto lo trasladamos a la actualidad, se traduce en transacciones electrónicas entre los estados asociados, y con el mundo.

Señalamos que, si bien existe un creciente interés, en las herramientas digitales y las nuevas tecnologías por parte de gobiernos de los países participantes de este organismo supranacional, afirmamos que este todavía tiene mucho camino por recorrer. En razón de ello se nos presenta una oportunidad para desarrollar mecanismos de apoyo a los gobiernos interesados en optimizar y avanzar en la

implementación de estas herramientas digitales de manera regional, tales como los que veremos más adelante, siendo este la creación de un marco legal en cuanto a las firmas electrónicas o digitales tal como lo mencionamos en el presente trabajo.

Los países integrantes del MERCOSUR participan en actividades y reuniones del bloque y cuentan con preferencias comerciales con los Estados Partes. También acuerdos de tipo comercial, político o de cooperación con una diversa cantidad de naciones y organismos del resto del mundo.

Es por ello que desde el vamos, el Tratado de Asunción para la Constitución de un Mercado Común en su último párrafo establece lo siguiente: “El compromiso de los Estados partes de armonizar sus legislaciones en las áreas pertinentes, para fortalecer el proceso de integración” (art. 1).

Opinamos, por lo tanto, que este objetivo primordial y fundacional del MERCOSUR coincide con la armonización que proponemos en la presente tesis.

A. Objetivos

Como lo mencionamos con anterioridad, en el Tratado de Asunción para la Constitución de un Mercado Común, los Estados partes decidieron constituir este organismo, el cual debía estar conformado al 31 de diciembre de 1994.

B. El MERCOSUR en la actualidad

Señalamos que el MERCOSUR en la actualidad, al igual que el resto del mundo entero, se encuentra atravesando una crisis sanitaria sin igual. Ante el panorama económico, social y sanitario sombrío provocado por el Covid 19, se hace más que necesario continuar trabajando para actualizar y fortalecer la mejor vía e implementación de herramientas, sobre todo las digitales, para enfrentar la situación de manera regional y de manera mundial.

La pandemia ocasionada por el Covid 19 ha hecho que los países integrantes del bloque regional se aislaran dentro de sus fronteras, pero gracias a las TIC y las nuevas herramientas digitales decimos que existe un futuro diferente. Por la realidad

regional y los inmensos desafíos que abrirá el escenario post Covid 19 establecemos que a través de las herramientas digitales se podrá aprovechar la integración que ofrece un bloque como el MERCOSUR, adaptarlo a los nuevos tiempos y cambiar cualquier tipo de pronóstico con la utilización de legislaciones en materia de firma digital, documentos digitales y la infraestructura aplicada por cada país. Esa modernización deberá tener como ejes centrales los objetivos pensados en la constitución de este gran mercado único pero aplicados al ecosistema digital de los países integrantes, el cual llamaremos tal como se hizo en la U.E, un Mercado Único Digital.

C. Organización del MERCOSUR

Decimos que el MERCOSUR es un proceso de integración de carácter intergubernamental, donde cada Estado parte tiene un voto, y las decisiones deben ser tomadas por consenso y con la presencia de todos los Estados parte.

Este organismo toma sus decisiones a través de tres órganos:

a. el Consejo del Mercado Común, órgano superior del MERCOSUR, el cual conduce políticamente el proceso de integración,

b. el Grupo Mercado Común, que vela por el funcionamiento cotidiano del bloque.

c. la Comisión de Comercio, encargada de la administración de los instrumentos comunes de política comercial.

Asistiendo a dichos órganos existen más de 300 foros de negociación en las más diversas áreas, los cuales se integran por representantes de cada país miembro y promueven iniciativas para ser consideradas por los órganos decisorios.

Una vez negociadas y aprobadas las normas por los órganos decisorios del bloque, éstas son obligatorias y cuando sea necesario, deberán ser incorporadas a los ordenamientos jurídicos nacionales mediante los procedimientos previstos por la legislación de cada país.

A efectos de asegurar la vigencia simultánea de las normas del MERCOSUR en los Estados parte se ha establecido un procedimiento para la incorporación de la normativa MERCOSUR al ordenamiento jurídico de los Estados parte con

fundamento en el art. 40 del Protocolo de Ouro Preto, complementario del Tratado de Asunción.

Con el transcurrir del tiempo y a los efectos de la implementación de sus políticas regionales, el MERCOSUR ha creado en distintas ciudades diversos organismos de carácter permanente entre los que se encuentran el Fondo para la Convergencia Estructural del Mercosur, el Instituto de Políticas Públicas en Derechos Humanos (IPPDH), el Instituto Social del Mercosur, el Parlamento del Mercosur, la Secretaría del Mercosur y el Tribunal Permanente de Revisión.

En lo que respecta a nuestra temática, la firma digital, debemos hablar más del Grupo Mercado Común, que ha aprobado resoluciones que regulan sobre la eficacia jurídica del documento electrónico, la firma electrónica y firma electrónica avanzada, y sobre los acuerdos de reconocimiento mutuo en el ámbito del MERCOSUR.

El encargado de llevar a adelante el tratamiento de estos temas que tanto nos interesan es el subgrupo de trabajo Nro. 13 (SGT 13) “Comercio Electrónico”, del Grupo de Mercado Común.

Con respecto a los subgrupos de trabajos, decimos que se encuentran establecidos en la Decisión Nro. 24 del MERCOSUR (2014)

> Se denominan Subgrupos de Trabajo (SGT) los órganos creados como ámbito técnico permanente de negociación para la coordinación de políticas públicas y el desarrollo de políticas comunes de la agenda del proceso de integración, en los términos del artículo 1 del Tratado de Asunción (art. 3).

Sus tres más importantes resoluciones en cuanto a Firma electrónica y digital en el MERCOSUR fueron:

1. La Res. No. 34/06 Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito del Mercosur (MERCOSUR, 2006).

2. La Res. No. 37/06 Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del MERCOSUR (MERCOSUR, 2006).

3. La Decisión del Mercosur 11/19 denominada como “Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del Mercosur”, siendo esta

la más actual y que debe ser ratificada e incorporada por los estados parte (MERCOSUR, 2019).

Mencionamos también a la antigua Directiva Nro. 4 del MERCOSUR (2010), a través de la cual se establece que los certificados de origen y demás documentos vinculados a la certificación de origen tendrán la misma validez jurídica que los emitidos en papel, siempre que sean emitidos conforme a las legislaciones de los Estados Partes, y los organismos habilitados del ALADI.

En el art. 2 se toma como referencia las especificaciones técnicas, procedimientos y demás parámetros establecidos por la Asociación Latinoamericana de integración también conocida como ALADI.

Esta norma fue una de los primeras en aprobar las directrices para la celebración de Acuerdos de Reconocimiento Mutuo de Firmas Electrónicas avanzadas en el ámbito del MERCOSUR, donde se prevén algunas definiciones básicas, y se nombran los estándares internacionales de interoperabilidad que serán aplicados.

En cuanto al reconocimiento de certificados digitales entre los Estados Partes en el MERCOSUR, destacamos que, desde sus comienzos, el Subgrupo de Trabajo Nro. 13 "Comercio Electrónico" del Mercosur ha trabajado sobre la necesidad de llevar adelante negociaciones tendientes a lograr mecanismos que posibiliten el reconocimiento de certificados digitales entre los Estados Partes.

Consideramos que la seguridad y confianza en las comunicaciones y transacciones electrónicas resultan esenciales para facilitar el desarrollo del comercio y del gobierno electrónicos, y entendiendo que el uso de la firma digital posibilita garantizar la validez legal de dichas transacciones y documentos electrónicos, el Subgrupo de Trabajo Nro. 13 "Comercio Electrónico" el cual intercambió información sobre los marcos normativos nacionales que atañen al reconocimiento de las firmas electrónicas y de los documentos electrónicos.

Partimos de esta iniciativa, la cual inició el proceso de redacción de normativa sobre la materia. Dicho proceso dio como resultado dos proyectos de resolución, La Res. No. 34/06 de Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR que establece lo siguiente:

1. Estándares generales de interoperabilidad;

2. Criterios de seguridad física y lógica de los prestadores de servicios de Certificación;

3. Criterios de auditoría y control de los prestadores de servicios de certificación;

4. Criterios para la emisión de certificados reconocidos;

Recomendación para la verificación segura de la firma electrónica avanzada y otras características;

Y el segundo resultado, la Resolución número 37/06 que trata acerca del reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada, y donde constan:

1. Principios;

2. Definiciones;

3. Efectos legales de los documentos electrónicos y las firmas electrónicas y Firma electrónica avanzada y su reconocimiento mutuo;

4. Certificados digitales reconocidas;

5. Prestación de Servicios de Certificación;

6. Responsabilidades;

7. Protección de Datos Personales;

Estos proyectos de resolución fueron consensuados en junio de 2006, pasaron por consultas internas en los estados partes y han sido aprobados por el Grupo Mercado Común.

Si bien con definiciones diferentes, los conjuntos de normas analizadas tienden a: 1. otorgar y reconocer eficacia y valor jurídico a la firma electrónica, a mensajes de datos y a toda información inteligible en formato electrónico;

2. reconocer la eficacia probatoria de todo tipo de información en forma de mensaje de datos;

3. brindar validez a los documentos. Una vez creado un mecanismo para la certificación de la firma, a la validez de la misma corresponderá la validez del documento electrónico entero.

4. introducir el concepto de firma electrónica avanzada, como aquella certificada por una prestadora acreditada, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control (MERCOSUR, 2006).

Los países que utilizan firma electrónica presentan regulaciones basadas en infraestructura de claves públicas. Esto significa que el usuario de un sistema genera un par de claves consistentes en una pública y otra privada, utilizando criptografía asimétrica.

D. Acuerdos en materia de Firma electrónica en el MERCOSUR

La labor del MERCOSUR en materia de firma electrónica y firma digital fue más que fecunda, la cual cuenta con las siguientes decisiones:

MERCOSUR N° 34/06: Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR.

MERCOSUR N° 37/06: Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del MERCOSUR.

La República Argentina y la República de Chile suscribieron el Acuerdo de reconocimiento mutuo de certificados de firma digital (2017) aprobado por la Resolución Nº 436/18.

Más adelante se firmaria el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del MERCOSUR (2019), nacido y gestado dentro de las principales iniciativas del GAD y su agenda propia.

Como gran novedad en nuestra temática tenemos el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital (2021) entre los gobiernos de la República Argentina y la República Oriental del Uruguay, el cual fue ratificado en agosto del pasado año por ambos países.

Observamos, la digitalización y su consiguiente necesidad de establecer la manifestación de la voluntad a través de la firma digital es una realidad para ciudadanos, empresas y para los gobiernos integrantes del MERCOSUR. Cada vez

son más los servicios y negocios que se hacen por Internet, más aún post pandemia Covid 19.

El acuerdo de reconocimiento mutuo de firmas digitales en el ámbito del MERCOSUR posibilitará el intercambio de documentos electrónicos entre gobiernos, empresas y ciudadanos de los países del bloque.

La digitalización en las relaciones comerciales y sociales entre entes públicos, empresas y ciudadanos de los países integrantes del bloque pasa a ser una realidad. El trámite de documentos y transacciones electrónicas en este escenario amplía la frontera digital.

El acuerdo posibilita:

a. Intercambio de documentos fiscales y aduaneros;

b. Firma de contratos entre empresas establecidas en los diferentes países del bloque;

b. Trazabilidad de productos de libre comercio;

c. Reconocimiento automático de documentos electrónicos, producidos a partir de certificados digitales, en el ámbito de las infraestructuras oficiales de cada país.

El intercambio de documentos electrónicos emitidos por órganos públicos de los países asociados facilitará la vida de ciudadanos en la comprobación de diversas situaciones rutinarias, como de certificados laborales, constancias, diplomas, entre otros, todos en formato digital. Los documentos podrán ser validados siempre que sean firmados mediante certificado digital proveído por una infraestructura acreditada en cualquiera de los países miembros.

En la práctica, decimos que las personas que se encuentran en un país integrante del MERCOSUR podrán usar el certificado digital emitido por una infraestructura acreditada en su país de origen para firmar contratos y otros documentos, siendo estos reconocidos sin impedimentos. Los documentos firmados con el certificado digital emitido por cualquier infraestructura acreditada por los países del bloque se presumen verdaderos con relación al signatario, garantizando eficacia jurídica según las leyes nacionales.

Para el comercio en el MERCOSUR, los negocios serán facilitados, incluso para validar propuestas y presupuestos comerciales y firmar contratos con empresas de

los países vecinos. La preocupación en saber con quién se está tratando deja de existir porque la autenticidad y la integridad de transacciones y documentos está garantizada con eficacia probatoria y jurídica, siempre que los mensajes y documentos estén firmados mediante certificado digital reconocido por los países.

Por último, tenemos el Acuerdo sobre comercio electrónico del 28 de enero del 2021, la Decisión del Mercosur 15/2021. Este Acuerdo sobre Comercio Electrónico cuenta con disposiciones que van a versar sobre la autenticación electrónica, firmas electrónicas avanzadas o firmas digitales, protección de datos personales y transferencia transfronteriza de información por medios electrónicos. Más adelante, específicamente en el próximo capítulo, desarrollaremos esta norma.

III. Grupo Agenda Digital del MERCOSUR. Acuerdo de Reconocimiento mutuo de los certificados de firma digital y Acuerdo sobre comercio electrónico del MERCOSUR

El Consejo del MERCOSUR estableció el GAD del MERCOSUR a través de la Decisión 27/2017 del Mercosur con el objetivo de “promover el desarrollo de un MERCOSUR Digital”, a través del “Plan de Acción, de plazo bienal, con propuestas de políticas e iniciativas comunes, así como plazos y metas”.

La Decisión del Mercosur 27/2017, establece

> Que resulta indispensable promover el desarrollo de un mercado digital regional libre y seguro, promoviendo el acceso de los ciudadanos y de las empresas al comercio por medio del fortalecimiento de la infraestructura de conectividad digital; del incremento de la confianza en las redes y en el intercambio de información; así como por el establecimiento de mecanismos efectivos de cooperación intergubernamental (considerando).

La Decisión también determinó que el GAD, presentará el plan de acción en el transcurso del primer semestre de 2018. En ese semestre, el GAD terminó presentando su primer plan de acción, con compromisos en materia de Infraestructura digital y conectividad, seguridad y confianza en el ambiente digital, economía digital, habilidades digitales, gobierno digital, gobierno abierto e innovación pública, aspectos técnicos y regulatorios, y coordinación en foros internacionales.

Hasta el establecimiento del GAD, el MERCOSUR no contaba con una agenda que coordinase los temas relativos a la economía digital de la manera que se venía haciendo en la Unión Europea. La firma electrónica, infraestructura de conectividad digital, la ciberseguridad, eran conducidos por foros independientes y sin una coordinación entre sí. La creación del GAD permitió al MERCOSUR coordinar la elaboración de agenda digital, con prioridades, metas y plazos en áreas prioritarias identificadas conjuntamente.

Señalamos que, del GAD, de la Agenda Digital y de sus iniciativas, nace el Acuerdo de reconocimiento mutuo de firmas digitales en el MERCOSUR y el último Acuerdo de comercio electrónico del MERCOSUR que veremos en breve.

A. Decisión N° 11/19 del Consejo Mercado Común: Reconocimiento mutuo de los certificados de firma digital

Dentro de la agenda del GAD del MERCOSUR se encontraba la iniciativa de reconocimiento mutuo de firmas digitales entre los estados parte del bloque, circunstancia que se termina de materializar con el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del MERCOSUR, el cual se estableció a través de Decisión del MERCOSUR 11/2019 del 4 de diciembre del 2019.

Este importante acuerdo en nuestra materia en el marco del MERCOSUR fue firmado por la Argentina, Brasil, Paraguay y Uruguay debiendo ser ratificado por cada uno de los países, circunstancia que todavía no fue concretada, pero es importante remarcar que una vez hecho esto, no necesita ser incorporada al ordenamiento jurídico de cada Estado parte.

De esta manera, dentro del MERCOSUR se podrá intercambiar documentos fiscales o aduaneros y reconocer la firma de contratos entre empresas establecidas en alguno de los Estados Parte, y de los documentos electrónicos producidos a partir de certificados digitales emitidos por prestadores de servicios de certificación acreditados o certificadores licenciados. Asimismo, se da un salto en materia de trazabilidad de los bienes intercambiados, pero también abarca al reconocimiento particular de los certificados de firma digital, garantizando la validez jurídica de los

mismos. También, los certificados de firma digital emitidos en un Estado tendrán la misma validez jurídica en otro, siempre que sean emitidos por un prestador de servicios de certificación.

En la Argentina, el nexo interinstitucional designado por el acuerdo es la autoridad de aplicación de la Ley 25.506, es decir, la Jefatura de Gabinete de Ministros.

La entrada en vigor del acuerdo será a los 30 días de la ratificación por parte del país del MERCOSUR que así lo haga.

A modo de ejemplo, el diploma académico digital del Brasil, si es firmado con un certificado digital de ese país, a partir del acuerdo de reconocimiento de firmas digitales, puede ser reconocido de forma electrónica en cualquiera de los países del MERCOSUR, facilitando así las relaciones transfronterizas de reconocimiento de títulos oficiales de las personas integrantes del bloque.

B. Aspectos principales del Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del Mercosur

En sintonía con el Acuerdo 11/19 del MERCOSUR y sus considerandos, decimos que es de innegable valor el mismo ya que “las operaciones internacionales usan métodos de comunicación, almacenamiento e identificación de la información sustitutivo de los que utilizan papel”.

Coincidimos con el acuerdo, en cuanto a que la utilidad de las nuevas tecnologías de Identificación personal, conocida como firma digital, permiten garantizar la autoría e integridad, situación establecida unánimemente en el MERCOSUR.

Además, en línea con estas ideas, el Acuerdo 11/19, establece lo siguiente: “RECONOCIENDO que, debido a la asimetría de los marcos jurídicos nacionales sobre la materia, es necesario suscribir acuerdos con estándares internacionales a fin de promover un entendimiento de las estructuras legales y técnicas de las partes en la materia (…)” (anexo).

Esta norma dentro de sus considerandos incluidos del Acuerdo 11/19, Anexo, se menciona que

> … el presente ACUERDO constituye un instrumento de utilidad en la promoción de una legislación uniforme para utilizar técnicas de identificación

> y desarrollar el uso de firmas digitales que sea aceptable para las partes. Esto contribuirá a promover relaciones armoniosas a nivel internacional …(anexo).

Nos encontramos frente a un tema crucial en la materia, la ya mencionada confianza digital, y como el desarrollo de las relaciones entre los ciudadanos, los Estados parte y de éstos entre sí, dependen de medidas que garanticen la seguridad y la confianza en el ecosistema digital. Hacemos énfasis en la confianza digital, y de cómo la firma digital tendrá en miras el fomento de la confianza en las firmas digitales de todo el MERCOSUR, siempre con los efectos jurídicos de la equivalencia funcional de las firmas ológrafas de antaño.

Además, el Considerando del Anexo del Acuerdo establece que este texto contribuirá a promover relaciones armoniosas a nivel internacional, teniendo en cuenta la necesidad de que el derecho aplicable a los métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel sea homogéneo, así como los medios de identificación de las personas en entornos informáticos.

En la Decisión 11/19, se establece que

> … 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 … (art. 1).

Los certificados digitales de firma digital en terceros Estados, que tuvieran validez en el territorio de cualquiera de las Partes, quedarán excluidos.

Por su parte la Decisión nos trae definiciones valiosas tal como

> 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 (art. 2).

El artículo tercero trata el tema de la validez de los certificados digitales estableciendo que tendrán la misma validez jurídica que si son emitidos en cualquiera de los estados parte, siempre que sean emitidos con los siguientes requisitos:

Que respondan a estándares reconocidos internacionalmente, conforme lo establezca la autoridad designada y que contengan, como mínimo, datos que permitan Identificar inequívocamente a su titular y al prestador de servicios de certificación que lo emitió, indicando su período de vigencia, ser susceptible de verificación respecto de su estado de revocación, detallar la información verificada incluida en el certificado digital, contemplar las informaciones necesarias para la verificación de la firma, e identificar la política de certificación bajo la cual fue emitido.

Por último, 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 artículo cuarto establece la evaluación y armonización de las prácticas de certificación referidas al ambiente operativo de los prestadores de servicios de certificación acreditados y por su parte el artículo quinto lo hace con la acreditación y control donde los estados parte se comprometen a asegurar la existencia de un sistema de acreditación y control de los prestadores de servicios de certificación.

El artículo sexto acertadamente, nos habla de la protección de datos personales, estableciendo que se garantizará que los prestadores de servicios de certificación acreditados deberán tratar los datos personales de conformidad con la legislación de datos personales de la parte en que hayan obtenido su licencia o acreditación. Por ejemplo, para nuestro país, se garantizará que el certificado digital, se encuentre dentro de los parámetros de la Ley Nacional de Protección de Datos Personales, la Ley Nacional 25.326.

El artículo séptimo del acuerdo establece como obligación para los estados publicar en los respectivos sitios web de las autoridades, las cadenas de confianza de los certificados de firma digital de otra parte, y/o los certificados de los prestadores de servicios de certificación.

El artículo octavo por su parte, va a establecer que las autoridades para actuar conforme al acuerdo son de los cuatros países que integran el país, siendo estos por parte de Argentina: la autoridad de aplicación de la Ley 25.506; de Brasil: el Instituto Nacional de Tecnología de la Información; del Paraguay: el Ministerio de

Industria y Comercio; y por parte del Uruguay: la Unidad de Certificación Electrónica y la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

Por su parte el artículo décimo primero, va a tratar el tema de las controversias que surjan sobre la interpretación, la aplicación, o el incumplimiento de las disposiciones contenidas en el Acuerdo entre los Estados Partes del MERCOSUR, se resolverán por el sistema de solución de controversias vigente en el mismo. Surjan por la interpretación, aplicación, o incumplimiento de las disposiciones contenidas en el presente Acuerdo entre uno o más Estados Partes del MERCOSUR y uno o más Estados Asociados que adhieran al presente Acuerdo se resolverán por negociaciones directas.

Por último, tenemos al decimosegundo, que establece cuando entra en vigencia el acuerdo, y será a partir de treinta días después del depósito del instrumento de ratificación por el segundo Estado Parte del MERCOSUR. En cuanto a los Estados Partes que lo ratifique con posterioridad, el presente Acuerdo entrará en vigor de la misma manera y de la misma forma.

Los Estados Asociados podrán adherir al Acuerdo después de su entrada en vigor para todos los Estados Partes, en conformidad con lo estipulado en el párrafo 1 del presente artículo.

C. Decisión N° 15/2021 Consejo Mercado Común. Acuerdo sobre comercio electrónico del MERCOSUR

Nuevamente dentro de la GAD del MERCOSUR nace una nueva iniciativa del MERCOSUR Digital, un proyecto conjunto para el desarrollo del comercio electrónico transfronterizo del bloque del MERCOSUR. El mismo va de la mano con el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del MERCOSUR.

El 28 de enero del 2021, se plasma la Decisión N° 15/2021, un nuevo acuerdo sobre Comercio Electrónico del MERCOSUR, el cual va a tratar la autenticación electrónica, las firmas electrónicas avanzadas o firmas digitales, la protección de

datos personales y la transferencia transfronteriza de información. Además, aclaramos que este Acuerdo sobre Comercio Electrónico se realizó a través del procedimiento de excepción previsto por la Mercosur/CMC Dec. N° 02/20 en razón de la pandemia ocasionada por el Covid 19.

En los considerandos de la decisión, tal como mencionamos, se establece que este Acuerdo es un complemento del Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del MERCOSUR y a otras normas relativas a la materia, surgida como iniciativa de la Agenda Digital del MERCOSUR del GAD, que consideró necesario la creación de un instrumento común que represente la importancia que los estados partes asignan al comercio electrónico.

Encontramos esto plasmado en el tercer párrafo del considerando: “Que es conveniente contar con un marco jurídico que consagre las normas y principios relativos al comercio electrónico en el MERCOSUR, con el objetivo de aprovechar el potencial económico y las oportunidades proporcionadas por el comercio electrónico”.

Este acuerdo va a consagrar una serie de normas y los principios relativos al comercio electrónico en el ámbito del MERCOSUR, con la finalidad de aprovechar el potencial de los canales digitales como instrumentos de desarrollo económico y social.

El acuerdo cuenta con 17 artículos, que tratan definiciones, ámbitos de aplicación y disposiciones generales, derechos aduaneros, autenticación y firmas electrónicas avanzadas o firmas digitales, protección al consumidor en línea, protección de los datos personales, transferencia transfronteriza de información por medios electrónicos, y demás artículos, que conforman una pieza fundamental para el desarrollo del comercio electrónico del bloque regional.

Para comenzar podemos señalar que el primero de los artículos nos trae una serie de definiciones estableciendo las siguientes:

Comercio electrónico: significa la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos.

Autenticación electrónica: significa el proceso o acción de verificar la identidad de una parte en una comunicación o transacción electrónica y de asegurar la integridad de una comunicación electrónica;

Comunicaciones comerciales directas no solicitadas: significa un mensaje electrónico que se envía con fines comerciales o publicitarios a la dirección electrónica de una persona sin el consentimiento del destinatario o contra el rechazo explícito del destinatario;

Firma electrónica: significa datos en forma electrónica anexos a, o lógicamente asociados con, un documento electrónico o mensaje, que pueden ser utilizados para identificar al firmante en relación con el documento electrónico o mensaje y que indican la aprobación por parte del firmante de la información contenida en el documento electrónico o en el mensaje;

Firma electrónica avanzada o firma digital: significa 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 de 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, y que, de acuerdo con las reglamentaciones locales, provee el mismo status legal que una firma escrita a mano.

Opinamos que de manera similar al Reglamento eIDAS de la U.E, pero de manera diferente, se comienza a armonizar en materia de firma digital y comercio electrónico en el MERCOSUR. Un claro ejemplo de esto es el de establecer una definición de conceptos en materia de firma electrónica, en un marco legal transnacional, en donde cada país podría contar con sus propias visiones en la materia.

El art. 2 del acuerdo nos da el ámbito de aplicación y disposiciones generales y el art. 3 habla acerca de derechos aduaneros.

Sin embargo, hacemos hincapié en el art. 4 de la Decisión en el cual tenemos la Autenticación y firmas electrónicas avanzadas o firmas digitales que establece que “Una Parte no negará la validez legal de una firma únicamente sobre la base de que

ésta sea realizada por medios electrónicos, salvo disposición expresa en contrario prevista en su respectivo ordenamiento jurídico".

Se establece por lo tanto como regla que no negarán la validez legal de las firmas únicamente con fundamento en su carácter electrónico (salvo disposición expresa en contrario prevista en su respectivo ordenamiento jurídico).

También se establece que no se adoptarán medidas de autenticación electrónica que prohíban a las partes de una transacción electrónica determinar mutuamente los métodos de autenticación adecuados para esa transacción o que impidan a las partes de tal transacción tener la oportunidad de probar ante las autoridades judiciales o administrativas que su transacción cumple con cualquier requerimiento legal respecto a la autenticación.

Por otro lado, se incentivará el uso interoperable de firmas electrónicas avanzadas y firmas digitales.

Por último, se establece que se arbitrará los medios necesarios para la suscripción de acuerdos de reconocimiento mutuo de firmas electrónica avanzadas y/o firmas digitales.

En el art. 5: "Protección al consumidor en línea", se establece la importancia de proteger a los consumidores de prácticas comerciales fraudulentas y engañosas cuando participan en el comercio electrónico. En ese sentido, cada parte se ajustará, en materia de protección al consumidor en el comercio electrónico.

Destacamos en este punto el art. 6 que va a tratar la Protección de los datos personales en este ámbito. Precisamente en el punto 2 de este artículo se establece que se adoptarán o mantendrán leyes, regulaciones o medidas administrativas para proteger los datos personales de los usuarios que participen en el comercio electrónico, tomando en cuenta estándares internacionales vigentes. Se fomentará la adopción de medidas de seguridad para el tratamiento de los datos personales de los usuarios e informarán a los usuarios acerca de sus derechos de acceso, rectificación y supresión.

En el punto 7 se establece que se aplicarán a los datos personales que reciban de otro Estado Parte un nivel de protección adecuado mediante leyes, regulaciones o, también, acuerdos mutuos –generales o específicos– y marcos internacionales

más amplios (admitiéndose, para el sector privado, la implementación de contratos o autorregulación).

En el punto 8 se establece que se arbitrará los medios necesarios para sentar medidas comunes para la protección de los datos personales y su libre circulación en el Mercosur.

También destacamos la importancia del art. 7, el cual legisla en materia de transferencias transfronterizas de información por medios electrónicos.

En el punto 1 del artículo se reconoce que cada Estado parte podrá implementar y/o mantener sus propios requisitos regulatorios incluso respecto a la protección de datos personales. Sin perjuicio de ello, se autorizan las transferencias transfronterizas de información cuando ellas sean necesarias para realizar la actividad comercial de una persona de un Estado Parte. Sin embargo, se aclara que los Estados Parte podrán restringir tales transferencias para alcanzar un objetivo legítimo de política pública y siempre que las restricciones no se apliquen arbitrariamente o encubra una restricción al comercio.

El Acuerdo sobre Comercio Electrónico incorpora disposiciones adicionales en relación con la protección del consumidor en línea, la ubicación de instalaciones informáticas, el acceso y el uso de Internet para el comercio electrónico, las comunicaciones comerciales directas no solicitadas, facilitación del comercio electrónico, intercambio de información con propósitos de cooperación y derechos aduaneros.

Con respecto a la Facilitación del comercio electrónico establece

> Facilitación del comercio electrónico. Las Partes reconocen la importancia de la facilitación del comercio por medios electrónicos para el desarrollo del comercio electrónico. En ese sentido, cada Parte se ajustará, en materia de facilitación del comercio electrónico, a lo establecido en las disposiciones relevantes de la normativa MERCOSUR vigente (art.11).

Destacamos la labor del GAD del MERCOSUR en favor de la armonización legislativa en materia de firma electrónica, pero sobre todo en marcar el rumbo hacia un mercado único digital tal como sucede en otras partes del mundo como por ejemplo en la U.E y que sin lugar a dudas en nuestra opinión es el camino indicado.

IV. La Firma electrónica en el MERCOSUR

Tratamos los acuerdos y decisiones del MERCOSUR como organismo y proceso de integración internacional, por lo que ahora es el tiempo de ver cada estado parte en particular.

Señalamos que la firma electrónica en el MERCOSUR avanzó de manera categórica y exponencial en los últimos tiempos, situación visible con la enorme cantidad de resoluciones y normas, que, a modo de avalancha, se produjeron en los últimos años. Ni hablar de la implementación masiva por parte de los ciudadanos del bloque del MERCOSUR de las herramientas digitales en razón de la pandemia del Covid 19.

Tal como mencionamos previamente, en los años 1996 y 2001, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), concibió un marco normativo que serviría de modelo para los países miembros y así para que estos pudieran elaborar sus respectivas legislaciones en materia de firma electrónica, todos reglados sobre las bases aportadas por las leyes modelos de ella. En primer término, la CNUDMI, realiza Ley Modelo sobre Comercio Electrónico en el año 1996 y con posterioridad Ley Modelo sobre Firmas Electrónicas en el año 2001.

La motivación principal de esta última labor fue evitar diferencias cualitativas y cuantitativas en la redacción de las leyes sobre firma electrónica, facilitando el trabajo y además facilitando la armonización al crear las normas.

La iniciativa de la CNUDMI tuvo una excelente recepción, ya que la mayoría de los países miembros adoptaron sus leyes modelos como base de su legislación sobre firma digital y comercio electrónico, actualmente vigentes en casi todos los países miembros de las Naciones Unidas y como no puede ser de otra manera, el MERCOSUR no es un caso ajeno.

El concepto de firma digital y el de firma electrónica comenzó materializarse en el cono sur, cuando los integrantes del MERCOSUR impulsaron y lograron posteriormente que se legislara al respecto en cada uno de ellos. Por ello la República del Uruguay se convirtió en el año 1998 en el primer país de América del

Sur en contar con firma digital (sin embargo, no disponía todavía de un marco específico en la materia) y en el mismo año así lo hizo Puerto Rico en Centroamérica. A partir de allí en 1999 siguió Colombia, en el 2000 México y Perú, en 2001 Argentina, Brasil, Panamá y Venezuela y así sucesivamente se incorporaron República Dominicana, Chile, Ecuador, Costa Rica, Guatemala, Paraguay, Bolivia, etc.

En la actualidad si hablamos de América Latina, de los 33 países, solo 7 no cuentan con legislación formal al respecto. Estos son Cuba, El Salvador, Guyana, Haití, Surinam, Dominica, San Cristóbal y Nieves.

En el año 2010, el Consejo del Mercado Común por Decisión 64/10, decidió impulsar la conformación progresiva de un “Estatuto de la Ciudadanía del MERCOSUR”, que compila un conjunto de derechos y beneficios en favor de los nacionales de los Estados Partes del Mercosur.

El Estatuto de ciudadanía del MERCOSUR, compila derechos y beneficios en favor de los nacionales, ciudadanos y residentes de los Estados Partes del MERCOSUR, y lo traemos debido a que se omite en este estatuto el ecosistema digital, las injerencias en materia de firma digital y sus alcances. Circunstancia que podría haber enriquecido de sobremanera este estatuto por lo que esperamos que al igual que los objetivos de esta tesis, se lleven adelante en un futuro más que cercano.

Destacamos que no regula nada acerca de la Identificación electrónica como se hace en la U.E con el Reglamento eIDAS.

A continuación, analizaremos la legislación en materia de firma digital y de firma electrónica de cada Estado miembro del MERCOSUR a excepción de la República Argentina, la cual tuvo un tratamiento especial en esta tesis.

A. República Federativa del Brasil

La firma digital en la República Federativa del Brasil se encuentra legislada a través de la Medida Provisional Nº 2.200-2/2001. Esta legislación fundacional en la

materia, crea el marco legal de la firma digital y también la infraestructura de clave pública brasileña, también conocida como ICP-Brasil.

Los Decretos Ley 3.996 de 2001 y 4.414, de 2002, que regulan la prestación del servicio de certificación digital y la firma electrónica.

El uso de la firma digital en el Brasil funciona por intermedio del uso de certificados digitales al igual que casi todas las legislaciones en la materia. En este caso en particular estos certificados digitales dependen de la infraestructura de clave pública de la ICP-Brasil.

Sin embargo, la ley también prevé la posibilidad de utilizar otros medios para acreditar la autoría e integridad de los documentos en formato electrónico, incluidos los certificados que no hayan sido emitidos por la ICP-Brasil, siempre que las partes los acepten como válidos.

En otras palabras, ICP-Brasil hace de autoridad oficial de fe pública en materia digital, que otorgará una de las técnicas disponibles para generar documentos digitales con validez legal, pero nada impide que las partes opten por otros medios de certificación.

A continuación, veremos un poco más en profundidad las disposiciones de este marco legal brasileño.

La Medida Provisional Nº 2.200-2, sancionada en Brasil, el 24 de agosto del año 2001, por el presidente de la República de Brasil, Fernando Henrique Cardoso, que permitió la posibilidad de utilizar certificados digitales y el establecimiento de la Infraestructura de Claves Públicas Brasileñas.

Comenzamos, con el art. 1 de la norma, que va a determinar los principales propósitos de esta normativa que son: garantizar la autenticidad, la integridad y validez legal de los documentos en formato electrónico, solicitudes de respaldo y aplicaciones habilitadas que utilizan certificados digitales, además de realizar transacciones en dispositivos electrónicos seguros.

Este artículo establece lo siguiente: “Se establece la Infraestructura Brasileña de Clave Pública para garantizar la autenticidad, integridad y validez legal de los documentos en formato electrónico, aplicaciones de soporte y aplicaciones

habilitadas que utilizan certificados digitales, así como transacciones electrónicas seguras" (art.1).

Por ello decimos que al igual que la LFD de Argentina, esta ley va a ser el pilar sobre el cual se asentará el ecosistema digital brasileño.

Otro artículo importante de la ley es el art. 2, el cual va a definir la composición del ICP-Brasil, como un conjunto de entidades, estándares técnicos y regulaciones, diseñadas para soportar un sistema criptográfico basado en certificados con el fin de garantizar una mayor seguridad en las transacciones electrónicas y fomentar el uso de los medios digitales para realizar negocios y actos legales, más aún en tiempos de cuarentena tal como los que vivimos actualmente.

Además, este artículo regula el Comité Directivo (CG-ICP) y una cadena de autoridades de organismos de certificación compuestos por la Autoridad de Certificación Raíz, Autoridades Certificadoras y Autoridades de Registro. Estas son estructuras jerárquicas donde la Autoridad de Certificación Raíz está en la parte superior, debajo de ella están las autoridades de certificación y en un nivel inferior a ellas las autoridades de registro de los certificados digitales de firma digital.

Como mencionamos previamente, el Comité de Gestión de ICP-Brasil (CG-ICP) es el eje de la legislación y del funcionamiento del sistema además de regular la infraestructura de claves públicas. Este va a actuar como una especie de consejo deliberativo que tiene como objetivo y es el responsable principal de coordinar la implementación y operación de ICP-Brasil, definiendo las normas técnicas que debe respetar. Además, se encarga de las resoluciones que son previamente analizadas por la Comisión Técnica Ejecutiva, que asiste y apoya el órgano deliberante.

Las resoluciones son aplicadas y ejecutadas por la Autoridad de Certificación Raíz, que es el Instituto Nacional de Tecnología de la Información, organismo federal vinculado a la Casa Civil de Presidencia de la República Federativa del Brasil.

El art. 3 de la Ley establece que la función de autoridad de gestión de políticas será ejercida por el Comité Directivo de ICP-Brasil, y que además se encuentra vinculado a la Oficina Civil de la Presidencia de República y compuesto por cinco

representantes de la sociedad civil, miembros de sectores interesados, todos designados por el presidente de la República.

De lo anterior se desprende la heterogeneidad de la composición del Comité de Dirección, que le da más legitimidad para actuar. Se pueden observar dos aspectos relevantes en este artículo, en primer lugar, la presencia de la sociedad civil en el Comité, una iniciativa loable del legislador como forma de dotar de estabilidad, transparencia y confiabilidad al sistema.

El apartado § 10 del mismo cuerpo legal es el que dispone que la coordinación del Comité de Dirección de ICP-Brasil será ejercida por el representante de la Casa Civil de la Presidencia de la República, por tanto, el control estatal sobre la cadena.

Los detalles de la estructura y competencias del Comité Directivo se encuentran en los arts. 3 y 4 de la Medida Provisional Nº 2.200-2, además del Decreto N° 6.605, del 14 de octubre de 2008.

El art. 3 por su parte proporciona la función, el enlace a la Casa Civil y la composición de la misma:

La función de autoridad de gestión de políticas será ejercida por el Comité Directivo de ICP-Brasil, vinculado a la Oficina Civil de la Presidencia de República y compuesto por cinco representantes de la sociedad civil, miembros de sectores interesados, designados por el presidente de la República. Lo dispuesto en el artículo transcrito anteriormente se repite en el art. 20 del Decreto No. 6.605 / 08.

Las competencias del CG-ICP (2001) son

> I - coordinar la implementación y operación de ICP-Brasil;
> II – establecer criterios y estándares para la acreditación y desempeño de CA, RA y otros proveedores de servicios que apoyan a ICP-Brasil;
> III - establecer las reglas operativas de la CA Raíz;
> IV - inspeccione la raíz AC;
> VII - evaluar las políticas externas del PCI, negociar y aprobar acuerdos bilaterales de certificación, acuerdos de certificación cruzada, reglas de interoperabilidad y otras formas de cooperación internacional. El CG-ICP, como se señaló, cuenta con una Comisión Técnica Ejecutiva, COTEC, para quien debe asistir y darle soporte técnico, según se especifica en los Arts. 4 y 5 del Decreto N° 6.605, además de una Secretaría Ejecutiva cuya competencia se especifica en los art. 6º y 7º del mismo decreto (MP 2.200-2 /01, art. 4).

Otras disposiciones sobre el Comité Directivo y la Comisión Técnica Ejecutiva se encuentran en el Decreto No. 6.605, en las Resoluciones del Comité Gerente de ICP-Brasil e Instrucciones Normativas y otros documentos

Cabe mencionar que la MP 2.200-2/01 en su artículo 8 prevé la posibilidad de actuar como AC y AR tanto organismos y entidades públicas como personas jurídicas privadas. En otras palabras, solo se espera que AC Raíz sea específicamente el ITI; de lo contrario, el MP 2.200-2/01 da lugar a que cualquier empresa o agencia, pública o privada, participe en la cadena, de acuerdo con los criterios establecidos por el Comité de Gestión de ICP-Brasil.

De lo anterior, podemos ver que se ha adoptado un modelo donde el gobierno brasileño a través de una autarquía federal, el Instituto Nacional de Tecnología de la Información, realiza la Función de Autoridad de Certificación Raíz, generando toda una estructura de confiabilidad a la cadena que viene por debajo del ITI.

Mencionamos el art. 10, donde se otorga la confianza en toda la cadena de certificación digital brasileña, por eso, este artículo da presunción de integridad a documentos electrónicos firmados digitalmente, es decir, a los documentos electrónicos generados mediante certificados emitidos por ICP Brasil (MP 2.200-2, 2001). Así, este artículo hizo de la firma digital un instrumento válido legalmente en Brasil. El mismo establece lo siguiente: “Los documentos públicos o privados se consideran para todos para efectos legales, los documentos electrónicos amparados por esta Medida Provisional” (art. 10).

El punto 1 de la Medida establece la equiparación de las firmas digitales a la ológrafa en tanto que

> Las declaraciones contenidas en documentos electrónicos producidos con el proceso de certificación de uso proporcionadas por ICP-Brasil presume que es cierto con respecto a los firmantes, en forma de art. 131 de la Ley 3071, 1 el de enero de 1916 - Código Civil brasileño (MP 2.200-2, 2001, § 1).

Estamos en presencia del principio de equivalencia funcional establecido en la ley modelo UNCITRAL y la mayoría de las legislaciones en la materia, al establecer el mismo valor en cuanto a documentos por medios electrónicos con los documentos en formato papel.

También de gran importancia es la disposición en el § 2 del art. 10 que nos brinda el segundo principio internacional en materia de firma digital y electrónica, el principio de neutralidad tecnológica.

> Las disposiciones de esta Medida Provisional no impedirán el uso de otros medios para probar la autoría e integridad de los documentos electrónicos, incluidos los que utilizan certificados no emitidos por ICP-Brasil, si las partes los aceptan como válidos o la persona quien se oponga al documento (MP 2.200-2, 2001, § 2).

Por lo tanto, el marco legal establece la posibilidad de la utilización de técnicas alternativas para probar autoría o de certificación digital o el uso de la propia técnica de firma digital en una cadena de certificación garantizada por ICP-Brasil pero que no han sido incluidas en ella, y estas técnicas deben ser previamente acordadas, conocidas, y aceptadas por las partes.

En el art. 12, MP 2.200-2 / 01 transforma el Instituto Nacional de Tecnología de Información (ITI) en una agencia federal vinculada al Ministerio de Ciencia y Tecnología, determinando inmediatamente, según lo dispuesto en el art. 13, que la ITI es la Autoridad Certificación raíz de la infraestructura de clave pública brasileña. Por lo tanto, la citada estructura piramidal de ICP-Brasil tiene en su apogeo el ITI, como AC Raíz.

Afirmamos que la MP 2,200-2/01 fue un hito regulatorio en el ordenamiento jurídico brasileño desde que fundó los cimientos del ICP-Brasil, con una infraestructura similar a la de sus países vecinos y un ecosistema digital que está en constante implementación al igual que en el resto de los países del MERCOSUR.

B. República del Paraguay

Por su parte, la República del Paraguay, contaba con la Ley 4.017, "De Validez Jurídica de la Firma Digital, Firma Electrónica, los Mensajes de Datos y Expedientes Electrónicos". Es la norma que regulaba el ecosistema digital guaraní, promulgada el 13 de diciembre del 2010, y reglamentada con el Decreto 7.369 del 2011. Además de ello, Paraguay aprobó y adhirió, mediante la Ley 6.055/18, a la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los

Contratos Internacionales. En el año 2012, se promulgaba la Ley 4.610, que introducía modificaciones importantes a la Ley 4.017, entre ellas, el cambio de la autoridad de aplicación de la referida norma, que de ser el Instituto de Tecnología y Normalización pasó a ser el Ministerio de Industria y Comercio.

Actualmente con la Ley Nº 6.822/2021 “De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos” se derogan todas las disposiciones de la Ley N° 4.017 “de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico”, y de la Ley N° 4610/2012 que modifica y amplía dicha ley.

La Ley 4.017 otorgaba validez jurídica a la firma electrónica y a la firma digital en el territorio paraguayo. Además, de distinguir la firma electrónica de la firma digital, confiriéndoles diferentes efectos jurídicos, reconociendo el principio de equivalencia funcional, siempre y cuando esta última haya sido certificada por un prestador de servicios habilitado por el Ministerio de Industria y Comercio de este pais.

Destacamos que la derogada Ley 4.017 facultaba a la administración pública para llevar a cabo trámites administrativos a través de medios electrónicos y a utilizar expedientes electrónicos y firmas digitales en sus actuaciones, también en línea con lo que sucedía en la República Argentina y el gran avance producido en materia de gobernanza digital en la administración pública.

Esta ley fue reglamentada por Decreto del Poder Ejecutivo Nº 7369/2011 y amplió su alcance en virtud de la Ley 4610, del 9 de mayo de 2012, que la modificó parcialmente en cuanto al ámbito de aplicación de expedientes electrónicos y la designación del Ministerio de Industria y Comercio como Autoridad de Aplicación.

A continuación, veremos los artículos más relevantes de la abrogada Ley 4.017. Comenzamos con el Título primero de la ley, en el que tenemos el objeto de la ley, las definiciones y por último los principios generales.

La Ley 4.017 nos daba varias e importantes definiciones, por ejemplo, las de

> … Firma electrónica: es el 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 … (art. 2).

Asimismo, definia a la firma digital como

> … Firma digital: es una firma electrónica certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría… (art. 2).

Lo mismo hacía con documento digital: "… Documento Digital: es un mensaje de datos que representa actos o hechos, con independencia del soporte utilizado para su creación, fijación, almacenamiento, comunicación o archivo …" (art. 2).

La norma de la República de Paraguay nos traía los principios generales que deben observarse y que encuentran su basamento en la ley UNCITRAL, así como también en Argentina y la de varios países de Latinoamérica.

> a) Neutralidad tecnológica: Ninguna de las disposiciones de la presente Ley podrá ser aplicada de forma que excluya, restrinja o prive de efectos jurídicos a cualquier otro sistema o método técnico conocido o por conocerse que reúna los requisitos establecidos en la presente Ley. b) Interoperabilidad: Las tecnologías utilizadas en la aplicación de la presente Ley se basarán en estándares internacionales. c) Interpretación funcional: Los términos técnicos y conceptos utilizados serán interpretados en base a la buena fe, de manera que no sean negados efectos jurídicos a un proceso o tecnología utilizado por otro Estado por el solo hecho de que se le atribuya una nomenclatura diferente a la prevista en la presente Ley (art. 3).

Más adelante, se establecen las obligaciones de los titulares de firmas electrónicas, e incluso responsabilidades, situación que no encontramos de manera similar en otras legislaciones.

> Actuar con diligencia razonable en la utilización de este tipo de firma; dar aviso si el titular signatario sabe que los datos de creación de la firma han quedado en entredicho o tiene conocimiento que dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado también en entredicho; actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con su período de validez o que hayan de consignarse en él sean exactas.
> El titular de este tipo de firma incurrirá en responsabilidad personal, solidaria e intransferible por el incumplimiento de los requisitos enunciados en este artículo, circunstancia que encontramos particularmente severa, pero que sin ningún lugar a dudas hace que se mantenga (art. 16).

Los arts. 17 y 18 de la derogada Ley 4.017 establecía los efectos y la validez jurídica de la firma electrónica, estableciendo en primer término y como efecto la presunción de que el mensaje de datos proviene del firmante, que este aprueba el contenido dejando así por sentado el principio de autoría. En cuanto a la validez de la firma electrónica en caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez de idéntica manera que la Ley de la República Argentina.

Por otro lado, en cuanto a la validez jurídica de la firma digital del Paraguay, el art. 20 de la norma establecía que cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Circunstancia que ya pudimos mencionar, y que es de gran relevancia porque significa el principio de equivalencia funcional consagrado en todos los países que tratamos.

El art. 21 de la norma establecía las exclusiones existentes en materia de la firma digital de ese país, que vale decir son idénticas a la redacción original de la LFD Argentina y que actualmente fue derogado en nuestro ordenamiento patrio. Se refiere a las disposiciones por causa de muerte; a los actos jurídicos del derecho de familia; a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes; y por último a los actos personalísimos en general.

A partir de la sección III y el art. 25 se van a tratar la infraestructura de la firma digital del Paraguay, los procedimientos para poder ser prestador de servicios de certificación, requisitos, obligaciones y responsabilidades de estos.

En él establece el reconocimiento de certificados digitales de firma de otros países, además estableciendo que estos podrán ser reconocidos por esta Ley

> … cuando reúnan las condiciones que establece la presente Ley y la reglamentación correspondiente y que tales certificados provengan de proveedores extranjeros que sean reconocidos o aprobados por la autoridad normativa, facultándose a ésta a reglamentar el procedimiento para este reconocimiento o aprobación (art. 36).

La ley abrogada era una de las más completas y ricas de las que encontramos en el MERCOSUR. Era la encargada de todo el andamiaje jurídico del ecosistema

de firma digital del país, una guía de conceptos y definiciones que la hacían referente en la materia.

Sin embargo, como ya mencionamos, la República del Paraguay actualmente cuenta con la destacable Ley Nº 6.822/2021 “De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos”, promulgada el 30 de diciembre de 2021 y publicada en la Gaceta Oficial N°2 el 04 de enero 2022.

Opinamos que esta norma se ha armonizado con vistas al Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de la Comunidad Europea, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas. Consideramos más que necesario tratar esta novedosa legislación, siendo la primera de su tipo en el MERCOSUR y que enriquecerá la investigación.

La Ley Nº 6.822/2021 cuenta con 105 artículos divididos en 6 títulos. El título primero de la ley contiene las “disposiciones generales”, el título segundo “los servicios de confianza”, el título tercero “documentos electrónicos”, el título cuarto “documento transmisible electrónico”, el título quinto “autoridad de aplicación'' y por último el título sexto “disposiciones finales”.

Esta norma es sin lugar a dudas la más actual y novedosa de toda Latinoamérica, donde se va a establecer

> … un marco jurídico para la identificación electrónica, firma electrónica, el sello electrónico, el sello de tiempo electrónico, el documento electrónico, el expediente electrónico, el servicio de entrega electrónica certificada, el servicio de certificado para la autenticación de sitios web, el documento transmisible electrónico y en particular para las transacciones electrónicas (art.1).

Establecemos que esta norma es pionera dentro del MERCOSUR, en tratar los “servicios de confianza” tal como se viene tratando a estos en la U.E. Es más, “incorpora la identificación electrónica” (en este caso como cédula de identidad electrónica) algo que analizamos en esta tesis.

Dentro de su articulado esta norma cuenta con los principios y definiciones (como lo haría la derogada Ley 4.017) pero en esta ocasión se incorporaron 51 definiciones, muchas de ellas nuevas y que jamás se legislaron en este país.

El art. 3 nos trae los principios que van a tener que observarse en la aplicación de la ley, la equivalencia funcional, la neutralidad tecnológica, la no discriminación contra el uso de las comunicaciones electrónicas, la libre competencia, la compatibilidad internacional y la buena fe.

En el art. 4 de la ley encontramos en muchos casos definiciones con similar técnica legislativa que la del Reglamento eIDAS.

Ya en el título segundo encontramos los “servicios de confianza”. Previamente el art. 4 definía los mismos como

> … servicio de confianza: el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios, d) servicio de expedición de medios de identificación en virtud a sistemas de identificación electrónica. (art.4).

Aquí encontramos lo novedoso de la ley, donde se incorporan los “servicios de confianza” de similar manera que en la U.E.

El art. 5 de la ley habla de los prestadores de confianza estableciendo que

> … La presente ley se aplica a los prestadores de servicios de confianza establecidos en la República del Paraguay. Se entiende que un prestador de servicios de confianza está establecido en Paraguay cuando su residencia o domicilio se halle en territorio paraguayo, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. (art.5).

Algo destacable es la incorporación del art. 7 en cuanto a los “aspectos internacionales”. En donde se establecen los requisitos para que estos sean reconocidos internacionalmente.

El art. 10 nos trae las obligaciones de los prestadores de servicios de confianza y el art. 11 la responsabilidad de los prestadores de servicios de confianza.

Dentro de este título, en la sección IV, la norma nos trae las infracciones y las sanciones que pueden recibir los prestadores de servicio que pueden ser leves, graves, y muy graves.

En la sección V encontramos los servicios de confianza cualificados que eran definidos en el art. 4 de la siguiente manera

> … Servicio de confianza cualificado: el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas cualificadas, sellos electrónicos cualificados, sellos cualificados de tiempo electrónicos, servicios cualificados de entrega electrónica certificada y certificados relativos a estos servicios, y/o b) la creación, verificación y validación de certificados cualificados para la autenticación de sitios web, y/o c) la preservación de firmas, sellos o certificados cualificados electrónicos relativos a estos servicios, d) servicio de expedición de medios de identificación en virtud a sistemas de identificación electrónica con nivel de seguridad alto. (art.5).

En los siguientes artículos se siguen viendo la supervisión, el Inicio de un servicio de confianza cualificado, las listas de confianza, los requisitos y la denominada etiqueta de confianza «PY» para servicios de confianza cualificados (de manera similar a como se ha implementado en la U.E).

La etiqueta de confianza mencionada es similar a la etiqueta de confianza del Reglamento eIDAS, y se encuentra en el art. 27 estableciendo lo siguiente

> … Etiqueta de confianza «PY» para servicios de confianza cualificados.
> 1. Una vez que la cualificación a que se refiere el artículo 25, apartado 2, párrafo segundo, se haya incluido en la lista de confianza a que se refiere el artículo 26, los prestadores cualificados de los servicios de confianza pueden usar la etiqueta de confianza «PY» para indicar de manera simple, reconocible y clara los servicios de confianza cualificados que prestan.
> 2. Al utilizar la etiqueta de confianza «PY» para los servicios de confianza cualificados a que se refiere el apartado 1, los prestadores de los servicios de confianza garantizan que en su sitio web exista un enlace a la lista de confianza pertinente.
> 3. La Autoridad de Aplicación elaborará especificaciones relativas a la forma y en particular la presentación, composición, tamaño y diseño de la etiqueta de confianza «PY» para servicios de confianza cualificados. (art.27).

En la sección VI llegamos a la “identificación electrónica” donde se establecerán los efectos jurídicos, los requisitos y los niveles de seguridad de los sistemas de identificación electrónica. La misma es definida previamente en el art. 4 como el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

Dentro de la sección VII de certificados electrónicos, encontramos la novedad incorporada en la ley, la Cédula de identidad electrónica. Para esta ley, conforme al art. 37, es el documento de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

La sección VIII trata sobre la “firma electrónica” y sus diferentes clases. Para la Ley 6.822/2021 la firma electrónica son los datos en formato electrónico anexos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

Por su parte la “firma electrónica cualificada” es una que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica. Además, tiene que estar vinculada al firmante, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados.

En la sección VIII se establecerán los efectos jurídicos, su impugnación y el empleo de la misma en la administración pública. También encontramos los requisitos para los certificados cualificados de firma electrónica, los requisitos de los dispositivos cualificados de creación de firma electrónica, la certificación de los dispositivos cualificados de creación de firmas electrónicas y los requisitos de validación de estas últimas.

La sección IX va a tratar al “sello electrónico”. Para la ley paraguaya el sello electrónico son datos en formato electrónico anexos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad. En esta sección encontraremos los efectos jurídicos, los requisitos y cómo estos pueden ser cualificados.

La sección X trata al “sello de tiempo electrónico”. Para la ley estos últimos son datos en formato electrónico que vinculan otros datos en un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante. En esta sección encontramos los efectos jurídicos, y cómo estos pueden llegar a ser cualificados.

La sección XI trata al “servicio de entrega electrónica certificada”. Para esta ley este servicio electrónico es el prestado por uno o más prestadores cualificados de servicios de confianza, que permiten asegurar con un alto nivel de fiabilidad la identificación del remitente, garantizar la identificación del destinatario antes de la entrega de los datos, estar protegidos el envío y recepción de datos por una firma electrónica o un sello electrónico de un prestador cualificado de servicios de confianza. Los arts. de esta sección establecen los efectos jurídicos y los requisitos.

La sección XII trae la “autenticación de sitios web”. Estos según el art. 60 proporcionan un medio por el que puede garantizarse a la persona que visita un sitio web que existe una entidad auténtica y legítima que respalda su existencia.

El título tercero se denomina documentos electrónicos. Previamente mencionamos la importancia de esta herramienta, circunstancia tratada por la ley en numerosos artículos.

La sección IV de este título va a regular al expediente electrónico, estableciendo su validez jurídica y su valor probatorio. Acerca de esto la ley dice que

> … 1. En todo proceso privado, judicial y administrativo podrá utilizarse el expediente electrónico con idéntica validez jurídica y valor probatorio que el expediente convencional.
> 2. En la tramitación del expediente electrónico podrá utilizarse documento electrónico, firma electrónica, sistemas de información electrónica, domicilio electrónico, siendo esta enumeración meramente enunciativa más no limitativa.
> 3. El expediente electrónico podrá ser mixto, compuesto por documentos de archivo electrónicos y tradicionales, relacionados entre sí, y conservados en parte en soporte electrónico y en parte como expediente tradicional. (art.75).

La Ley 6822/2021 terminó siendo una sorpresa y de las más interesantes de todas las legislaciones del MERCOSUR que tratamos. Después de conocer la última legislación del Paraguay, concluimos que estamos frente a una de las más completas del MERCOSUR y de toda Latinoamérica.

Además, opinamos que más allá de novedad, la técnica legislativa adoptada por el legislador, que asimila mucho del Reglamento eIDAS, la hacen una pionera en la región y un referente en la materia.

C. República Oriental del Uruguay

La República Oriental del Uruguay, cuenta con la Ley 18.600, del “Documento electrónico y Firma electrónica”, que reconoce su validez y eficacia jurídica en todo el territorio uruguayo. Esta Ley fue aprobada el 21 de septiembre del año 2009 y su Decreto Reglamentario 436/2011, el 8 de diciembre del año 2011.

La Ley mencionada es la que va a regir en materia de firma digital, firma electrónica, documentos electrónicos y toda la infraestructura de clave pública de la República Oriental Uruguay.

Existen modificaciones a la misma en las leyes 18.996 del 7 de noviembre del año 2012, arts. 41 y 423 y la ley 19.355, del 30 de diciembre del año 2015, en el art. 85 de esta última.

La Ley 18.600 establece al comenzar que

> Los servicios de certificación deberán ajustarse a lo previsto en esta ley, su actividad no estará sujeta a autorización previa y se realizará en régimen de libre competencia, sin que ello implique sustituir o modificar las normas que regulan las funciones que corresponde realizar a quienes están facultados legalmente para dar fe pública (art. 1).

Destacamos, que la ley distingue entre certificado electrónico (artículo 2 inciso B) y certificado reconocido (en el mismo artículo inciso C.5). El certificado reconocido es el expedido por el prestador de servicio de certificación acreditado ante la unidad de certificación electrónica uruguaya. Esta unidad creada por la ley es ante quien se acreditan los prestadores de servicios de certificación y es la encargada de implementar las políticas para la mejor aplicación de la normativa, entre otras tareas.

Resaltamos al prestador de servicio de certificación acreditado, porque de acuerdo con lo establecido en la ley es el único que puede expedir la firma electrónica avanzada.

Los arts. 5 y 6 establecen los efectos jurídicos de la firma electrónica y la electrónica avanzada respectivamente. Esta última es aquella a la que se le otorga según el art. 6 referido, “idéntica validez y eficacia que la firma autógrafa consignada en documento público o en documento privado con firmas certificadas siempre que esté debidamente autenticada por claves u otros procedimientos seguros”.

En el capítulo II de la ley se establece todo lo referente a la infraestructura nacional de certificación electrónica del Uruguay. En esa estructura de confianza digital, se crea la Autoridad Certificadora Raíz Nacional conforme al art. 15, siendo la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento. Luego, en esa cadena tenemos a los prestadores de servicios de certificación acreditados que veremos a continuación.

Actualmente, en Uruguay existen tres prestadores de servicios de certificación acreditados: el Correo (ente público), Abitab, empresa privada que actúa en régimen de libre competencia, y por otro lado el Ministerio del Interior, que expide el documento de identidad electrónico desde el mes de mayo de 2015. Destacamos como en la República del Paraguay, el documento electrónico cuenta con la firma electrónica avanzada del titular de la misma, aunque todavía no es obligatoria su obtención por parte de aquellos ciudadanos que tengan identificación electrónica vigente.

Opinamos que la Ley 18.600 uruguaya, es una legislación bastante interesante que contiene definiciones y características que resultan valiosas tratar.

El Ámbito de aplicación en dicha Ley se establece así: “Queda reconocida la admisibilidad, validez y eficacia jurídicas del documento electrónico y de la firma electrónica…” (art. 1).

Además, deja establecido que las disposiciones de esta Ley no alteran el derecho preexistente respecto a la celebración, perfeccionamiento, validez y eficacia de los actos y negocios jurídicos.

Por su parte el art. 2 de la Ley 18.600, realiza una serie de definiciones, que facilitan la tarea a la hora de que entendamos la legislación de este país.

A los efectos de esta ley se entenderá por

> Acreditación: estableciendo que es el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Unidad de Certificación Electrónica que cumple con esta ley de firma digital y su respectiva reglamentación.
> Certificado electrónico: tratándose este de un documento electrónico firmado electrónicamente que da fe del vínculo entre el firmante o el titular del certificado y los datos de creación de la firma electrónica.
> Certificado reconocido: Siendo este un certificado electrónico emitido por un prestador de servicios de certificación acreditado.

> Datos de creación de firma: los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.
> Datos de verificación de firma: los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.
> Dispositivo de creación de firma: siendo un componente informático que sirve para aplicar los datos de creación de firma.
> Dispositivo de verificación de firma: siendo este un componente informático que sirve para aplicar los datos de verificación de firma.
> Documento electrónico o documento digital, siendo este la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.
> Fecha electrónica: conjunto de datos en forma electrónica utilizados como medio para determinar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que está asociado.
> Firma electrónica: son los datos en forma electrónica anexos a un documento electrónico o asociados de manera lógica con el mismo, utilizados por el firmante como medio de identificación (art. 2).

Con respecto a este punto, destacamos que la ley uruguaya al contrario que la Argentina o el Brasil para referirse a la “firma digital”, utiliza la acepción “firma electrónica avanzada” tal como se hace por ejemplo en el Reglamento eIDAS u otras legislaciones.

La firma electrónica avanzada en la Ley 18.600 del Uruguay, y adquiere los efectos y las características debe cumplir con una serie de requisitos

> "Firma electrónica avanzada": la firma electrónica que cumple los siguientes requisitos: 1) Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca; 2) Ser creada por medios que el firmante pueda mantener bajo su exclusivo control; 3) Ser susceptible de verificación por terceros; 4) Estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detestable; y 5) Haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma (art. 2).

En el caso de no cumplir con estos requisitos solo será una firma electrónica.

Firmante o signatario: es la persona que utiliza bajo su exclusivo control un certificado electrónico o un certificado reconocido para efectuar operaciones de firma electrónica o firma electrónica avanzada.

Prestador de servicios de certificación: es la persona física o jurídica, pública o privada, nacional o extranjera, que expida certificados electrónicos o preste otros servicios de certificación en relación con la firma electrónica.

Prestador de servicios de certificación acreditado: siendo el prestador de servicios de certificación acreditado ante la Unidad de Certificación Electrónica.

Titular del certificado: siendo esta la persona que utiliza bajo su exclusivo control un certificado electrónico.

La Ley 18.600 por su parte establece los principios generales que rigen en materia digital

> Sin que la enumeración tenga carácter taxativo, los actos y negocios jurídicos realizados electrónicamente, las firmas electrónicas o firmas electrónicas avanzadas y la prestación de los servicios de certificación, se ajustarán a los principios generales: A) equivalencia funcional; B) neutralidad tecnológica; C) libre competencia; D) compatibilidad internacional; y E) buena fe (art. 3).

Aclaramos que todos estos conceptos los tratamos previamente, por eso solo los mencionaremos. Estos principios generales sirven como criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones de la Ley. Además, sobre este punto inferimos, que estos principios emanan de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas de año 2001 que ya tratamos.

La Ley 18.600 establece los efectos legales de los documentos electrónicos. “Los documentos electrónicos satisfacen el requerimiento de escritura y tendrán el mismo valor y efectos jurídicos que los documentos escritos, salvo las excepciones legalmente consagradas” (art. 4).

Además, establece algo importante en la materia, una sanción del tipo penal dentro del cuerpo legal, el que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento electrónico, incurrirá en los delitos previstos por los artículos 236 a 245 del código penal uruguayo.

El art. 5 va a establecer los efectos jurídicos de la firma electrónica estableciendo que la misma no cuenta con la presunción “iuris tantum”, característica de la firma avanzada.

La Ley 18.600 también va a consagrar los efectos jurídicos de la firma electrónica avanzada estableciendo que: “La firma electrónica avanzada tendrá idéntica validez y eficacia que la firma autógrafa consignada en documento público o en documento privado con firmas certificadas” (art. 6).

El documento electrónico en Uruguay, al ser suscripto con firma electrónica avanzada tendrá idéntico valor probatorio al documento público o al documento privado con firmas certificadas en soporte papel.

Además, el documento electrónico no hará fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador de servicios de certificación acreditado.

La ley al referirse al uso de la firma electrónica avanzada en la función notarial establece que: “Autorizase el uso de documentos electrónicos y firma electrónica avanzada en la función notarial, de conformidad con la reglamentación que establezca la Suprema Corte de Justicia” (art.7).

Por consiguiente, decimos que este autoriza el uso del documento electrónico y la firma electrónica avanzada en la función notarial. Interesantísimo aspecto que se incluya a los escribanos y su relación tan controvertida en este ámbito.

Por su parte la Ley 18.600 (empleo de la firma electrónica o firma electrónica avanzada en los órganos del estado) establece que

> El Estado, los Gobiernos Departamentales, los entes autónomos, los servicios descentralizados y, en general, todos los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica o firma electrónica avanzada (art. 8).

De igual manera que en nuestro país, la norma de Uruguay establece el uso de esta herramienta en el sector público, contemplando así la posibilidad del gobierno digital y todo lo que ello significa.

En cuanto al régimen de uso de la firma electrónica o firma electrónica avanzada en las profesiones de abogado, escribano y procurador, la ley establece

> La Suprema Corte de Justicia expedirá, en forma exclusiva, los certificados reconocidos para ser utilizados en el ejercicio de las profesiones de Abogado, Escribano y Procurador, si se constituye como prestador de servicios de certificación acreditado bajo las condiciones que establece esta ley (art. 10).

En caso de que la Suprema Corte de Justicia no se constituya como prestador de servicios de certificación acreditado, tendrán plena validez y eficacia para ser utilizados en el ejercicio de las profesiones de abogado, escribano y procurador, los certificados reconocidos expedidos por otro prestador de servicios de certificación

acreditado. Tal vez sea la única legislación que conocimos que menciona a los profesionales del derecho, que tanto uso dieron y les dan a estas herramientas digitales.

A partir del Capítulo II por su parte, nos habla de la infraestructura nacional de certificación electrónica de Uruguay y nos da nuevamente una definición.

> Esta es el conjunto de equipos y programas informáticos, dispositivos criptográficos, políticas, normas y procedimientos, dispuestos para la generación, almacenamiento y publicación de los certificados reconocidos, así como también para la publicación de información y consulta del estado de vigencia y validez de dichos certificados (art. 11).

Por último, veremos el art. 15 de la ley, donde se trata la Autoridad Certificadora Raíz Nacional, estableciendo que es la primera autoridad de la cadena de certificación a la cual le compete emitir, distribuir, revocar y administrar los certificados digitales de los prestadores de servicios de certificación acreditados. En su último párrafo designa a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

A través de la Ley N° 14.063, del 23 de septiembre de 2020, se va a establecer el objeto y las clasificaciones de la firma por medios electrónicos. Dispone sobre el uso de firmas electrónicas en las interacciones con las entidades públicas, en los actos de las personas jurídicas y en materia de salud, y en las licencias de software desarrolladas por las entidades públicas, y modifica la Ley N° 9.096, de 19 de septiembre de 1995, la Ley N° 5.991, de 17 de diciembre de 1973 y la Medida Provisional N° 2.200-2, de 24 de agosto de 2001.

Concluimos, que la legislación que tratamos es una de las más completas y ricas de los países integrantes del MERCOSUR. Celebramos la tarea del legislador del país, que de manera acertada cubrió casi todos los aspectos como sus países vecinos e incluso a veces fue más allá.

D. El Estado Plurinacional Bolivia

El Estado Plurinacional de Bolivia se encuentra en proceso de adhesión al MERCOSUR, aun así, pasaremos a conocer y a analizar la labor por parte de este país en la materia.

La firma digital en Bolivia fue introducida por la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación N° 164 promulgada el 08 de agosto de 2011. El art. 78 de dicha ley otorgaba por primera vez la validez jurídica y probatoria a la firma digital en Bolivia.

El Decreto Supremo No. 1793, de 13 de noviembre de 2013, por su parte aprobó el Reglamento para el Desarrollo de las Tecnologías de Información y Comunicación y delegó a la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes la elaboración de los reglamentos y procedimientos específicos que las Entidades Certificadoras deben cumplir para la prestación del servicio de certificación digital en el país.

Resolución Administrativa Regulatoria RAR ATT-DJ-RA-TL LP 1211/2014, de 11 de julio de 2014, por otro lado, aprobó los “Estándares técnicos y otros lineamientos establecidos para el funcionamiento de las entidades certificadoras”, que posteriormente se complementó y actualizó el 9 de enero de 2015 con la RAR ATT-DJ-RA-TL LP 32/2015.

El Decreto Supremo N° 1793 define firma electrónica y digital, le va a dar validez jurídica a los certificados digitales y a los documentos digitales bolivianos.

El decreto mencionado, define firma electrónica como que: “Es el 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 carece de alguno de los requisitos legales para ser considerada firma digital” (inciso d de parágrafo III del art. 3).

Decimos que Bolivia ha sido uno de los últimos países en regular la firma digital en Latinoamérica y en el Mercosur. No obstante, aunque su legislación en materia puede parecer dispersa, esta permite la implementación de la firma electrónica y digital en sus ámbitos públicos y privados.

E. República Bolivariana de Venezuela

La República Bolivariana de Venezuela se encuentra suspendida en todos los derechos y obligaciones inherentes a su condición de Estado parte del MERCOSUR, de conformidad con lo dispuesto en el segundo párrafo del art. 5 del Protocolo de Ushuaia.

El régimen legal en materia de firma digital se encuentra en el decreto con fuerza de Ley, sobre Mensajes de Datos y Firmas Electrónicas, el cual desarrolla y establece el valor y eficacia de este tipo de firmas.

La norma fue promulgada en el año 2001 y publicada en la Gaceta Oficial Nº 37.076 de fecha 13 de diciembre del 2000. Reglamento Parcial del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas publicado en la Gaceta Oficial N° 38.086 del 14 de diciembre de 2004, también lo regula la normativa impuesta por la Superintendencia de Servicios de Certificación Electrónica.

La Ley Sobre Mensajes de Datos y Firmas Electrónicas establece que: “Otorga y reconoce 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 …” (art. 2).

Por otro lado, la ley de este país al igual que todos los que vimos va a hacer la diferenciación entre firma digital y electrónica, establecer sus requisitos, así como también establecer la infraestructura venezolana en la materia.

Opinamos que Venezuela, en materia de firma digital, implementación, y puesta en práctica se encuentra rezagada a diferencia de países como Argentina, Brasil, Uruguay y Paraguay, por lo que tiene una ardua tarea por delante.

VI. Estados asociados del MERCOSUR

A continuación, con el fin de enriquecer el panorama en materia digital, decidimos incluir los estados asociados al MERCOSUR y sus legislaciones en materia de firma electrónica y digital.

A. República de Chile

La República de Chile, cuenta con la Ley 19.799 sobre “Documentos Electrónicos, Firma Electrónica y Servicios de Certificación”, la cual fue publicada el 15 de septiembre de 2003 por el Ministerio Secretaría General de la Presidencia.

Esta ley regula en Chile la firma electrónica con su correspondiente infraestructura digital. Comprende los diferentes tipos de firma electrónica, los documentos electrónicos, las características de los certificados de firma electrónica, y los derechos y obligaciones de los titulares de firma electrónica.

En cuanto a los ejes principales de esta ley, están en sintonía con el resto de las legislaciones de sus países vecinos, heredando de La Ley Modelo de Firmas Electrónicas de la UNCITRAL los principios establecidos en el art. 1 de la misma.

Además, al igual que las legislaciones de los estados parte del MERCOSUR, reconoce que los órganos del estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica simple. La norma establece en el art. 6 que los documentos, firmados mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos en soporte de papel.

En cuanto a firma electrónica, adhiere a la acepción de “firma electrónica avanzada” tal como lo hicieran varios países, en contraposición a la de firma digital para este tipo de firma.

La Ley del país trasandino define varios de los conceptos en un solo lugar, definiendo en él la firma electrónica y la firma electrónica avanzada de la siguiente manera

> f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor; g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría… (art. 2).

Nuevamente vemos los principios rectores de la Ley Modelo de firmas electrónicas en varios artículos como, por ejemplo

> Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito (art. 3).

Opinamos que estamos frente a una legislación que se encuentra a la altura de las circunstancias, una norma completa, de fecunda y longeva implementación al igual que la de sus países vecinos.

Por último, mencionamos el Acuerdo de Complementación Económica Mercosur - Chile ACE No 35. Este acuerdo constituye una nueva etapa del proceso de integración económica entre Argentina y Chile, que comenzó en 1995, y alcanzó el libre comercio en 2014 el cual complementa una serie de entendimientos vigentes, como el Acuerdo de Complementación Económica 35 MERCOSUR-Chile (ACE 35) de 1996 y el acuerdo para evitar la doble tributación de 2015 en vigencia desde octubre de 2016. Constituye, un paso importante en el objetivo de estrechar los vínculos con los países de la Alianza del Pacífico. Este acuerdo entre la República Argentina y la República de Chile aprueba un acuerdo de reconocimiento mutuo de certificados de firma digital, de la Ley 25.506 Argentina y la Ley 19.799 de Chile promoviendo de manera particular una suerte de armonización temprana entre ambos países.

B. República de Colombia

La República de Colombia dictó la Ley 527 (1999), ley que fue aprobada el 18 de agosto de 1999, donde se 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 además de dictarse otras disposiciones en materia digital.

Posteriormente Colombia a través del Decreto 19 del año 2012 reglamentó las características y requerimientos de las entidades de certificación del país.

La Ley 527 define firma digital como

> … c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación… (art. 2).

Por su parte, el Decreto 2364 de 2012 reglamenta el artículo 7° de la Ley 527, sobre la firma electrónica complementando el marco jurídico de esta ley.

En el del decreto que mencionamos, define a la firma electrónica como

> Firma electrónica. Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente (art. 1).

Con posterioridad Colombia incorpora como novedad la firma electrónica certificada que a diferencia de las anteriores en la materia es emitida por una entidad de certificación digital y solo puede emitirla esta entidad, la cual garantizará su confiabilidad y su legalidad. El proceso de creación y emisión está acreditado por el Organismo Nacional de Acreditación de Colombia. La misma se encuentra regulada mediante el Decreto 333 de 2014 (que a su vez deroga el Decreto 1747 de 2000), que establece de manera detallada los aspectos relacionados con las entidades de certificación, los certificados y las firmas digitales.

No dudamos que el ecosistema digital en la República de Colombia se encuentra un poco disperso normativamente, sin embargo, esto no le impide la eficacia jurídica a la firma digital.

C. República del Ecuador

La República de Ecuador cuenta con la "Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos” N° 2002-67, la cual se encuentra vigente desde el año 2002, con su reglamento también redactado y registrado en el mismo año siendo este uno de los pocos países que reglamentó su firma electrónica de manera temprana.

La Ley N° 2002-67 es la encargada de regular los documentos electrónicos, la firma electrónica, los servicios de certificación, la contratación electrónica y la prestación de servicios electrónicos, incluido el comercio electrónico y la protección a los usuarios del ecosistema digital ecuatoriano.

La firma electrónica avanzada, es definida en el Título II

> Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos (art. 13).

Por su parte, esta ley establece que la firma electrónica debe cumplir requisitos para su validez siendo estos los siguientes

> a) Ser individual y estar vinculada exclusivamente a su titular; b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos; c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado; d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y, e) Que la firma sea controlada por la persona a quien pertenece (art. 15).

La firma electrónica tiene igual validez y se le reconocen los mismos efectos jurídicos que a una firma ológrafa estableciendo así el principio de equivalencia funcional plasmada en las legislaciones que vimos.

Además, al igual que otros países, este país no utiliza la denominación firma digital o firma electrónica avanzada, como ocurre en otros países, para diferenciar a la firma electrónica avanzada o digital por una entidad acreditada ante la autoridad

competente de aquella firma electrónica que no cuenta con dicha certificación denominándolas a ambas como firma electrónica.

Esta ley se encuentra reglamentada por el Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el Decreto Ejecutivo 3496, publicado en el Registro Oficial Suplemento N° 577 el 17 de abril del 2002.

Concluimos brevemente que esta ley no solo regula a la firma por medios electrónicos, documentos electrónicos y su infraestructura, sino que además tiene en su articulado cuestiones que van desde el comercio electrónico hasta la protección a los usuarios.

D. República Cooperativa de Guyana

La República Cooperativa de Guyana no cuenta con legislación en materia de Firma Digital.

E. República de Perú

La República de Perú cuenta con la Ley N° 27.269, la “Ley de Firmas y Certificados Digitales” promulgada el 26 de mayo de 2000 y publicada el 17 de julio del 2000 en el boletín oficial del país, la cual regula la utilización de la firma electrónica, su infraestructura y su ecosistema digital. Actualmente se encuentra modificada por Ley Nº 27.310.

Además, Perú cuenta con la reglamentación de la misma, el Reglamento de la Ley de Firmas y Certificados Digitales a través del Decreto Supremo N° 052-2008-PCM.

Decimos que esta normativa peruana es una breve, pero concisa legislación donde se definen de manera breve a la firma electrónica y la firma digital.

Encontramos definida a la firma electrónica y esta no cuenta con su propio artículo, sino que se encuentra dentro del texto del Objeto de la Ley 27.269 estableciendo lo siguiente: “Entiéndase por firma electrónica a 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".

Por su parte la Ley 27.269 nos da una definición de firma digital

> La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada (art. 3).

Esta ley, no cuenta con muchos artículos, tal como lo hacen otras legislaciones que vimos. A modo de ejemplo, esta ley ni siquiera define documento ni menciona muchos de los principios básicos en la materia, algo que termina por suceder en el Decreto reglamentario de la Ley de Firmas y Certificados Digitales.

Por su parte el decreto si es más completo y se expide en muchos temas completando así el marco legal en materia de firma digital, y cubriendo en su totalidad los aspectos legales en la materia.

Este decreto tiene por fin regular en los sectores públicos y privados, la utilización de las firmas digitales y el régimen de la Infraestructura Oficial de Firma Electrónica de Perú. También regula el ecosistema legal ya que trata en sus artículos al documento digital, los documentos firmados digitalmente como medio de prueba, características de la firma digital, presunciones de ella, etc.

F. República de Surinam

La República de Surinam no cuenta con legislación específica en materia de firma digital ni electrónica, solamente cuenta con proyectos de ley, como por ejemplo el Proyecto de Ley sobre transacciones comerciales electrónicas que fue presentado en el parlamento de ese país en el año 2017.

VII. Conclusión

Después de conocer y analizar las legislaciones en materia de firma digital en el MERCOSUR y la de los países asociados, sacamos varias conclusiones parciales para la presente tesis.

De manera previa, apreciamos como el tratado fundacional emanado del órgano de integración regional ya dentro de sus objetivos promovía la integración regional, circunstancia que si lo llevamos al terreno digital actual imperante se traduce en armonización a través de marcos legales en materia digital.

Por otra parte, identificamos los elementos fundamentales en materia de firma electrónica, características y diferentes aspectos en materia de firma electrónica de cada país que forman parte del MERCOSUR.

Por lo pronto, ya vislumbramos la existencia de barreras que dificultan el desarrollo óptimo del comercio y del gobierno electrónico debido a la falta de armonización legislativa relativa a la firma electrónica, o mejor dicho no existe un marco de referencia general transfronterizo y multisectorial para la interoperabilidad de identificación y de firmas electrónicas.

El Grupo Agenda Digital del MERCOSUR, se elaboró la Decisión N° 11/19 del Consejo Mercado Común: el Reconocimiento mutuo de los certificados de firma digital y también la Decisión N° 15/2021 del Consejo Mercado Común: Acuerdo sobre comercio electrónico del MERCOSUR. Sin embargo, no hay en agenda proyectos de mercado único digital similar al de la U.E. Esto y la incorporación de una filosofía de mercado único digital, promovería y haría alcanzar al Mercosur nuevos horizontes, así como más beneficios a sus estados miembros.

Destacamos la necesidad de una norma supranacional que permita eliminar las barreras al mercado único para firmas electrónicas, firmas digitales, documentos digitales y servicios de confianza relacionados a las transacciones electrónicas transnacionales entre estados miembros, asegurando que estos servicios digitales tendrán el mismo valor legal que en los procesos que tradicionalmente se hacían en papel y que ahora en la actualidad se hacen de manera completamente digital.

Más adelante veremos que la firma electrónica es uno de los servicios de confianza existentes en la U.E, por lo que también en ella se incluyen herramientas que benefician a la confianza digital tales como sellos electrónicos o sellos del tiempo electrónicos, servicios de autentificación web y demás herramientas que permiten florecer el mercado digital transaccional.

Por lo tanto, decimos que se necesita trabajar más en profundidad en la creación de un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web en el MERCOSUR.

No hallamos un trabajo de armonización en cuanto a la identificación electrónica de los ciudadanos del MERCOSUR ni tampoco una agenda que lo incluya. En los países que integran el MERCOSUR los efectos jurídicos de la firma digital y de la firma electrónica como la identificación electrónica de los firmantes, puede disponerse de manera diferente en cada país a diferencia de lo que sucede en la U.E. y que veremos más adelante, por lo que se hace necesario empezar a trabajar en el ID electrónico de los ciudadanos.

Por ello finalizamos el capítulo estableciendo que actualmente existen barreras en cuanto a la firma electrónica en el MERCOSUR; y esto hace necesario armonizar las legislaciones en torno a firmas electrónicas en el bloque regional, más aún en la situación actual mundial y regional en la que el comercio electrónico paso a ser la regla y todo lo que no sea digital, la excepción.

Capítulo V

El Reglamento eIDAS. La Identificación Electrónica y los Servicios de Confianza en la Unión Europea

I. Introducción

En este capítulo, conoceremos el ecosistema digital de la U.E, para ello, destacamos al igual como lo venimos haciendo en toda la tesis doctoral, la vital importancia del Reglamento N° 910/2014 del Parlamento Europeo y del Consejo, del 23 de julio de 2014, que significó un cambio de paradigma en la identificación digital y los servicios de confianza los cuales incluyen, entre otras cosas, a la firma electrónica.

Del mismo modo, identificaremos los elementos fundamentales del Reglamento, y adelantamos que no nos limitaremos a hablar de la firma electrónica, sino que también analizaremos la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior del bloque europeo.

Por otro lado, conoceremos los orígenes de este marco legal, como por ejemplo lo es la Directiva 1999/93/CE, marco comunitario para la firma electrónica la cual fue derogada por el reglamento.

Conoceremos la materialización de proyectos llevados adelante como la Agenda Digital en favor del desarrollo de un Mercado Único Digital de la U.E, que hizo posible a la interoperabilidad, estándares, confianza digital o seguridad que encontramos en el Reglamento eIDAS y que no lo encontramos sin ir más lejos, en nuestra región.

Por último, también conoceremos el último proyecto de reglamento que modifica el Reglamento eIDAS en lo que respecta al establecimiento de un marco para una “Identidad Digital Europea”. Vale decir que esta propuesta de la Comisión Europea no sustituye el Reglamento eIDAS, solo modifica algunos aspectos de este y que

todavía no tuvo efectos jurídicos, pero nos dará un adelanto de lo que se viene en la U.E. en materia digital.

II. La Unión Europea. El Tratado constitutivo de la Comunidad Europea

Para situarnos en el tiempo y espacio en el presente trabajo de investigación, analizaremos brevemente la asociación política y económica europea de la U.E, para llegar a la Comisión Europea y avanzar con nuestro tema principal, el Reglamento eIDAS.

La U.E es una asociación económica y política que abarca cuestiones de política económica, de política exterior y de seguridad, y decimos sin lugar a dudas que este bloque regional compuesto por 27 países europeos (desde febrero de 2020 con la salida del bloque por parte del Reino Unido), siendo una de las entidades jurídicas más importantes y avanzadas en el mundo.

En el año 1958 se creó la Comunidad Económica Europea, creada por el Tratado de Roma de 1957, que en un principio establecía una cooperación económica cada vez más estrecha entre seis países: Alemania, Bélgica, Francia, Italia, Luxemburgo y los Países Bajos. Con posterioridad se unieron a ellos otros 22 países, creando un enorme mercado único que sigue avanzando hasta lograr el que conocemos en la actualidad.

El Tratado de Funcionamiento de la Unión Europea, junto con el Tratado de la Unión Europea o Tratado de Maastricht, el Tratado constitutivo de la Comunidad Europea de la Energía Atómica y la Carta de Derechos Fundamentales de la Unión Europea son los cuatro documentos que configuran la constitución material de la Unión Europea (U.E, s.f.)

Decimos que se produce el cambio de nombre de Comunidad Económica Europea a Unión Europea, en el año 1993.

Todas las acciones emprendidas por la U.E. se basan en tratados que han sido aprobados voluntaria y democráticamente por todos los países miembros que la componen. Estos tratados establecen los objetivos de la unión, las normas

aplicables a sus instituciones, la manera en que se toman las decisiones y la relación existente entre esta y sus países miembros.

Reiteramos que el 31 de enero de 2020, el Reino Unido de Gran Bretaña terminó abandonando la U.E., pero esto no afecta los objetivos y los planteamientos del presente trabajo.

Es relevante la gran tarea y obra realizada por la Comisión Europea, encargada de traernos el Reglamento eIDAS, por ello pasaremos a analizar brevemente dicho órgano.

La Comisión Europea es una de las siete instituciones que conforman el órgano de la U.E. Esta comisión es la encargada de proponer legislación, aplicar las decisiones comunitarias, defender los tratados de la Unión y en general se ocupa de los asuntos diarios de la U.E. Es importante remarcar que es un ente políticamente independiente de los gobiernos europeos que integra, representa y defiende los intereses de la Unión Europea (U.E, s.f.).

La principal función es la de velar por los intereses generales de la U.E. proponiendo, comprobando que se cumpla la legislación y aplicando las políticas y el presupuesto de la U.E. La misma se encuentra integrada por un equipo ("colegio") de comisarios, se trata de un equipo de 27 comisarios uno por cada país integrante de la U.E, todo ello bajo la dirección del presidente de la Comisión, que decide quién es responsable de cada política (U.E, s.f.).

La comisión es la única instancia responsable de elaborar propuestas de nueva legislación europea y de aplicar las decisiones del Parlamento Europeo y el Consejo de la U.E. Esta comisión dentro de su fecunda labor nos trajo las normas que trataremos a continuación.

III. La Directiva 1999/93/CE: Marco regulatorio comunitario sobre la firma electrónica

La Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, del 13 de diciembre de 1999, establecía un marco comunitario para la firma electrónica, la

cual fue publicada en el Diario Oficial de las Comunidades Europeas de 19 de enero de 2000.

La directiva sentó un marco común para la firma electrónica que se concretó con la transposición de la directiva a las diferentes legislaciones nacionales de los países miembros del bloque regional europeo.

Decimos que este marco regulatorio tuvo a grandes rasgos dos objetivos, por un lado, facilitar el uso de la firma electrónica tal como se venía implementando en casi todo el mundo, solo que en este caso en el bloque regional y por el otro lado, el de contribuir al reconocimiento jurídico de la firma electrónica, garantizando así el correcto funcionamiento de la misma en el bloque regional.

La directiva actualmente se encuentra derogada, y contaba con solo 14 artículos, sin embargo, su texto dejó definiciones, principios, efectos jurídicos, responsabilidades, aspectos internacionales, incluso protección de datos personales, que fueron enriquecedores en el derecho informático y que aún se siguen implementando en muchas otras legislaciones.

Dentro sus considerandos, dejaba en claro la necesidad de promover la interoperabilidad de los productos de firma electrónica. Además, establecía satisfacer los requisitos esenciales específicos de los productos de firma electrónica a fin de garantizar la libre circulación en el mercado interior y fomentar la confianza en la firma electrónica, importantísimo punto ya que, en el momento de la sanción de la misma, era vital el correcto desarrollo de la confianza digital.

Además, la directiva establecía en sus considerandos que para la prestación de servicios de certificación no era necesaria la obtención de autorización previa. Esta premisa se declaraba compatible con el posible establecimiento de sistemas voluntarios de acreditación que promuevan una mejora en los niveles de la calidad de prestación de servicios de certificación, tal como reza la directiva

> Los sistemas voluntarios de acreditación destinados a un nivel reforzado de prestación de servicios pueden aportar a los proveedores de servicios de certificación un marco apropiado para aproximarse a los niveles de confianza, seguridad y calidad exigidos por un mercado en evolución. Dichos sistemas deben fomentar la adopción de las mejores prácticas por parte de los proveedores de servicios de certificación; debe darse a los proveedores de servicios de certificación libertad para adherirse a dichos sistemas de acreditación y disfrutar de sus ventajas (considerando 11).

Asimismo, la directiva establecía, en cuanto al correcto funcionamiento del mercado interior, que los estados miembros no podrán restringir la prestación de servicios de certificación que procedan de otro estado miembro.

Tal como la directiva dejaba establecido

> Los Estados miembros pueden decidir cómo llevar a cabo la supervisión del cumplimiento de lo dispuesto en la presente Directiva. La presente Directiva no excluye el establecimiento de sistemas de supervisión basados en el sector privado. La presente Directiva no obliga a los proveedores de servicios de certificación a solicitar ser supervisados con arreglo a cualquier sistema de acreditación aplicable (considerando 13).

Por lo que decimos en este punto, que se encontraba a favor del desarrollo del sector privado resguardando la libertad en todo momento.

Tal como mencionamos, la Directiva 1999/93/CE nos trajo definiciones de firma electrónica, incluso requisitos

> 1) "firma electrónica": los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación; 2) "firma electrónica avanzada": la firma electrónica que cumple los requisitos siguientes: a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable (art.2).

En cuanto a los efectos jurídicos de la firma electrónica en la U.E, la directiva establecía en el art. 5 una equivalencia entre una firma manuscrita y una firma electrónica avanzada, que para nosotros sería una firma digital.

Por su parte, los efectos jurídicos de la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma, estarían dados por los estados miembros tal como establece

> a) satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel; y b) sea admisible como prueba en procedimientos judiciales. (art. 5).

En cuanto a los requisitos del punto a. del art. 5 tiene que ver el anexo I de la Directiva, que contiene la indicación de que el certificado se expide como

reconocido, la identificación del prestador y del Estado parte en que está establecido.

También decimos que para la directiva la equivalencia funcional de la firma ológrafa con la firma electrónica avanzada no excluía la eficacia jurídica de una firma electrónica que no cumplía con los requisitos del art. 5, debiendo determinarse en cada caso, su validez y su eficacia jurídica.

El régimen de responsabilidades de la directiva se centraba en los prestadores de servicios que expiden certificados reconocidos, siendo responsables: de la veracidad de los datos contenidos en los mismos, de la complementariedad de los datos de creación y verificación de firma expedidos por el prestador, de que el titular del certificado dispone de los datos de creación de firma correspondientes a los datos de verificación que figuran en el certificado y de registrar la revocación de los certificados.

No obstante, observamos que se contemplaba la posibilidad de eximir al prestador de estas responsabilidades cuando demuestre que no ha actuado con negligencia.

Asimismo, la directiva preveía una limitación de la responsabilidad de los prestadores de servicios de certificación por la utilización de certificados reconocidos emitidos por ellos, en caso de que no se respeten los límites de utilización o los valores límite de transacciones establecidas en los certificados, siempre y cuando estos límites sean reconocibles para terceros.

Finalmente, destacamos que la Directiva creaba un comité de firma electrónica, cuyos trabajos se centrarán en la clarificación de los requisitos establecidos en los anexos de la Directiva y en determinar las normas técnicas que gocen de reconocimiento general para productos de firma electrónica.

En la Directiva 1999/93/CE cada estado de la U.E interpretaba la norma a su manera, lo que significaba una complicación para el reconocimiento y la validez de las firmas electrónicas entre países y sus correspondientes legislaciones.

Por ejemplo, existía una laguna legislativa en el área de identificación de usuarios en los servicios electrónicos, puesto que cada país disponía de su propia forma de reconocerlos. Y cada una de estas formas de reconocimiento de identidades no

siempre coincidía con las formas o mecanismos establecidos en otros Estados miembros de la U.E.

Por otro lado, existían lagunas en la regulación de servicios de confianza, ya que no estaban incorporadas herramientas como los sellos electrónicos, sellos del tiempo electrónico, etc.

Con la sanción del Reglamento eIDAS, se termina regulando la identificación electrónica y establecieron pautas para los servicios de confianza relativos a las transacciones electrónicas que son comunes para los países que integran la U.E.

En este caso hablamos de reglamento y no directiva, lo que significa que no necesita transposición en los estados miembros y se aplica directamente ampliando lo dispuesto por la Directiva 1999/93/CE, regulando el establecimiento de un marco legal común para la interacción electrónica segura entre ciudadanos, empresas y autoridades públicas que integran la U.E.

IV. El Reglamento eIDAS (UE) Nº 910/2014

A. Origen y antecedentes

El Reglamento eIDAS se crea bajo la base de la propuesta realizada en el artículo 114 del Tratado de Funcionamiento de la Unión Europea (antiguo artículo 95 Tratado de la Comunidad Europea). La selección de un reglamento en virtud del art. 288 del tratado daría así mayor seguridad jurídica a diferencia de la Directiva.

En el año 2010 la Comisión Europea emite una comunicación o MEMO/10/20 bajo el título “Una Agenda Digital para Europa” dejando establecido que: “La Agenda Digital para Europa ayudará a los ciudadanos y empresas de Europa a sacar el máximo partido de las tecnologías digitales”.

Dentro de sus puntos más importantes menciona el reto que significa, atento la fragmentación del mercado digital, y cómo la U.E iba a la zaga con respecto a otros países en cuanto a redes digitales veloces, fiables y conectadas del marco del *Digital Single Market* [Mercado Digital Único].

Este concepto de Mercado Único Digital se le designa a la estrategia de los años 2014 al 2019 de la Comisión Europea para el mejor acceso posible al mundo en línea para individuos y empresas. Este lo podemos definir como aquel en el que se garantiza la libre circulación de personas, servicios, capital y por el cual las personas o empresas puedan acceder sin problemas, participar en actividades en línea en condiciones de competencia leal, un alto nivel de consumo y personal, protección de datos, independientemente de su nacionalidad o lugar de residencia.

La comisión desde los años 2014 al 2019 había identificado la finalización de este reto como una de sus diez prioridades políticas y estratégicas.

La estrategia de este Mercado Digital Único se basó en tres pilares: acceso, con un mejor acceso de consumidores y empresas a bienes y servicios digitales en toda Europa; Medio ambiente, en el sentido de crear las condiciones adecuadas y la igualdad de condiciones para que prosperen las redes digitales y los servicios innovadores; Y por último economía y sociedad, favoreciendo maximizar el potencial de crecimiento de la economía digital.

En el MEMO/10/20 “Una Agenda Digital para Europa” sostiene que: “La Agenda Digital para Europa se creó en mayo de 2010 para impulsar la economía europea aprovechando las ventajas económicas y sociales sostenibles del mercado único digital” (p. 3).

Además, afirma lo siguiente: “La Agenda Digital para Europa modernizará las normas de la UE sobre el mercado único digital para hacer más fácil el comercio electrónico” (p. 5).

Por último, deja establecido los principales retos que atraviesa la Agenda Digital para Europa. Por un lado, la incorporación de la banda ancha de internet, ya que esta significó un gran avance en materia de telecomunicaciones al momento de redactar este MEMO. Por último, establece que el Mercado Único Digital será accesible a los consumidores.

En otro informe de la Comisión Europea sobre la ciudadanía de 2010, titulado “La eliminación de los obstáculos a los derechos de los ciudadanos de la U.E”, se resaltó la necesidad de resolver los principales problemas que impiden a los ciudadanos de

la U.E disfrutar de los beneficios de un Mercado Único Digital y de los servicios digitales transfronterizos.

A través de la “Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Acta del Mercado Único (2011)”, se establecieron doce prioridades para estimular el crecimiento y reforzar la confianza, donde el Consejo Europeo invitó a la Comisión Europea a crear el denominado “Mercado Único Digital” a fin de progresar rápidamente en ámbitos clave de la economía digital y promover un mercado único digital plenamente integrado, facilitando el uso transfronterizo de los servicios en línea, con especial atención a la identificación y autenticación electrónicas seguras.

La Comunicación establecía lo siguiente

> Mercado único digital. Medida clave: Legislación que garantice el reconocimiento mutuo de la identificación y autentificación electrónicas en toda la UE y revisión de la Directiva sobre la firma electrónica. El objetivo es conseguir una interacción electrónica segura y sin obstáculos entre empresas, ciudadanos y administraciones públicas para aumentar, incluso en su dimensión transfronteriza, la eficacia de los servicios, de los contratos públicos, de la prestación de servicios y del comercio electrónico (2.7).

Por otro lado, esta comunicación es crucial ya que nos trae también la necesidad de que la reglamentación con especial atención en materia de identificación electrónica en la U.E. algo que quedó plasmado cuando refiere que: “El marco garantizará también el reconocimiento mutuo de los servicios de identificación y de autentificación electrónicas y abordará el funcionamiento transfronterizo de algunos otros servicios de confianza” (2.7).

Ya mencionamos que en ese momento se encontraba como Marco Regulatorio Comunitario sobre firma electrónica en la U.E, la Directiva 1999/93/CE que al parecer y según lo que podemos inferir de estos informes, no tenía el éxito esperado.

En ese panorama, la comisión presentó una “Propuesta de Reglamento” relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mes junio del 2012, para que se estudie y se debatiera en el Parlamento Europeo. La propuesta se basaba en la mencionada normativa sobre

firma electrónica en la U.E., la Directiva 1999/93/CE que intentaba armonizar las firmas electrónicas.

Puntualmente se denominaba como “Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior”.

Posteriormente, se crea la iniciativa Mecanismo Conectar Europa o en inglés *“Connecting Europe Facility”,* la cual se crea mediante el Reglamento Nº 1316/2013 del Parlamento Europeo y del Consejo. Este reglamento determina las condiciones, métodos y procedimientos para proporcionar asistencia financiera de la U.E a las redes europeas a fin de apoyar proyectos de interés común, además de establecer el desglose de los recursos disponibles para el periodo que fue desde el 2014 al 2020 en los campos de transporte, telecomunicaciones y energía.

En este contexto, el Reglamento eIDAS, se termina publicando en el año 2014, el cual tiene como función principal armonizar los sistemas de identificación electrónica de la U.E y sus integrantes, así como el reconocimiento mutuo para los servicios de confianza en línea realizados por los organismos públicos a efectos de la autenticación transfronteriza.

Entre los objetivos y sus considerandos veremos que lo que busca este marco legal, es reforzar la confianza en las transacciones electrónicas en el mercado interior europeo digital, el ya mencionado Mercado Único Digital, con un marco regulatorio que logre que las interacciones electrónicas sean seguras entre los ciudadanos, las empresas y las administraciones públicas.

Antonio Merchán Murillo (2015) detalla al respecto

> Con este Reglamento se viene a plantear un mercado único de la firma electrónica y los servicios de confianza en línea afines más allá de las fronteras, asegurando que esos servicios funcionen y gocen del mismo estatuto jurídico que los trámites tradicionales en papel, dándose pleno efecto a los posibles ahorros propiciados por la contratación electrónica. Por otro lado, se pretende respetar los sistemas de identificación nacionales, así como las preferencias de los Estados miembros que no tienen sistemas nacionales de identificación, permitiendo a los países que si tienen sistemas de identificación electrónica optar por quedar fuera del sistema paneuropeo (p. 43).

B. introducción al Reglamento eIDAS

En este punto, nos introduciremos de lleno en el denominado Reglamento eIDAS Nº 910/2014 del Parlamento Europeo y del Consejo, del 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. Este reglamento es conocido por sus siglas en inglés eIDAS, "*electronic IDentification, Authentication and trust Services",* que en español lo traducimos como identificación electrónica, autenticación y servicios de confianza.

Se establecía que a partir del 1 de julio de 2016 fuese obligatoria la validación de todos los certificados digitales europeos incluidos en las listas de confianza de sus estados miembros conforme al artículo 52.2.

Además, establece que los estados que integran el bloque regional deben reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro estado miembro. También establece los denominados "servicios de confianza", algo muy interesante en nuestra materia, un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

Establecemos que hasta este punto, se venían analizando y tratando legislaciones que solo trataban como eje principal a la firma electrónica. El Reglamento da un enfoque más global y mucho más amplio.

Merchán Murillo (2016), explica la construcción del Mercado Único Digital

> … en definitiva, lo que se pretende es hacer plenamente interoperables los servicios de e-Administración, superando las barreras organizativas, técnicas, semánticas y jurídicas, para garantizar que los puntos de contacto únicos funcionen como verdaderos centros de e-Administración, permitiendo el acceso a los ciudadanos y empresas y que se cree una lista común de servicios públicos transfronterizos esenciales, que correspondan a necesidades bien definidas (p. 123).

Además, Merchán Murillo (2016) establece que: "…solo de esta manera, se puede determinar un sistema jurídico específico, que permita a los actores

actuantes en el mercado comunicarse, intercambiar información, ofrecer y usar servicios y productos en tiempo real” (p. 123).

Este reglamento tiene también como objetivo proporcionar un marco legal de confianza que permita el comercio y las interacciones electrónicas seguras y sencillas entre las administraciones públicas, los ciudadanos y las empresas.

Entonces afirmamos, que esta norma es de aplicación directa en todo el territorio de la U.E, la cual consta de dos bloques fundamentales, el primero relativo a la identificación electrónica transfronteriza, y el segundo a los servicios de confianza.

En otras palabras, este marco legal establece:

Las condiciones en que los estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro estado miembro, una suerte de ID electrónica europea transfronteriza en la U.E.

Y por el otro lado, las normas para los servicios de confianza, en particular para las transacciones electrónicas, y el marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

El reglamento cuenta 77 considerandos, con 6 capítulos, y con 4 anexos. Es un vasto y completo marco legal no solamente referente a la firma digital como veníamos viendo en la tesis doctoral, sino de muchos más aspectos.

V. Considerandos del Reglamento eIDAS

Tal como ya mencionamos, el Reglamento eIDAS cuenta con la importante cantidad de 77 considerandos, por lo cual consideramos necesario tratar las razones que apoyan o sirven de fundamento al texto del reglamento, pero por razones lógicas sólo seleccionamos los más importantes.

El reglamento inicia su texto en miras de uno de los principales objetos del mismo

> La creación de un clima de confianza en el entorno en línea es esencial para el desarrollo económico y social. La desconfianza, en particular debida a la inseguridad jurídica percibida, hace que los consumidores, las empresas y las administraciones públicas duden a la hora de realizar transacciones por vía electrónica y adoptar nuevos servicios (considerando).

Por ello opinamos que se busca la creación de un clima de confianza digital, el cual es esencial para el desarrollo económico y social. Por otro lado, el considerando menciona a la desconfianza, en particular la menciona como a la inseguridad jurídica percibida, que hace que los consumidores, las empresas y las administraciones públicas duden a la hora de realizar transacciones por vía electrónica y adoptar nuevos servicios.

Lo mencionado por el primer considerando se encuentra en sintonía con el considerando segundo, donde también se propone reforzar la confianza de las transacciones electrónicas entre los ciudadanos, las empresas, las administraciones públicas incrementando la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la U.E.

Los servicios electrónicos de confianza son el eje central del mercado digital que pretende eliminar las barreras al comercio electrónico y todo tipo de transacciones electrónicas entre los diferentes estados integrantes de la U.E. Estos engloban los servicios relativos a la creación, verificación y validación de firmas electrónicas, sellos electrónicos, o certificados para la autenticación de sitios web, entre otros, no solamente como otras legislaciones en materia de firma digital.

Decimos nuevamente en este punto, que la confianza digital y el fomento de la confianza en el comercio electrónico se encuentra en casi todas las legislaciones

en materia de firma digital, ni hablar de la Ley Modelo de la CNUDMI sobre comercio electrónico en la que se basan casi todas las legislaciones del MERCOSUR.

En el tercer considerando del Reglamento menciona a la Directiva 1999/93, y de cómo esta directiva no ofrecía un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables, etc. Y como el Reglamento eIDAS viene a reforzar y a ampliar el acervo hereditario que deja la directiva.

Los siguientes considerandos continúan hablando del Mercado Único Digital, por ejemplo, el cuarto considerando nos habla de la comunicación “Una Agenda Digital para Europa” la cual señalaba la fragmentación del mercado digital, la falta de interoperabilidad y el incremento de la ciberdelincuencia constituían obstáculos importantes para el ciclo virtuoso de la economía digital.

También en el cuarto considerando nos menciona como en el Consejo Europeo ya se había estipulado la necesidad de crear este Mercado Único Digital para el año 2015 a fin de progresar rápidamente en ámbitos clave de la economía digital y promover un mercado digital plenamente integrado, facilitando el uso transfronterizo de los servicios en línea, con especial atención a la identificación y servicios de confianza.

En ese orden de ideas en el sexto considerando, menciona la necesidad de contribuir al Mercado Único Digital a través de las fronteras de instrumentos clave tales como la identificación electrónica, los documentos electrónicos, las firmas electrónicas y los servicios de entrega electrónica, así como para unos servicios de administración electrónica interoperables en toda la U.E.

El Considerando número doce tiene uno de los objetivos más importantes, eliminar las barreras existentes para el uso transfronterizo de los medios de identificación electrónica utilizados en los estados miembros para autenticar al menos en los servicios públicos.

Estas cuestiones nos planteamos en la presente tesis, es su principal problema y es algo que vino a tratar el presente reglamento. ¿Por qué existen barreras en cuanto a la firma electrónica en un bloque regional como el MERCOSUR? ¿Cómo armonizar las legislaciones en torno a firmas electrónicas en él?

Los siguientes tres considerandos nos hablan del reconocimiento, seguridad y la necesidad de fomento de los medios de identificación electrónica establecidos en el reglamento. Sobre todo, coincidimos en la seguridad, ya que se establecerán más adelante los niveles de seguridad que deben caracterizar el grado de confianza de un medio de identificación electrónica. Más adelante, en los siguientes considerandos números 21, 22 y 23 se mencionan cuestiones referentes al marco regulatorio, tales como que el reglamento es un marco jurídico general, pero permitiéndoles a los países integrantes mantener o introducir sus propios servicios de confianza, Los estados miembros deben conservar la libertad para definir otros tipos de servicios de confianza. Los siguientes considerandos, los 26 y 27 incorporan en el reglamento el principio de neutralidad tecnológica que ya tratamos con anterioridad.

En razón de la rápida evolución de la tecnología, el presente reglamento debe adoptar un planteamiento abierto a innovaciones. El reglamento debe ser neutral en lo que se refiere a la tecnología, esto significa que los efectos jurídicos que otorga deben lograrse por cualquier medio técnico, siempre que se cumplan los requisitos que en él se estipulan. Así encontramos referencias sobre el “principio de neutralidad tecnológica”.

> El principio de neutralidad tecnológica significa que (…) pretende abarcar todas las situaciones de hecho en que la información se genera, archiva o transmite en forma de comunicaciones electrónicas, independientemente de la tecnología o del medio que se haya utilizado (anexo XI).

El principio de neutralidad tecnológica por lo tanto establece que la Ley y su implementación no debe estar sujeta a una tecnología en particular, sino que debe considerar también a las tecnologías que propiciaron su elaboración y reglamentación, así como también las nuevas tecnologías.

Por otro lado, en los considerandos 48 en adelante hasta el 57 menciona a la firma electrónica, estableciendo como debe ser tratada en el reglamento por parte los estados integrantes de la U.E como, por ejemplo, cuando es necesario un alto nivel de seguridad para garantizar el reconocimiento mutuo de las firmas electrónicas, deben aceptarse también las firmas electrónicas que tienen una menor garantía de la seguridad. También se menciona el principio de que no se deben

denegar los efectos jurídicos de una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla todos los requisitos de la firma electrónica cualificada.

Los considerandos desde el 58 al 62 van a tratar los sellos electrónicos mencionando que cuando una transacción electrónica exija un sello electrónico cualificado de una persona jurídica, debe aceptarse una firma electrónica cualificada del representante autorizado de la persona jurídica. Por otro lado, establece que los sellos electrónicos deben servir como prueba para un documento electrónico. El reglamento debe garantizar la conservación a largo plazo de la información, es decir, la validez jurídica de la firma electrónica y los sellos electrónicos con el fin de garantizar la seguridad de los sellos cualificados de tiempo electrónicos.

Los últimos considerandos que trataremos son los nro. 63, 65 y 66 que nos traen los fines y objetivos relativos a los documentos electrónicos en el reglamento estableciendo el principio de que no se deben denegar efectos jurídicos de un documento electrónico por el solo hecho de estar en formato electrónico, esto es al objeto de garantizar que no se rechazará una transacción electrónica aportando más seguridad jurídica y por consiguiente confianza digital.

Como consecuencia de la lectura de los considerandos, establecemos que sirvieron para plantear los objetivos y lineamientos que debe tener un marco legal de semejantes características, más aún en la presente tesis doctoral donde se tratará con posterioridad la posibilidad y la necesidad de lograr los resultados de armonización logrados por la U.E en otro lugar.

VI. Disposiciones generales del Reglamento eIDAS

Las disposiciones generales de este marco legal se encuentran en el Capítulo I del mismo y cuentan con 5 artículos, que van a tratar el objeto, el ámbito de aplicación, las definiciones, el principio del mercado interior, y el tratamiento y protección de los datos.

En el primer artículo encontramos el objeto de la ley

> El objeto del reglamento es el de garantizar el correcto funcionamiento del mercado interior aspirando al mismo tiempo a un nivel de seguridad

adecuado de los medios de identificación electrónica y los servicios de confianza por lo que se establece que:
a) las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro.
El Reglamento eIDAS al establecer las condiciones mencionadas en el artículo 1 inciso a), condiciones que orbitan fuertemente alrededor de las cuestiones de seguridad e interoperabilidad de los sistemas y medios de identificación electrónica, como tendremos ocasión de analizar en detalle en el capítulo II.
b) las normas para los servicios de confianza, en particular para las transacciones electrónicas. Los servicios de confianza que menciona son los servicios relativos a la creación, verificación y validación de firmas electrónicas, sellos electrónicos, o certificados para la autenticación de sitios web, entre otros, circunstancia que veremos más adelante, en donde se le dedica un capítulo completo.
c) establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web (art.1).

Como vemos, el Reglamento eIDAS, delimita un nuevo marco jurídico para las firmas electrónicas en la U.E, modernizando y actualizando la Directiva 1999/93, y sumando muchos más elementos.

A. Las definiciones en el Reglamento

El art. 3 del reglamento nos va a dar al igual que lo hacen muchas legislaciones, definiciones acerca de la terminología utilizada en el entramado normativo, pero vale mencionar que esta vez tenemos el considerable número de 41 definiciones, que se aplican en el reglamento.

Este artículo es de especial interés, ya que no siempre la definición jurídica coincide con la definición técnica, más aún, en un marco legal que engloba tantos temas técnicos y de tantos países. Por consiguiente, aclaramos que haremos más énfasis en las definiciones clave y no en la totalidad de ellas.

La “identificación electrónica”, en el Reglamento eIDAS es definida como:

“El proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica” (art.3).

Por ello señalamos que esta definición trata de la identificación de los ciudadanos en distintos países a través de medios digitales, de los documentos de identidad electrónicos como el DNI electrónico, licencias de conducir, tarjetas bancarias, etc. con la cual es posible acceder a los servicios públicos de la U.E de manera online.

La Comisión Europea estableció una serie de objetivos e hitos para la identificación electrónica en su *Comunicación 2030 Digital Compass: The European Way for the Digital Decade* [Comunicación 2030 Brújula Digital: El Camino Europeo para la Década Digital]. Por ejemplo, en ella establece que para el año 2.030 todos los servicios públicos clave deberían estar disponibles online, también que todos los ciudadanos de la U.E. tendrán acceso a registros médicos electrónicos; y como otro objetivo, se establece que el 80% de los ciudadanos deberían utilizar la identificación electrónica, dejando de lado el papel.

Por otro lado, tenemos la nueva Propuesta de Reglamento sobre Identidad Digital Europea que modifica el Reglamento eIDAS mejorando así la eficacia del marco legal y extendiendo sus beneficios al sector privado con una nueva infraestructura para la identidad digital de la U.E. que también analizaremos más adelante. Destacamos que la extensión de la identificación electrónica puede utilizarse para garantizar el cumplimiento de labores, así como también para garantizar la mayoría de edad de los usuarios que se registran en las redes sociales.

La identidad electrónica en este capítulo cobra un relevante interés, ya que encontramos un virtual vacío imperante en nuestro país y en el MERCOSUR, circunstancia que hace necesario analizar este punto en profundidad más adelante cuando tratemos el CAPÍTULO II, IDENTIFICACIÓN ELECTRÓNICA del reglamento.

En el inciso 2 del art. 3 del Reglamento eIDAS encontramos los “medios de identificación electrónica” se encuentran también en el definido como: “… una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea”. (art. 3).

Por su parte, el reglamento en el inciso 3 del art. 3 define los “datos de identificación de la persona” como: “… un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica” (art.3).

El reglamento en el inciso 4 del art. 3 establece que los “sistemas de identificación electrónica”, se definen como: “… un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica” (art.3).

Llegamos finalmente a los conceptos de firma electrónica y firma electrónica avanzada en el Reglamento eIDAS, en el inciso 5, encontramos “Firma electrónica”, la misma se define en el reglamento de la siguiente manera: “… los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar” (art.3).

Estamos frente a la firma electrónica simple, siendo el género y de la cual surgen las demás siempre y cuando cumplan los requisitos que pasamos a ver a continuación en el siguiente punto.

Y en el inciso 6 del mismo artículo encontramos “Firma electrónica avanzada”, (que en otras legislaciones adoptan el término firma digital): “… la firma electrónica que cumple los requisitos contemplados en el artículo 26” (art.3).

¿Y qué dice el art. 26 del reglamento? Establece como requisitos que esta clase de firma debe vincularse de forma exclusiva a la persona que firma los datos en formato electrónico y pueden detectar posteriormente cualquier cambio realizado en los datos dentro del documento, deben permitir la identificación del firmante. Por otro lado, deben haber sido creadas utilizando datos de creación de la firma bajo su control exclusivo, y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable. Todos estos requisitos le dan a la firma electrónica la autoría, la integridad y el no repudio característico de la firma electrónica avanzada.

El inciso 7 del art. 3 del Reglamento eIDAS nos trae la “firma electrónica cualificada”, la cual es definida de la siguiente manera: “… una firma electrónica

avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica" (art.3).

Las firmas electrónicas cualificadas tienen las mismas características que las firmas electrónicas avanzadas, pero se crean utilizando tecnología más sofisticada, cumplen con un estándar más alto de seguridad, cumplen con criterios de validación más estrictos y están respaldadas por un certificado más detallado. Por lo tanto, la firma electrónica cualificada utiliza un dispositivo cualificado de firma electrónica.

El inciso 8 del reglamento nos trae el "Certificado de firma electrónica" definido como: "… una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, el nombre o el seudónimo de esa persona" (art.3).

En el inciso 9 del art. 3 del reglamento nos trae su novedosa incorporación, el "servicio de confianza" el cual definido en el art. 3

> … el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios (art.3).

Los servicios de confianza tienen como objetivo garantizar la confianza, la seguridad y la seguridad jurídica en las transacciones electrónicas. Hay cinco tipos específicos de servicios de confianza cubiertos por las regulaciones del eIDAS las cuales veremos en el capítulo correspondiente y son los siguientes: firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, servicios de entrega electrónica certificada, y certificados de autenticación de sitios web.

En nuestra opinión, la incorporación de las herramientas digitales dentro de esta categoría es invaluable, debido a que las herramientas que van surgiendo con el pasar de los años no son pocas, más aún en el terreno de las nuevas tecnologías.

Por su parte el inciso 10 del art. 3 del reglamento define el "servicio de confianza calificado" como: "…un servicio de confianza que cumple los requisitos aplicables establecidos en el presente Reglamento" (art.3).

Los servicios de confianza cualificados son servicios de confianza que han sido evaluados por un organismo de evaluación acreditado por eIDAS en la U.E. Los servicios de confianza cualificados tienen un reconocimiento especial en el reglamento y pueden ser ofrecidos exclusivamente por proveedores de servicios de confianza calificados. Al cumplir los requisitos establecidos en el reglamento, brindan un alto grado de confianza digital, confiabilidad y seguridad, por ejemplo, estableciendo métodos estrictos de autenticación y validación de los usuarios, mediante la adopción de fuertes controles de seguridad operativa, etc.

El reglamento en el inciso 11 del art. 3 define el “prestador de servicios de confianza” como: “… una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas” (art.3).

Un prestador de servicios de confianza es cualquier persona física o jurídica dentro del territorio de la U.E que brinda un servicio de confianza establecido en el reglamento. Este término incluye proveedores de servicios fiduciarios calificados y no calificados.

El inciso 12 del art. 3 del reglamento define el “prestador cualificado de servicios de confianza”, como: “… un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación” (art.3).

Para lograr ser un proveedor de servicios de confianza este debe cumplir con los requisitos para los proveedores de servicios de confianza establecidos en las Regulaciones de los países miembros de la U.E y demostrar su cumplimiento a través de un proceso que implica una evaluación por parte de un organismo de evaluación acreditado por eIDAS. Después de la aprobación la información del proveedor de servicios de confianza calificado y los servicios calificados que brindan se publican en una lista de confianza, la cual sirve para verificar el estado calificado de un servicio de confianza.

El inciso 13 del art. 3 del reglamento define “sello electrónico” como: “… datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de

manera lógica con ellos, para garantizar el origen y la integridad de estos últimos” (art.3).

Los sellos electrónicos permiten a las empresas y otras entidades "estampar el sello electrónico" en documentos electrónicos y certificarlos como genuinos, de la misma manera que un individuo puede hacerlo a través de la utilización de la firma electrónica en un documento.

Al igual que con las firmas electrónicas, existen sellos electrónicos avanzados y calificados que ofrecen beneficios adicionales sobre los sellos electrónicos básicos.

En el inciso 14 del art. 3 del reglamento encontramos definido el “Sello electrónico avanzado" como: “…un sello electrónico que cumple los requisitos contemplados en el artículo 36” (art.3).

Al igual que la firma electrónica avanzada, para que un sello sea “avanzado”, tienen que cumplir con similares requisitos establecidos en otro artículo, en este caso el art. 36 del reglamento: El mismo debe estar vinculado al creador del sello de manera única; debe permitir la identificación del creador del sello; haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, bajo su control exclusivo, y estar vinculado con los datos. Nuevamente estas características les garantizan autoría, integridad y no repudio, pero esta vez a un sello.

Este tipo de sello está vinculado de manera más confiable a la organización que crea el sello y, al igual que las firmas electrónicas avanzadas y calificadas, permiten la detección de cualquier cambio realizado posteriormente en los datos sellados.

El inciso 15 del art. 3 del reglamento define “sello electrónico cualificado”, como: “… Un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico” (art.3).

Esta clase de sellos electrónicos con las mismas características que los sellos electrónicos avanzados, pero estos son creados utilizando tecnología más avanzada, cuentan con el respaldado de certificados aún más detallados, cumplen con criterios de validación más estrictos y gracias a ello cumplen con un estándar más alto de seguridad.

El inciso 16 del art. 3 del reglamento va a definir el “sello de tiempo electrónico”, el mismo es la prueba electrónica de que existieron datos particulares en un momento determinado y que no se han modificado desde entonces. Se define el art. 3 del reglamento como: “… 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” (art.3).

El inciso 17 del art. 3 del reglamento nos trae el “sello cualificado de tiempo electrónico” el cual se configura cuando: “Un sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42” (art.3).

Los servicios de sello de tiempo electrónicos calificados deben ser operados por un proveedor de servicios de confianza calificado y deben cumplir con los requisitos del reglamento para sellos de tiempo electrónicos cualificados.

Los requisitos son los siguientes: debe vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte; debe basarse en una fuente de información temporal vinculada al tiempo universal coordinado, y por último haber sido firmada mediante el uso de una firma electrónica avanzada o sellada con un sello electrónico avanzado del prestador cualificado de servicios de confianza.

En el caso del Sello cualificado de tiempo electrónico vemos como aumenta la seguridad y los requisitos como el de establecer la utilización del tiempo universal coordinado o UTC, siendo este el principal estándar de tiempo por el cual el mundo regula los relojes y el tiempo.

También aporta más seguridad el hecho de que sea necesario la utilización de la firma electrónica avanzada o sello avanzado.

En el inciso 18 del art. 3 del reglamento “Documento electrónico” es definido como: “… todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual” (art.3).

Con respecto al documento electrónico aclaramos que lo trataremos más adelante en el capítulo, todo ello debido a la relevancia y recepción que tiene el mismo en las legislaciones en materia de firma digital.

El inciso 19 del art. 3 del reglamento define “servicio de entrega electrónica certificada” como

> … un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada (art.3).

Vemos que los servicios de entrega electrónica registrados actúan como una especie de prueba online segura de envío o un servicio de entrega registrada. Los mismos proporcionan una prueba electrónica de que la información fue enviada y recibida y que no fue interceptada ni alterada en el camino.

El inciso 20 del art. 3 del reglamento define el “servicio cualificado de entrega electrónica certificada” como: “Un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el artículo 44” (art.3).

Un certificado calificado debe ser emitido por un proveedor de servicios de confianza calificado e incluir la información específica establecida en los anexos del Reglamento eIDAS.

Por último, el inciso 21 del art. 3 del reglamento define “certificado para la autenticación de sitios web”: Los mismos identifican a la persona o empresa detrás de un sitio web y ayudan a verificar que el sitio web es genuino. Se definen en el art. 3 del reglamento como una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado.

Los certificados de autenticación de sitios web calificados deben ser emitidos por un proveedor de servicios de confianza calificado y deben cumplir con los requisitos del reglamento para los certificados de autenticación de sitios web calificados. Vale decir que un certificado de firma electrónica o sello es diferente de un certificado de autenticación de un sitio web.

Destacamos la importancia de estas definiciones, sobre todo a la hora de entender herramientas digitales tan novedosas que vino a incorporar este marco legal.

B. El Principio de Mercado Interior, y el Reglamento

El art. 4 del reglamento nos trae el “principio del mercado interior”. Este principio responde a los objetivos de la U.E plasmados en el art. 4, apartado 2, letra a), y los arts. 26, 27, 114 y 115 del Tratado de Funcionamiento de la Unión Europea, así como también como continuación de la Estrategia de Lisboa.

Esta estrategia comienza hace más de 20 años por parte de la Comisión Europea, y tal como constan en las Conclusiones de la Presidencia, Consejo Europeo de Lisboa, del 23 Y 24 de marzo 2000”, aspiraba a la transformación de la U.E en una economía basada en el conocimiento más competitiva y una de las más dinámica del mundo, capaz de generar un crecimiento económico sostenible que permita más y mejores puestos de trabajo y una mayor cohesión social.

Por otro lado, este principio va en línea con la “Estrategia Europa 2020” que introdujo la “Agenda Digital para Europa”, la cual es receptada como una de las siete iniciativas emblemáticas, reconociendo así el papel clave de capacitación que el uso de las TIC tendrá que desempeñar para que consiga lo que ambicionaba para el año 2020. Con posterioridad, este principio también va en línea con el “Mercado Único Digital” reconocido por la Comisión como una prioridad en su Estrategia para el Mercado Único Digital, establecido en la “Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones”.

El art. 4 consta de dos incisos, en el primero se establece

> No se impondrá restricción alguna a la prestación de servicios de confianza en el territorio de un Estado miembro por un prestador de servicios de confianza establecido en otro Estado miembro por razones que entren en los ámbitos cubiertos por el presente Reglamento (inciso 2).

Y por su parte el segundo establece: “Se permitirá la libre circulación en el mercado interior de los productos y servicios de confianza que se ajusten al presente Reglamento” (inciso 2).

Este artículo es receptado nuevamente en la Agenda para Europa 2019-2024, por lo que destacamos la vigencia y la importancia de este principio.

C. El tratamiento de la Protección de Datos Personales en el Reglamento eIDAS

El art. 5 del reglamento contiene el “Tratamiento y protección de los datos”. Este artículo establece que el tratamiento de los datos por parte del reglamento será conforme a lo dispuesto en la Carta de los Derechos Fundamentales de la Unión Europea, además conforme al art. 16, en el apartado 1, del Tratado de Funcionamiento de la Unión Europea, de la ya derogada Directiva 95/46/CE del Parlamento Europeo, y actualmente conforme a la vigente Reglamentación en materia de Protección de datos personales, el Reglamento (U.E) 2016/679.

Además, no debemos olvidar a la carta de Derechos Fundamentales de la U.E del año 2000, que recogía en sus derechos fundamentales la protección de datos personales, establecido bajo el título “Protección de datos de carácter personal” lo siguiente

> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
> 2. Estos datos se tratan de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
> 3. El respeto de estas normas quedaran sujeto al control de una autoridad independiente (art. 8).

La Directiva de Protección de Datos mencionada en este artículo, fue sustituida por el Reglamento (U.E) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE aplicable en todos los países integrantes del bloque regional europeo.

El nuevo Reglamento europeo en materia de protección de datos personales entró en vigor el 24 de mayo de 2016, aprobado por el Parlamento Europeo el 14 de abril de 2016 y publicado en el Diario Oficial de la U.E. el 4 de mayo de 2016. Por lo que este reglamento sale con posterioridad al Reglamento eIDAS.

Decimos que el Reglamento RGPD representa un intento por armonizar al igual que el Reglamento eIDAS, solo que en este caso las normas relativas a la

protección de datos personales en los distintos Estados miembros y se pone como objetivo principal el desarrollo de un mercado digital único mediante la creación de nuevos servicios, aplicaciones, plataformas y software. Según las disposiciones del propio reglamento, está previsto un plazo de dos años para permitir a las distintas instituciones de los países miembros organizarse y adecuar el derecho nacional al contenido de las nuevas normas.

Por último, el inciso segundo del art. 5 menciona que sin perjuicio de los efectos jurídicos que la legislación nacional de cada país integrante de la UE contemple para los seudónimos, este no prohibirá su utilización en las transacciones electrónicas. Aclaramos al respecto, que los seudónimos, alias, apodos, *nicknames* o sobrenombres son particularmente importantes en el terreno digital como, por ejemplo, en los medios de entretenimiento digital, videojuegos, redes, en las que muchas personas utilizan un seudónimo y no su nombre real, por lo que este inciso es más que acertado.

VII. Identificación electrónica en el Reglamento eIDAS

Una de las novedades más importantes que nos trae el Reglamento eIDAS y vale decir que no lo podemos encontrar en otros marcos regulatorios internacionales, es la regulación de la identificación electrónica para la autenticación transfronteriza.

Los principales aspectos de esta ID electrónica de la U.E, se encuentran en el Capítulo II del Reglamento eIDAS, así como en diferentes actos de ejecución dictados por la Comisión Europea.

Mencionamos que abordar el concepto de identificación electrónica en la normativa de la U.E. fue una tarea compleja en el presente debido a lo novedoso y disruptivo del marco legal.

Merchán Murillo (2015) explica respecto a este tema que una identidad se establece a partir de un conjunto de características vinculadas a la propia persona, que en suma constituyen un DNI, es decir, una identificación nacional. En cambio, en el mundo digital la identidad se atribuye al conjunto de rasgos que caracterizan al individuo en un medio de transmisión electrónico.

Merchán Murillo (2015) define de manera muy clara la identidad electrónica estableciendo que

> … la identidad electrónica es un conjunto de informaciones y datos relevantes para una persona, física o jurídica, que se almacenan y se trasmiten a través de los sistemas electrónicos y se utiliza con el fin de identificar a una persona (p. 106).

De acuerdo al art. 3 del reglamento, este es definido como al proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

Por lo tanto, a los fines del reglamento este sirve principalmente para la autenticación transfronteriza en el acceso electrónico a servicios ofrecidos en la U.E.

La anterior definición va en relación con el art. 3 inciso 3 del reglamento que define los datos de identificación personal de la persona como al conjunto de datos que permite establecer la identidad de una persona ya sea física o jurídica, o de una persona física que representa a una persona jurídica. Con respecto a los medios de identificación electrónica, el reglamento los entiende por: “una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea”.

Todas estas definiciones son necesarias para comprender el concepto de identificación electrónica adoptado U.E, único en su clase, ya que se caracteriza por tratarse de un régimen que sustenta el proceso de identificación electrónica de manera internacional.

Con respecto a las especificaciones técnicas, estas se encuentran en el Reglamento de ejecución (U.E) 2015/1502 del 8 de septiembre del año 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica de la U.E.

> El artículo 8 del Reglamento (UE) no 910/2014 establece que un sistema de identificación electrónica notificado en virtud del artículo 9, apartado 1, debe especificar los niveles de seguridad bajo, sustancial y alto de los medios de identificación electrónica expedidos en el marco de ese sistema (considerandos).

Además, el reglamento de ejecución se va a encargar de

> Determinar las especificaciones, las normas y los procedimientos técnicos mínimos es fundamental a fin de garantizar un entendimiento común en cuanto a los detalles de los niveles de seguridad, así como la interoperabilidad al correlacionar los niveles de seguridad nacionales de los sistemas de identificación electrónica notificados con los niveles de seguridad contemplados en el artículo 8, de conformidad con el artículo 12, apartado 4, letra b), del Reglamento (UE) no 910/2014.

Toda esta serie de conceptos y lineamientos que venimos tratando, terminaron por plasmarse en la llamada “Identidad Digital Europea”, establecida en la última modificación, más precisamente en la llamada Propuesta que modifica el Reglamento eIDAS en lo que respecta al establecimiento de un marco para una identidad digital europea (SEC (2021) 228 final) - (SWD (2021) 124 final) - (SWD (2021) 125 final).

En este documento se establece el derecho de toda persona que pueda optar a un documento nacional de identidad a tener una identidad digital reconocida en cualquier lugar de la U.E. Se trata de una identificación para los ciudadanos, residentes y empresas de la U.E. que deseen identificarse o confirmar determinada información personal la cual puede utilizarse para acceder a servicios, tanto públicos como privados, en línea o fuera de línea, en toda la U.E.

Opinamos que esta modificación al Reglamento eIDAS, es la más importante que vimos en años, nos trae novedades en materia de identificación electrónica, situación que hace necesaria que le prestemos atención.

A. Reconocimiento de la Identificación Electrónica en la U.E

La identificación electrónica y la autentificación transfronteriza es uno de los aspectos más importantes y uno de los principales objetivos del Reglamento eIDAS. Lo encontramos en el Considerando 6: “Uno de los objetivos del presente reglamento es eliminar las barreras existentes para el uso transfronterizo de los medios de identificación electrónica utilizados en los Estados miembros para autenticar al menos en los servicios públicos”.

Esta intención se encuentra plasmada cuando se establecen las condiciones necesarias para que opere el reconocimiento de la identificación electrónica de la siguiente manera

> … para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro, siempre que:
> a) este medio de identificación electrónica haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9;
> b) el nivel de seguridad de este medio de identificación electrónica corresponda a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto;
> c) el organismo público en cuestión utilice un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea (art. 6).

El art. 7 por su parte establece las condiciones para la notificación de los sistemas de identificación electrónica. El 7 de noviembre de 2018 se publicó en el Diario Oficial de la U.E la lista de sistemas de identificación electrónica notificados por los estados miembros con arreglo al art. 9, apartado 1, con el número de referencia de publicación (2018/C 401/08).

B. Las condiciones de notificación y la notificación de los sistemas de identificación electrónica

El reglamento va a establecer en el art. 7 las condiciones necesarias para la notificación de los sistemas de ID electrónica que se implementan, para que el reconocimiento mutuo entre servicios digitales, se haga efectivo y tenga efectos jurídicos entre los países de la U.E.

Por lo tanto, se establece en ese artículo que un sistema de identificación electrónica podrá ser objeto de notificación con arreglo al art. 9, apartado 1, ya que el mismo establece que el estado miembro que efectúa la notificación transmitirá a la Comisión determinada información, sin dilaciones indebidas, y cualquier modificación posterior de la misma.

Recordemos que los datos de identificación de la persona son los que permiten establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica según el reglamento.

Los sistemas de ID electrónica podrán ser objeto de notificación si se cumplen la totalidad de las condiciones en el art. 7 del reglamento

> a) que los medios de identificación electrónica hayan sido expedidos: por el Estado miembro que efectúa la notificación; por mandato del Estado miembro que efectúa la notificación, o independientemente del Estado miembro que efectúa la notificación y reconocidos por dicho Estado miembro.
> b) que los medios de identificación electrónica puedan usarse para acceder al menos a un servicio prestado por un organismo del sector público que exija la ID electrónica en el Estado miembro.
> c) que tanto el sistema de ID electrónica como los medios de ID electrónica cumplan los requisitos de al menos uno de los niveles de seguridad previstos en el acto de ejecución a que hace referencia el art. 8, apartado 3, o sea que cumplan con las especificaciones técnicas mínimas, las normas y los procedimientos con referencia a los niveles de seguridad bajo, sustancial y alto.
> d) que el Estado garantice que los datos de ID de la persona se atribuyen de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente conforme al art. 8, apartado 3 nuevamente, a la persona física o jurídica a la que se refiere el art. 3, punto 1,

e) que la parte que expide los medios de identificación electrónica garantice que los medios de ID electrónica se atribuyan a la persona conforme al art. 8, apartado 3.
f) el Estado miembro que efectúa la notificación debe garantizar la disponibilidad de la autenticación en línea de manera que cualquier otro Estado miembro pueda confirmar los datos de ID (art. 7).

Respecto a este último punto, se deja establecido que la autenticación transfronteriza deberá ser gratuita cuando sea un servicio público y que no se impondrán requisitos técnicos específicos desproporcionados.

C. Niveles de seguridad de los sistemas de identificación electrónica

El art. 8 del reglamento es el que establece los niveles de seguridad que deben cumplir los sistemas de ID.

Un sistema de identificación electrónica que sea notificado por un Estado miembro deberá especificar los niveles de seguridad bajo, sustancial y alto para los medios de identificación electrónica.

En este artículo se establecen tres niveles de seguridad, el bajo, sustancial y alto, que cumplirán los siguientes criterios:

El nivel de seguridad bajo es un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad.

Por su parte, el nivel de seguridad sustancial es igual al primero solo que establece un grado sustancial y superior al bajo.

Por su parte el nivel de seguridad alto establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial.

El art. 11 del reglamento establece la responsabilidad en la que incurrirá el estado miembro y las partes de los perjuicios ocasionados a personas físicas y jurídicas.

El estado miembro que efectúa la notificación y la parte que expida los medios de identificación electrónica será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones. Estos daños ocasionados se aplicarán con arreglo a las normas nacionales sobre responsabilidad.

Por último, recordemos que la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de los medios de ID están establecidos en el Reglamento de ejecución 2015/1502 del Reglamento eIDAS.

VIII. Servicios de confianza en el Reglamento eIDAS

Como el propio Reglamento eIDAS indica, uno de sus principales objetivos es el de: "…eliminar las barreras existentes para el uso transfronterizo de los medios de identificación electrónica utilizados en los Estados miembros para autenticar al menos en los servicios públicos" (considerando 12).

El Reglamento eIDAS persigue, por tanto, asegurar la interoperabilidad por consiguiente la armonización en la UE: De la Identificación Electrónica (de personas y entidades), que acabamos de tratar en el capítulo anterior; y además de los Servicios de Confianza.

Opinamos que estos servicios son de vital importancia ya que engloban, además de la conocida firma electrónica, al sello electrónico, sellos del tiempo, servicios de entrega electrónica certificada y certificados de autenticación de sitio web. Por lo que a simple vista notamos que ya no se trata de una nueva normativa en materia de firma electrónica, sino un marco legal muchísimo más avanzado y completo.

Por lo tanto, decimos que los "servicios electrónicos de confianza" establecidos en el reglamento son otro concepto central del mercado único digital, que pretende eliminar las barreras al comercio electrónico y a todo tipo de transacciones electrónicas entre los diferentes estados miembros de la U.E.

Volviendo a la definición de lo que entiende el Reglamento eIDAS como "servicio de confianza", este el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en la creación, verificación y validación de firmas

electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o la creación, verificación y validación de certificados para la autenticación de sitios web, o la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

También recordemos que estos servicios pueden ser cualificados si cumplen los requisitos específicos establecidos en el reglamento para otorgarles este nivel.

Los Servicios de Confianza son una novedad que introduce el Reglamento eIDAS, con el fin de incrementar los niveles de confianza y denominando "prestadores de servicios de confianza" a los "prestadores de servicios de certificación", de la antigua Directiva.

El reglamento trata los Aspectos Internacionales garantizando que

> Los servicios de confianza prestados por los prestadores de servicios de confianza establecidos en un tercer país serán reconocidos como legalmente equivalentes a los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la Unión si los servicios de confianza originarios del tercer país son reconocidos en virtud de un acuerdo celebrado entre la Unión y el tercer país en cuestión… (art. 14).

A través de esto último, se buscaba la armonización internacional de los servicios de confianza, algo conseguido en el territorio de la U.E.

A. Firma electrónica

Ya tratamos bastante la herramienta electrónica por excelencia junto con el documento electrónico, "la firma electrónica", por lo que consideramos que no será necesario sobreabundar mucho en el tema. Aun así, trataremos la firma electrónica en el Reglamento eIDAS.

La regulación de la firma electrónica en la U.E está incorporada en el Capítulo I, artículo 3 del Reglamento eIDAS, y de acuerdo con este, se entiende por firma electrónica a los datos en formato electrónico anexos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

La Directiva 1999/93/CE, definía la firma electrónica como:

“Los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación” por lo que no se aparta demasiado de su concepto” (art. 2.1).

Por ello, el reglamento contempla tres tipos de firma electrónica en función de los distintos niveles de seguridad que aporten:

“Firma electrónica”, en este caso se refiere a la firma electrónica simple.

La “Firma electrónica avanzada” por su parte, es tratada en el reglamento yendo un paso más allá y permitiendo utilizar las últimas tecnologías, ya sea hardware o servicios en la nube. Este último punto queda aclarado en el artículo 3.22 del reglamento que establece la necesidad de utilización de: “un equipo o programa informático configurado que se utiliza para crear una firma electrónica”.

Es la firma electrónica que conocemos en la legislación argentina como firma digital, la que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere.

Por último, el reglamento nos trae también a la “firma electrónica cualificada”. En este caso, la diferencia de la firma electrónica cualificada es que se trata de una firma electrónica basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Este “dispositivo cualificado de creación de firma electrónica”, es un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del reglamento.

En el art. 25 del reglamento encontramos a los efectos jurídicos de las firmas electrónicas.

En el primer apartado se establece que no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.

Todo esto es en consonancia con el del reglamento que dice

> El presente Reglamento debe establecer el principio de que no se deben denegar los efectos jurídicos de una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla todos los requisitos de la firma electrónica cualificada (considerando 49).

Recordemos que, para la obtención de la firma electrónica, los requisitos son menos severos, lo que la hace mucho más fácil de obtener y por consiguiente más implementada. En miras de tal situación, la firma electrónica igualmente gozará de validez legal, solo que esta no tendrá los beneficios de la firma electrónica avanzada o de la cualificada.

En materia probatoria recordemos también que la firma electrónica no cuenta con la presunción iuris tantum con la que goza la firma electrónica avanzada. Más allá de eso, los usos y costumbres y su practicidad hacen que sea la más utilizada en todos los ecosistemas digitales del mundo.

Por lo que decimos que este artículo solo viene a reforzar uno de los principios establecidos en materia de firma electrónica y establecidos en el reglamento

> … Sin embargo, corresponde a las legislaciones nacionales determinar los efectos jurídicos de las firmas electrónicas en los Estados miembros, salvo para los requisitos establecidos en el presente Reglamento según los cuales una firma electrónica cualificada debe tener el efecto jurídico equivalente a una firma manuscrita (considerando 49).

En el segundo apartado del reglamento, se establece que una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma ológrafa, estableciendo así el principio de equivalencia entre la firma electrónica avanzada y la firma ológrafa consagrada a nivel internacional hace ya mucho tiempo.

Por último, en el tercer apartado establece que una firma electrónica cualificada emitida en un estado miembro será reconocida como una firma electrónica cualificada en todos los demás estados miembros de la U.E.

El art. 26 por su parte establece los requisitos para que una firma electrónica sea considerada una firma electrónica avanzada.

Recordemos que previamente en las definiciones del art. 3 ya las define con este imperativo, estableciendo que si cumple los requisitos del art. 26 será considerada firma electrónica avanzada. Por lo tanto, los requisitos son los siguientes:

Debe estar vinculada al firmante de manera única, debe permitir la identificación del firmante, debe haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar con un alto nivel de confianza y bajo su

control exclusivo, y por último debe estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Tal como ya mencionamos, en el Anexo II encontramos los requisitos de los dispositivos cualificados de creación de firma electrónica del Reglamento eIDAS.

Estos certificados de firma electrónica cualificados sólo pueden ser emitidos por Autoridades de Certificación acreditadas que reúnan los requisitos del reglamento.

B. Sellos electrónicos

Uno de los servicios de confianza tratados por el Reglamento eIDAS, son los sellos electrónicos.

Podemos establecer, que un sello electrónico es una pieza de datos añadidos a un documento electrónico u otro dato, que asegura el origen de los datos y la integridad en el caso de ser cualificado. Estos sellos funcionan de manera similar al estampado físico en documentos en papel solo que, en este caso, en documentos electrónicos.

Recordemos que los sellos electrónicos según el Reglamento eIDAS, son datos en formato electrónico anexos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

En él nos da una pauta estableciendo en el que: “Los sellos electrónicos deben servir como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento” (considerando 59).

Por lo tanto, decimos que estos sellos electrónicos son utilizados por personas jurídicas para sellar electrónicamente documentos de la misma manera que las personas físicas lo hacen con la firma electrónica.

De manera parecida a lo que sucede en la firma electrónica, este cuenta con diferentes tipos de sellos electrónicos dependiendo si cumple o no los requisitos establecidos para considerarse, sello electrónico simple, avanzado o cualificado de la misma manera que sucede con la firma electrónica.

El art. 35 de la sección 5 del reglamento, trata los efectos jurídicos del sello electrónico y son los siguientes:

En primer término, se establece que no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado. Algo lógico ya que en varias oportunidades mencionamos que el hecho de que sea solo electrónico, igualmente tendrá efectos jurídicos y sumada la cualificación que dará más beneficios y seguridad.

Un sello electrónico cualificado disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos que se sellaron. Por lo tanto, se incorpora integridad al sello cualificado.

Además, un sello electrónico cualificado basado en un certificado cualificado emitido por estado miembro será reconocido en todos los demás estados miembros.

Un sello electrónico será avanzado si cumple los requisitos contemplados en el art. 36 y un sello electrónico será cualificado si se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.

Esto va en consonancia con el del reglamento cuando dice lo siguiente: “para contribuir al uso transfronterizo general de los servicios de confianza, debe ser posible utilizarlos como prueba en procedimientos judiciales en todos los Estados miembros” (considerando 22).

El Reglamento eIDAS establece los requisitos para que los sellos electrónicos sean considerados avanzados

> Debe estar vinculado al creador del sello de manera única; Debe permitir la identificación del creador del sello; Desde haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo, y debe estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable (art. 36).

Para cerrar, en el Anexo III del reglamento encontramos los requisitos para que un sello electrónico sea cualificado.

C. Sello de tiempo electrónico

El sello de tiempo electrónico es introducido de manera novedosa por el Reglamento eIDAS, el mismo sirve para demostrar que una serie de datos han existido y permanecen inalterados desde un punto específico en el tiempo. El sello del tiempo se conoce también como marca temporal, registro de tiempo, cronomarcador o también en inglés como *time stamp*.

El servicio de confianza del sellado de tiempo electrónico se encuentra dentro del proceso de firmas electrónicas avanzadas y generalmente es un servicio adicional que prestan las autoridades de certificación o autoridades que brindan servicios de confianza, es por ello que el legislador consideró pertinente incluirlo dentro del reglamento como un servicio aparte. Al existir muchos estándares involucrados en este tipo de sellado, el reglamento va a armonizar los estándares válidos en él.

Por lo tanto, decimos a grandes rasgos, que un tercero de confianza va a ser el que dará fe o certificará de la fecha y hora exacta de una transacción electrónica incorporando este dato en el documento.

El sello de tiempo electrónico se encontraba definido en el art. 3 del reglamento, como los datos en formato electrónico que vinculan otros datos con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

También nos introduce el sello cualificado de tiempo electrónico. En este caso, el sello electrónico para que sea cualificado debe cumplir con los requisitos establecidos en el art. 42 del reglamento: vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte;

Debe basarse en una fuente de información temporal vinculada al tiempo universal coordinado, y haber sido firmada mediante el uso de una firma electrónica avanzada o sellada con un sello electrónico avanzado del prestador cualificado de servicios de confianza o por cualquier método equivalente.

El tiempo universal coordinado o también conocido con sus siglas en inglés como UTC es el principal estándar de tiempo por el cual el mundo regula los relojes y el tiempo y es el lógicamente seleccionado por el legislador de la U.E para vincular

este servicio de confianza UTC. Este sistema de tiempo está seleccionado por muchos estándares de Internet y la WWW.

El art. 41 de la sección 6 del reglamento trata efectos jurídicos de los sellos de tiempo electrónicos.

En primer término, se establece que no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello de tiempo electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de sello cualificado de tiempo electrónico. De igual manera que en los anteriores servicios de confianza del reglamento.

Los sellos cualificados de tiempo electrónicos disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas.

Por último, se establece que un sello cualificado de tiempo electrónico emitido en un estado miembro será reconocido como sello cualificado de tiempo electrónico en todos los estados miembros. Por lo que decimos que prevalece el uso transfronterizo general de los servicios de confianza en esta herramienta.

D. Servicio de entrega electrónica certificada

Los servicios de entrega electrónica certificada son introducidos novedosamente también por el reglamento, los mismos son definidos en el art. 3 ya mencionado, por lo que concluimos que se trata de un servicio que permite transmitir datos entre partes y aportar pruebas relacionadas con la gestión de estos datos, incluida la prueba del envío y la recepción de los datos, y que protege los datos frente a los riesgos de pérdida, robo, deterioro o alteración. Se conoce también por sus siglas en inglés QERDS, de *Qualified Electronic Registered Delivery Service* [Servicio de Entrega Registrado Electrónico Calificado].

Por otra parte, tenemos el servicio cualificado de entrega electrónica certificada, un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el art. 44.

Este artículo del Reglamento eIDAS establece los requisitos para que estemos frente a un servicio cualificado de entrega electrónica certificada

> Debe ser prestado por uno o más prestadores cualificados de servicios de confianza; Debe asegurar con un alto nivel de fiabilidad la identificación del remitente; Debe garantizar la identificación del destinatario antes de la entrega de los datos; Deben estar protegidos el envío y recepción de datos por una firma electrónica avanzada o un sello electrónico avanzado de un prestador cualificado de servicios de confianza de tal forma que se impida la posibilidad de que se modifiquen los datos sin que se detecte; Debe indicar claramente al emisor y al destinatario de los datos cualquier modificación de los datos necesarios a efectos del envío o recepción de los datos; Debe indicar mediante un sello cualificado de tiempo electrónico la fecha y hora de envío, recepción y eventual modificación de los datos (art. 44).

Volviendo hacia atrás el art. 43 del reglamento nos daba los efectos jurídicos de un servicio de entrega electrónica certificada de la U.E.

A los datos enviados y recibidos mediante un servicio de entrega electrónica certificada no se les denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales por el mero hecho de que estén en formato electrónico o no cumplan los requisitos de servicio cualificado de entrega electrónica certificada. Tal como sucede en los anteriores Servicios de confianza que tratamos hasta este punto.

Los datos enviados y recibidos mediante un servicio cualificado de entrega electrónica certificada disfrutarán de la presunción de la integridad de los datos, el envío de dichos datos por el remitente identificado, la recepción por el destinatario identificado y la exactitud de la fecha y hora de envío y recepción de los datos que indica el servicio cualificado de entrega electrónica certificada.

E. Autenticación de sitios web

El Reglamento eIDAS introduce también esta novedosa herramienta dentro de los servicios de confianza, definida en el art. 3 por lo que entendemos que un certificado de autenticación de sitio web, es una declaración que permite autentificar un sitio web y vincularlo con la persona física o jurídica.

Al igual que otros servicios de confianza del reglamento este puede ser cualificado cuando se cumplen determinados requisitos.

En este caso para que un certificado sea cualificado de autenticación de sitio web, debe ser expedido por un prestador cualificado de servicios de confianza que cumpla con los requisitos establecidos en el anexo IV.

Es así que en el art. 45 se van a establecer los requisitos que deben reunir los certificados cualificados de autenticación de sitios web. Primero se establece que los certificados cualificados de autenticación de sitios web cumplirán los requisitos establecidos en el anexo IV. Después se establece que la Comisión de la U.E podrá establecer números de referencia de normas relativas a los certificados cualificados de autenticación de sitios web. Se presumirán cumplidos los requisitos establecidos en el anexo IV cuando un certificado cualificado de autenticación de sitios web se ajuste a esto último.

IX. Los Servicios de confianza cualificados

Los servicios de confianza calificados se encuentran en la Sección 3 del Reglamento eIDAS, en el que se van a establecer la supervisión de los prestadores cualificados de servicios de confianza; el inicio de un servicio de confianza cualificado; las listas de confianza; la etiqueta de confianza «UE» para servicios de confianza cualificados; y por último el art. 24 establece los requisitos para los prestadores cualificados de servicios de confianza.

Recordemos que el reglamento definía en el art.3 al prestador de servicios de confianza, como al prestador de uno o varios servicios de confianza cualificados y que el organismo de supervisión ha concedido la cualificación.

Destacamos la introducción de la mencionada “etiqueta de confianza de la U.E. para servicios de confianza cualificados” que la encontramos en el art. 23 del reglamento. Para garantizar y permitir verificar este tipo de servicios y transacciones de confianza se implementa una etiqueta, en este caso la etiqueta de confianza de la U.E para servicios de confianza cualificados que se visualiza al momento de acceder a dicho servicio.

> … debe crearse una etiqueta de confianza «UE» que identifique los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza. Esta etiqueta de confianza «UE» para los servicios de confianza cualificados diferenciaría claramente los servicios de confianza cualificados de otros servicios de confianza, contribuyendo así a mejorar la transparencia del mercado… (considerando 47).

Podrán acceder a esta etiqueta de confianza los prestadores cualificados incluidos en la lista del art. 22. Estos son los que se encuentran en las listas de confianza y que se publican cumpliendo con lo dispuesto en el artículo 23.1. del reglamento.

Cabe destacar que para ser reconocido en la U.E como un prestador de servicios de confianza y poder expedir servicios cualificados con los alcances del reglamento tal como se establece

> Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios electrónicos de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado (art. 24).

X. Documentos electrónicos en el Reglamento eIDAS

Opinamos nuevamente que uno de los principales protagonistas, sino el principal, es el documento electrónico.

En el Reglamento eIDAS, encontramos un apartado completo para los documentos electrónicos, además, donde trata los efectos jurídicos de los documentos electrónicos, se establece de igual manera que se encuentra en los considerandos que: “No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero hecho de estar en formato electrónico” (art. 46).

La consagración de este principio encuentra su fundamento en el principio de equivalencia funcional consagrado a nivel internacional.

En el art. 3 del reglamento, donde encontramos todas las definiciones ya lo define como a todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual.

Por otro lado, también lo encontramos como pieza fundamental estableciendo lo siguiente

> Los documentos electrónicos son importantes para que sigan desarrollándose las transacciones electrónicas transfronterizas en el mercado interior. El presente Reglamento debe establecer el principio de que no se deben denegar efectos jurídicos a un documento electrónico por el mero hecho de estar en formato electrónico al objeto de garantizar que no se rechazará una transacción electrónica por el mero hecho de que el documento está en formato electrónico (considerando 63).

XI. Disposiciones finales

Dentro de las disposiciones finales del reglamento encontramos cuatro artículos que van a tratar cuestiones administrativas, donde se establecen en primer término la “revisión” que debía sufrir la norma conforme a las experiencias que van surgiendo, todo ello dio como resultado la propuesta de modificación que trataremos más adelante. Actualmente la propuesta de modificación del Reglamento eIDAS se basa en la información recopilada de la consulta a las partes interesadas en vista de la obligación de tal revisión establecida en el art. 49.

También contiene la derogación de la Directiva 1999/93/CE con efectos a partir del 1 de julio de 2016 y medidas transitorias también con respecto a servicios otorgados en la misma directiva.

Por último, se encuentra la entrada en vigor del reglamento, situación que aconteció el 1 de julio de 2016.

XII. Anexos del Reglamento elDAS

El Reglamento contiene 4 anexos los cuales son los encargados de: I requisitos de los certificados cualificados de firma electrónica, II requisitos de los dispositivos cualificados de creación de firma electrónica, III requisitos de los certificados cualificados de sello electrónico y IV requisitos de los certificados cualificados de autenticación de sitios web.

Destacamos el primer anexo, donde se establecen los requisitos que deben contener los certificados cualificados de firma electrónica

a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica;
b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales, para personas físicas, el nombre de la persona;
c) al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;
d) datos de validación de la firma electrónica que correspondan a los datos de creación de la firma electrónica;
e) los datos relativos al inicio y final del período de validez del certificado; f) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;
g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;
h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);
i) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;
j) cuando los datos de creación de firma electrónica relacionados con los datos de validación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático (Anexo I).

Como podemos apreciar los mismos abundantes, sin embargo, la practica demostró su eficacia en la U.E.

XIII. Modificación al Reglamento eIDAS. Perspectivas y futuro del Reglamento EIDAS

El 3 de junio del 2021, en plena marcha de elaboración de la presente tesis, la Comisión Europea presentó en Bruselas la “Propuesta de modificación del Reglamento (UE) 910 eIDAS”. El título completo de la misma es “Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento de un marco para

una identidad digital europea (SEC (2021) 228 final) - (SWD (2021) 124 final) - (SWD (2021) 125 final)".

Decimos que por ahora se trata de una propuesta de modificación, por lo que el Reglamento eIDAS se mantiene vigente y sin cambios, mientras que la comisión comienza a trabajar y negociar con los estados miembros de la U.E, situación que debería concluir como máximo en septiembre del año 2022.

La Comisión Europea en su programa de trabajo propuso la identidad digital europea, mencionada en el Discurso sobre el estado de la Unión (2021) en el cual se pronuncia lo siguiente

> Esta es la razón por la que la Comisión propondrá en breve una identidad electrónica europea segura. Una en la que confiemos y que cualquier ciudadano pueda utilizar en cualquier lugar de Europa para cualquier operación, desde el pago de sus impuestos hasta el alquiler de una bicicleta. Una tecnología con la que nosotros mismos podamos controlar qué datos compartimos y cómo se utilizan.

En la exposición de motivos, la modificación del Reglamento eIDAS menciona que el Reglamento eIDAS y la identidad electrónica incluida en el mismo, solo se limitó a tratar en su articulado al sector público, además este no cubrió todas las soluciones de identidad. Además, menciona que no todos los Estados miembros proporcionaron soluciones de identificación electrónica notificadas. Esto, junto con el hecho de que no todos los nodos técnicos del marco de interoperabilidad eIDAS están en pleno funcionamiento, significaba que el acceso transfronterizo era limitado.

La Propuesta de modificación del Reglamento eIDAS (2021), en el apartado Contexto de la Propuesta, Razones y objetivos de la propuesta, menciona lo siguiente

> Lo que está surgiendo en el mercado es un nuevo entorno en el que el enfoque ha pasado de la provisión y el uso de identidades digitales rígidas a la provisión y dependencia de atributos específicos relacionados con esas identidades. Existe una mayor demanda de soluciones de identidad electrónica que puedan ofrecer estas capacidades proporcionando ganancias de eficiencia y un alto nivel de confianza en toda la UE, tanto en el sector público como en el privado, basándose en la necesidad de identificar y autenticar a los usuarios con un alto nivel de garantía (punto 1).

El marco regulatorio para la prestación de servicios de confianza del Reglamento eIDAS es tal como mencionamos uno de los más avanzados y completos en su categoría, sin embargo, algunos servicios de confianza no se encontraban comprendidos en la norma.

La evaluación efectuada por la Comisión del Reglamento eIDAS, reveló que el marco legal actual no logra abordar las nuevas demandas del mercado, debido a sus limitaciones inherentes al sector público, la complejidad para que los proveedores privados en línea se conecten al sistema, su insuficiente disponibilidad de soluciones de identificación electrónica notificadas en todos los estados miembros y su falta de flexibilidad para admitir una variedad de casos de uso. Además, las soluciones de identidad que quedan fuera del alcance de eIDAS, como las que ofrecen los proveedores de redes sociales y las instituciones financieras, plantean problemas de privacidad y protección de datos.

Desde la entrada en vigor de la parte del reglamento, sólo 14 estados miembros han notificado al menos un sistema de identificación digital. Como resultado, solo el 59% de los residentes de la UE tienen acceso a esquemas de identificación electrónica confiables y seguros a través de las fronteras.

La propuesta no sustituye el Reglamento eIDAS, solo lo modifica razón por la cual podríamos decir que se trata de un eIDAS 2.0 y uno de los cambios más novedosos es la introducción de una “cartera de identidad digital europea”. Por ello la modificación del Reglamento, se realiza también con el objetivo de que los ciudadanos de la U.E dispongan de carteras digitales que permitan acceder a servicios online en toda Europa además de permitir a los estados miembros mantener su antiguo sistema.

La propuesta para modificar el Reglamento eIDAS el art. 3 nos trae las “carteras de identidad digital”

> … un producto y servicio que permite al usuario almacenar datos de identidad, credenciales y atributos vinculados a su identidad, para proporcionarlos a las partes que confían cuando lo soliciten y utilizarlos para la autenticación, en línea y fuera de línea, para un servicio de conformidad con el artículo 6 bis; y crear sellos y firmas electrónicas cualificadas (Art. 1 (3) (i)).

Dentro de la propuesta encontramos que se sustituye el Capítulo II del reglamento insertándose las carteras europeas de identidad digital.

El nuevo art. 6 bis establece con el fin de garantizar que todas las personas físicas y jurídicas de la U.E tengan un acceso seguro, confiable y sin problemas a los servicios públicos y privados transfronterizos, además que cada Estado miembro emitirá una cartera de identidad digital dentro de los doce meses siguientes a la entrada en vigor de la Propuesta.

Las carteras europeas de identidad digital serán emitidas por un estado miembro de la U.E, pero siempre que sean reconocidas por un estado miembro. Estas permitirán al usuario de las mismas la posibilidad de solicitar y obtener, almacenar, seleccionar, combinar y compartir de forma segura, de manera transparente y rastreable por el usuario, los datos de identificación de persona jurídica necesarios y la atestación electrónica de atributos para autenticarse online, así como también offline con el fin de utilizar en línea público y privado servicios. Además, de la posibilidad de firmar mediante firma electrónica cualificada a través de esta nueva herramienta.

Esta modificación en la identidad digital europea estará a disposición de todos los ciudadanos y empresas de la U.E, de tal manera que a través de sus carteras digitales los ciudadanos puedan demostrar su identidad y compartir documentos electrónicos, además de otros certificados personales como por ejemplo registro de conducir, etc.

El uso de las carteras europeas de identidad digital será gratuito para las personas físicas de la U.E., el mismo quedará siempre a discreción del usuario y además tendrá pleno control sobre los datos. Es importante remarcar que garantizará el control del ciudadano de sus datos, pues estas carteras de identidad digital europea les permitirán elegir qué aspectos de su identidad, datos y certificados comparten con terceros. Este control por los usuarios garantiza que solo se comparta aquella información que realmente deba compartirse respetando siempre el RGPD, el Reglamento 2016/679 de la U.E.

Por otro lado, la modificación del Reglamento eIDAS también va a introducir tres nuevos servicios de confianza.

El primero de los servicios de confianza introducido es el archivo electrónico de documentos electrónicos, siendo este un servicio que garantiza la recepción, el almacenamiento, la eliminación y la transmisión de datos o documentos electrónicos con el fin de garantizar su integridad, la exactitud de su origen y las características legales durante todo el período de conservación.

Además, introduce la gestión de dispositivos de creación de sellos y firmas electrónicas remotas, insertándose los siguientes puntos (23a) y (23b) respectivamente. Con respecto al último, se trata de un dispositivo de creación de firma electrónica cualificado en el que un proveedor de servicios de confianza cualificado genera, gestiona o duplica los datos de creación de firma electrónica en nombre de un firmante.

Por su parte, el dispositivo de creación de sellos electrónicos cualificados en el que un proveedor de servicios de confianza cualificado genera, gestiona o duplica los datos de creación de firmas electrónicas en nombre de un creador de sellos. Por último, también se incorpora el registro de datos electrónicos en un libro de contabilidad electrónico: Este es un registro electrónico de datos a prueba de manipulaciones, que proporciona autenticidad e integridad de los datos que contienen, precisión de su fecha y hora y de su ordenamiento cronológico.

“La notificación voluntaria anterior de los sistemas de identificación electrónica se convierte en una obligación para los Estados miembros de notificar al menos un sistema de identificación electrónica que incluya al menos un medio de identificación” (propuesta de artículo 1 (9)).

También se introduce la obligación de que los Estados miembros incluyan en el conjunto mínimo de datos de identificación de personas un identificador único y persistente (propuesta de artículo 1 (12)).

También destacamos que, debido a la naturaleza de la identificación electrónica, la propuesta modificatoria del eIDAS incluye muchas referencias a otras leyes ya existentes de la U.E, por ejemplo, el Reglamento (UE) 2016/679 que el Reglamento eIDAS no mencionaba por su posterior promulgación.

El art. 15 acerca de la accesibilidad para personas con discapacidad también es sustituido en el reglamento, estableciéndose que la prestación de servicios de

confianza y productos para el usuario final será accesible para las personas con discapacidad de conformidad con los requisitos de accesibilidad del anexo I de la Directiva 2019/882 del año 2019. El objetivo de esta última Directiva es contribuir al correcto funcionamiento del mercado mediante la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en lo relativo a los requisitos de accesibilidad exigibles a determinados productos y servicios en la U.E. como por ejemplo equipos informáticos, terminales de autoservicio, terminales de pago, cajeros automáticos, máquinas expendedoras de billetes, máquinas de facturación, etc.

Para finalizar, la propuesta de modificación del Reglamento eIDAS, establece que los estados miembros deben crear un conjunto común de herramientas a partir desde que se presenta hasta septiembre de 2022. Este conjunto de herramientas debe incluir la arquitectura y las normas técnicas, así como directrices de mejores prácticas que normalmente y con terminología técnica se le dicen *Toolkits* [kit de herramientas].

XIV. Conclusión

Conocimos el impacto del Reglamento eIDAS, el cual cambió todos los paradigmas existentes en la U.E. en materia digital, paradigmas que consideramos, promovían la falta de interoperabilidad transnacional en el mercado digital de la U.E.

Como pudimos apreciar, antes de la promulgación del Reglamento eIDAS, en cada estado miembro de la U.E, los certificados electrónicos emitidos para firmar electrónicamente no eran válidos entre países a menos que haya un convenio entre ambos países, esto es la entidad emisora del certificado digital y el país de destino.

Conocimos también como la Comisión de la U.E a través de proyectos como el del Mercado único Digital en consonancia con el Reglamento eIDAS, lograron aumentar la eficacia de los servicios públicos y privados online, así como también lograron potenciar el comercio electrónico en el territorio europeo.

Pero el Reglamento eIDAS no solo armoniza las firmas electrónicas, sino que va más allá, introduciendo el término servicios de confianza y englobando todas las

herramientas digitales similares dentro del ámbito de la confianza digital, como por ejemplo firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o la creación, verificación y validación de certificados para la autenticación de sitios web, todos ellos armonizados y enmarcados logrando la legislación más disruptiva y evolucionada del mundo en esta materia.

Por otro lado, identificamos los aspectos principales fundamentales del reglamento, el cual termina demostrando su utilidad y su total acierto, en un contexto internacional donde se hizo necesaria toda regulación posible y acompañamiento en materia digital por parte de los estados, ni hablar de la revolución exponencial de la digitalización durante la pandemia ocasionada por el Covid 19.

Mencionamos esto porque a diferencia de lo que sucede en el resto de los bloques regionales como el nuestro, que no cuentan con una regulación similar, demuestran la importancia del interrogante suscitado y que trataremos de responder con esta investigación al compararlo con la legislación del MERCOSUR.

La LFD Argentina y sus normas complementarias no contienen dentro de sus artículos algún vestigio de autoridades de creación, verificación y validación de sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o la creación, verificación y validación de certificados para la autenticación de sitios web, o la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios. Sin embargo, el art. 17 de dicha ley, menciona la posibilidad de que se brinden otros servicios de certificación relacionados con la firma digital, entre los cuales se pueden incluir los servicios de confianza del reglamento.

Tampoco encontramos en los Acuerdos y Decisiones del MERCOSUR algo al respecto, no existen otros servicios de confianza o servicios de certificación relacionados a la firma electrónica a excepción de la firma electrónica en sí entre los países miembros, así como tampoco existe artículo alguno en materia de estandarización o armonización en materia de Identificación electrónica de los ciudadanos de los estados miembros.

Por último, identificamos y conocimos la reciente Propuesta de Reglamento del Parlamento Europeo y del Consejo que propone modificar el Reglamento 910/2014 incorporando muchísimas cosas nuevas.

Las novedades introducidas por el Reglamento eIDAS sentaron las bases de una seguridad y confianza digital sin precedentes, que permitieron que la U.E. pudiese ocuparse de otros temas importantes en materia digital, que van desde el RGPD, reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, e incluso a temas tan disruptivos como la I.A con el trabajo en constante desarrollo de la Comisión Europea siendo de los primeros en crear una regulación sobre la materia en el mundo.

Capítulo VI

Marco Metodológico

I. Introducción

En este capítulo trataremos las características y la metodología utilizada en el desarrollo de la presente tesis doctoral, también vamos estableceremos las técnicas y los instrumentos aplicados, además del procedimiento que empleamos de recopilación de información.

En los anteriores capítulos tratamos los elementos teóricos de la investigación los cuales nos permitieron dar cuenta del cumplimiento de los objetivos, ya sean específicos o generales y así dar con la respuesta a la pregunta de esta investigación.

> En principio lo que debimos hacer es identificar la problemática. Lo esencial consistió en realizar el planteo del problema mediante un lenguaje claro, sin ambigüedades ni vaguedades, de modo preciso delimitándose adecuadamente el espacio físico-geográfico, la temporalidad, la semántica a través de la determinación de los conceptos centrales, aludiendo al interés esperado mediante la especificación de los objetivos generales y secundarios que se deseaban alcanzar; y puntualizando los recursos disponibles (Heinz Dietrich, 1996, p.57).

Por su parte el objeto de estudio son la firma electrónica y sus legislaciones. El campo de investigación de la presente tesis doctoral, se encuadra dentro del derecho informático y del derecho civil privado.

II. Antecedentes de la investigación

El eje central en cual centramos la tesis doctoral es la firma electrónica y la digital. Se hace necesario sumarle, por ejemplo, la infraestructura y los andamiajes normativos que sostienen los ecosistemas digitales de los países tratados y de los procesos de integración regionales.

Por ello, después de realizar una investigación a nivel nacional, regional e internacional con el fin de encontrar una investigación similar a nuestro trabajo, podemos decir que la misma es original.

Seguimos a Hernández Sampieri et al. (2014)

> No investigar sobre algún tema que ya se haya estudiado a fondo. Esto implica que una buena investigación debe ser novedosa, lo cual puede lograrse al tratar un tema no estudiado, profundizar poco en uno medianamente conocido, o darle una visión diferente o innovadora a un problema aunque ya se haya examinado repetidamente … (p.26).

Por otro lado, afirmamos que este trabajo es actual. Esto último responde a la naturaleza de constante avance del derecho informático y de las tecnologías.

III. Planteamiento del problema y justificación

El eje central en cual centramos la presente tesis doctoral es la firma electrónica y además se hizo necesario sumar, por ejemplo, los andamiajes normativos que sostienen los ecosistemas digitales. El análisis del derecho comparado nos permitió conocer nuevos paradigmas en materia de firma electrónica y la incorporación de nuevos institutos como por ejemplo los servicios electrónicos que engloban a su vez más herramientas de este estilo.

Por su parte, decimos que el problema que traemos en cuestión surge dentro del MERCOSUR, más específicamente en cuestión normativa regional, donde cada país integrante interpreta a su manera la firma electrónica, firma electrónica avanzada o firma digital.

Las normas que regulan las firmas electrónicas han sido establecidas en nuestra legislación, así como en el resto del mundo con el objeto de facilitar de manera segura e inmediata la firma de documentos electrónicos como prueba de la autoría de la declaración de voluntad. La firma electrónica a nivel internacional también logró agilizar y dar seguridad jurídica a los procesos y las operaciones que utilicen este medio.

Sostenemos que los efectos jurídicos de la firma digital y de la firma electrónica, se dispone de manera diferente puesto que cada país integrante del MERCOSUR diferencia la manera en que se van a implementar estas firmas electrónicas lo cual es un problema que genera un atraso con respecto a otras legislaciones del derecho comparado.

Contrariamente, la U.E cuenta con el Reglamento eIDAS con todo su andamiaje legal, en cuanto a la identificación electrónica de sus firmantes, las pautas para la generación de los servicios de confianza y que sean comunes para los integrantes, asimismo como una base común para la interacción electrónica entre los ciudadanos, empresas y autoridades públicas de los países miembros.

A grandes rasgos, decimos que las normas analizadas, las instituciones del derecho informático que tratamos, el impacto que está teniendo a nivel local, regional y mundial nos permite imbuirnos de los conocimientos necesarios para así, dar respuestas a las principales cuestiones de la presente tesis doctoral.

Así exponemos nuestras razones, tal como refieren Hernández Sampieri et al. (2014): “Justificación de la investigación Indica el porqué de la investigación exponiendo sus razones. Por medio de la justificación debemos demostrar que el estudio es necesario e importante” (p.40).

En consecuencia, el interrogante que ello suscita y que tratamos de responder con esta investigación es: ¿Por qué existen barreras en cuanto a la firma electrónica en el MERCOSUR? ¿Cómo armonizar las legislaciones en torno a firmas electrónicas en el MERCOSUR?

IV. Tipo de investigación

Realizamos la investigación a través del tipo de investigación de estudios explicativos.

El estudio se basó en bases prioritariamente normativas, y se limita en tal sentido el campo de investigación. Los escasos aspectos pragmáticos son de acuerdo a la naturaleza de la materia a tratar.

Se incluyeron análisis comparativos y deductivos.

Por otra parte, realizamos la investigación a través de un diseño no experimental, ya que en la presente tesis observamos los fenómenos tal y como ocurren, sin intervenir en su desarrollo.

V. Unidades de análisis.

Las unidades de análisis que consideramos son la LFD Argentina, el CCyCN, las normas complementarias, así como también los decretos reglamentarios de la LFD.

Por otro lado, tenemos la Ley Modelo sobre las Firmas Electrónicas de la CNUDMI que sirve de modelo a las legislaciones en Latinoamérica y casi en todo el mundo en materia de legislaciones de firma electrónica.

También son unidades de análisis las diferentes normas que regulan la firma electrónica de los países que integran el MERCOSUR, sus países asociados y las emanadas del MERCOSUR como organismo.

Por último, también tenemos en la U.E al actual Reglamento eIDAS y la antigua Directiva de la U.E acerca de firma electrónica.

Las variables de análisis son completitud, coherencia, lagunas jurídicas, y las incongruencias normativas de las legislaciones tratadas.

En cuanto al objeto en análisis, este tiene como beneficiarios directos los ciudadanos integrantes de la comunidad del MERCOSUR.

VI. Criterio de selección de casos

Elegimos analizar con mayor énfasis los países miembros del MERCOSUR y sus países asociados porque representan los distintos sistemas instaurados en Latinoamérica con relación a la ley de firma digital y electrónica. También elegimos analizar la legislación como organismo del MERCOSUR en materia de firma electrónica. Por último, elegimos y analizamos la legislación emanada por la comisión de la U.E, el Reglamento elDAS por ser un importante paradigma en materia digital y referente a la materia.

VII. Técnicas e instrumentos

El abordaje que utilizamos en esta investigación fue el abordaje cualitativo. Seguimos en ello a Hernández Sampieri et al. (2014): “El enfoque cualitativo también se guía por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos …” (p.7).

Como técnica cualitativa utilizamos la observación indirecta a través del análisis de legislación, doctrina, jurisprudencia de nuestro país, de los países del MERCOSUR, sus estados asociados y de los miembros de la U.E.

VIII. Cumplimiento de Objetivos

En este punto explicaremos cómo dimos cumplimiento de los objetivos específicos a través de los cuales nos permitió cumplir con los objetivos generales y, por ende, dimos respuesta a la pregunta que gira en torno a la tesis.

Los objetivos específicos de la tesis fueron los siguientes:

1). Conocer la legislación, doctrina, jurisprudencia en el Mercosur y la U.E respecto de la ley de firma digital y firma electrónica.

2). Identificar los elementos fundamentales de la ley de firma digital y electrónica argentina, la de los países integrantes del Mercosur, y de sus estados asociados y la U.E.

3). Determinar el grado de adopción e implementación de la firma digital y de la firma electrónica en el Mercosur y la U.E.

4). Realizar una propuesta que contemple la armonización de la firma digital y firma electrónica de las diferentes legislaciones del Mercosur.

Estos objetivos específicos los cumplimos de la siguiente manera: El primero de los objetivos lo cumplimos, cuando se dio a conocer la legislación, doctrina en el Mercosur en el capítulo IV y la U.E respecto de la ley de firma digital y firma electrónica en el Capítulo V.

Por su parte el segundo objetivo específico, siendo el mismo el de identificar los elementos fundamentales de la LFD de la República Argentina, la de los países integrantes del MERCOSUR, de sus Estados asociados y de la U.E, fueron cumplimentados en los Capitulo III, Capitulo IV y Capítulo V.

Establecemos que para determinar el grado de adopción e implementación de la firma digital y de la firma electrónica en el MERCOSUR y la U.E, abordamos estos temas en los Capítulo IV y Capítulo V.

El último de los objetivos específicos lo cumplimos en el Capítulo VII donde se encuentran las propuestas del presente trabajo.

Los objetivos generales por su parte, son los siguientes:

1). Establecer por qué existen barreras en cuanto a la firma electrónica en el MERCOSUR.

2). Determinar cómo armonizar las legislaciones en torno a firmas electrónicas en el MERCOSUR.

Establecemos que, para cumplir el primer objetivo general del trabajo, necesitamos establecer por qué existen barreras en cuanto a la firma electrónica en el MERCOSUR, para lo cual fue necesario el cumplimento de los objetivos específicos primero, segundo y tercero.

El segundo objetivo general fue determinar “cómo armonizar las legislaciones en que versan sobre firma digital en el MERCOSUR”, para ello necesitamos la totalidad

de los capítulos desde el Capítulo I hasta el Capítulo VII donde dimos cumplimiento con la pregunta principal, algo que respondemos con la conclusión y con la propuesta de nuestra tesis.

IX. Hipótesis

Decimos que, para hablar de la hipótesis del presente trabajo, explicaremos qué tipo de hipótesis es la que sometimos a prueba convirtiéndola en nuestra tesis el trabajo de investigación.

Seguimos de cerca a Heinz Dietrich (1996) a los fines de identificar que nuestra hipótesis se trata de una hipótesis de constatación (primer grado). Para este autor, una hipótesis de estas características, es una proposición científica que en el conocimiento científico trata de establecer, en este caso una ausencia de una característica.

La pregunta que trataremos de responder con esta investigación es: **¿Por qué existen barreras en cuanto a la firma electrónica en el MERCOSUR? ¿Cómo armonizar las legislaciones en torno a firmas electrónicas en el MERCOSUR?**

La Hipótesis que pretendemos demostrar en este trabajo es la siguiente: La creación de un marco jurídico contribuye a la armonización de las legislaciones en torno a las firmas electrónicas en el ámbito del MERCOSUR.

Por lo tanto, en la presente tesis postulamos la necesidad de lograr una adecuada armonización legislativa sobre firma electrónica en el ámbito del MERCOSUR.

En cuanto a la constatación de la hipótesis, seguimos a Heinz Dietrich (1996) nuevamente, el cual menciona que es la actividad mediante la observación, la experimentación, la documentación, etc. es que comprobaremos si la hipótesis que planteamos es correcta.

X. Tipo de diseño

El tipo de diseño que utilizamos fue no experimental. Los diferentes tipos de investigación que pueden realizarse, los distinguimos siguiendo a Hernández Sampieri et al. (2014) de la siguiente manera:

“Estudios Explicativos: buscan el porqué de los hechos, estableciendo relaciones de causa- efecto. “Está dirigido a responder a las causas de los eventos físicos o sociales” (p.62).

“También añaden que ninguna investigación debe basarse en un solo tipo de estudios, deben aplicarse diferentes tipos de investigación en relación al tipo de enfoque que se haya planteado” (p.58).

No experimentales: “es la que se realiza sin manipular deliberadamente las variables” (Hernández Sampieri et al., 2014, p.58).

Podemos identificar distintas metodologías, una denominada transversal siendo la que consiste en el diseño de investigación que recolecta datos de un solo momento, o sea, en un tiempo único y cuyo objetivo es describir variables y analizar su incidencia e interrelación en un momento dado; y otra signada como método longitudinal y reside en la recolecta datos a través del tiempo en puntos o períodos especificados, para hacer inferencias respecto al cambio, sus determinantes y consecuencias.

Finalmente, establecemos que la técnica consiste en el conjunto de instrumentos realizados en el cual se efectúa el método. Recordemos que método es el conjunto de pasos y etapas que debe cumplir una investigación.

El problema que planteamos se formula dentro de un marco teórico sobre los cuales desarrollamos los conceptos fundamentales a fin de poder desplegar y resolver el problema de la pregunta que nos planteamos para finalmente analizar los resultados de la investigación que puede confirmar, refinar o falsear esos presupuestos teóricos.

Consideramos, por lo tanto, que la estrategia adoptada nos dio las mejores oportunidades para responder del modo más efectivo a la pregunta del objeto de estudio.

XI. Problemas

Mencionamos en este punto una de las dificultades que atravesó este trabajo de investigación, y tal vez el mundo entero. El problema que surgió fue el de los efectos de la pandemia que azotó en el momento de realización de los últimos capítulos de la tesis. El 19 de marzo de 2020 se publicó en el Boletín Oficial argentino el DNU N° 297/2020 por el cual se decretó el Aislamiento Social, Preventivo y Obligatorio que fue prorrogado por otros decretos debido al Covid 19. Lo cual hizo que la asistencia a Bibliotecas físicas fuera interrumpida.

Más allá de que la totalidad de las legislaciones en que tuvimos que analizar e investigar se encuentra de manera online, la dificultad surge en poder acceder a la doctrina y demás material que hace a este trabajo. Por suerte nuestra tesis al ser materia de derecho informático, un derecho bastante joven y versátil, se halló la gran mayoría de los autores de manera digital, además de la novedosa labor de las bibliotecas que también permitieron el trabajo remoto.

Vale decir por lo tanto que siempre se dio prioridad a publicaciones digitales y artículos on-line, siempre en miras de tener a la mayor actualización y mayor estado del arte posible.

XII. Estructura de la Tesis

Llegado a este punto desarrollaremos la estructura que le dimos a la presente tesis. La misma cuenta con 7 capítulos, que fueron diseñados para que de manera lógica, escalonada y ordenada se llegue de los conocimientos más básicos en materia de estado del arte, conceptos, institutos primordiales, hacia conceptos más complejos y nuevos en el ámbito del derecho informático y las nuevas tecnologías. Por otro lado, también los Capítulos respetan una lógica y un orden.

Esto lo observamos en el Capítulo I. Estado del arte; y en el Capítulo II. Introducción, evolución y avance en materia de firma electrónica.

En el Capítulo III tratamos “La firma digital en Argentina”. Este capítulo como vemos se trata de un nivel local. Después avanzamos hacia el Capítulo IV, donde se tratará “La firma electrónica en el MERCOSUR”. Como se puede observar avanzamos sobre nuestros temas, esta vez desde el proceso de integración regional, integrado por Argentina y varios países de América Latina, el MERCOSUR, uno de los puntos más importantes de la tesis.

Con posterioridad tenemos el Capítulo V. donde también tratamos uno de los puntos más importantes para el presente trabajo, el Reglamento eIDAS. La Identificación Electrónica y los Servicios de Confianza en la Unión Europea.

En este Capítulo avanzamos a un nivel más regional e internacional, y en miras al orden que intentamos dar nos permite llegar a las conclusiones.

Por su parte el Capítulo VI contiene el “Marco Metodológico” de la investigación, que nos servirá para dar cuenta de todos los mecanismos, técnicas, herramientas, etc. empleadas en la investigación que nos permitieron dar respuesta al problema y a la hipótesis de nuestra investigación.

Por último, el Capítulo VII nos da las “Conclusiones finales y propuestas”. La conclusión final de la tesis retoma cada una de las conclusiones parciales de cada capítulo dando así un resultado holístico del trabajo.

Por su parte la propuesta para que se contemple un marco jurídico común para los Estados miembros del MERCOSUR. Las conclusiones y las propuestas, son una serie de observaciones, argumentos o deducciones que, relacionándolos, nos llevan con por lo tanto a la solución del problema planteado en la presente investigación, para que exista una mayor armonización legislativa en el MERCOSUR.

Capitulo VII

Conclusiones finales y propuestas

I. Conclusiones finales

1ª. En primer lugar desarrollamos la introducción, evolución y avance en materia de firma electrónica y su impacto como parte del derecho informático. Se estableció la revolución que significó la implementación de la firma electrónica en la historia del derecho produciendo un cambio de paradigma entre lo físico y lo digital. Conocimos los aspectos básicos y generales que se encuentran en la firma electrónica, firma digital, documentos electrónicos, infraestructura de firma digital, la criptografía, e incluso las nuevas tecnologías disruptivas como por ejemplo la tecnología del *blockchain*, y su relación con la firma electrónica.

2ª. Identificamos los elementos fundamentales de la firma digital en la legislación en la República Argentina. Del análisis a la LFD Argentina logramos identificar la labor en materia legislativa, así como también la incorporación de ella en la normativa de fondo nacional, la cual consideramos acertada, ya que permitió el florecimiento del ecosistema digital actual.

Altmark y Molina Quiroga (2012) han sostenido que

> … el uso cotidiano y cada día más extendido de aplicaciones informáticas documentales, la adhesión de las provincias a la ley 25.506, como las decisiones de tribunales superiores de implementar infraestructuras de firma digital, el impulso a las notificaciones electrónicas, las contrataciones estatales por medios electrónicos, el domicilio fiscal electrónico, la factura electrónica, la historia clínica informatizada, entre muchas otras iniciativas, van derribando —lenta pero inexorablemente— las barreras culturales que pudieron justificar la resistencia a admitir al documento electrónico o digital como un eficaz y seguro medio de registración de hechos y manifestaciones de voluntad, con plena eficacia probatoria (p. 448).

3ª. Concluimos acertada la introducción de conceptos, diferenciaciones, principios, valor probatorio y estructura que contiene la LFD Argentina, solo se le puede criticar su tardía reglamentación e implementación, que terminó por subsanarse con el pasar de los años. Y si hablamos de actualidad vale decir que la

firma digital permitió la realización de los procesos administrativos y judiciales nacionales. Lo mismo hizo con las transacciones electrónicas durante la crisis sanitaria ocasionada por el Covid 19, con una gran seguridad jurídica y una utilización masiva que llegó incluso a salvaguardar la salud de muchas personas.

4ª. Identificamos la implementación de la firma digital en el sector público nacional argentino, y establecimos como este último no fue ajeno al impacto de las nuevas tecnologías y por consiguiente, de la firma digital. Ante este cambio de paradigma, los modelos y conceptos de gobierno electrónico y de gobierno abierto, nacen con la misión de obtener mejores prácticas y procedimientos administrativos para ofrecer al gobierno alternativas y soluciones frente a los retos que se presentan actualmente en nuestro país. Dentro del considerando del Decreto Reglamentario 182/2019 de la firma digital de Argentina reza lo siguiente

> La sanción de la Ley N° 25.506 otorgó un decisivo impulso para la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información pública y posibilitar la realización de trámites por Internet en forma segura (considerando).

5ª. Identificamos en la legislación nacional argentina, la necesidad de avanzar sobre temas como el sello electrónico, sellos electrónicos del tiempo, o diferentes servicios digitales que promueven la confianza digital en todas las transacciones electrónicas inclusive tecnologías como el *blockchain* tan en boga en la actualidad y que aún no han sido tratadas.

6ª. Conocimos la legislación en materia de firma digital en el MERCOSUR y la de los países asociados, lo que nos permitió comprender la dimensión y los alcances de esta herramienta digital del MERCOSUR, de sus países miembros y de los estados asociados. Por otra parte, identificamos los elementos fundamentales en materia de firma electrónica, características y diferentes aspectos en materia de firma electrónica de cada país que forman parte del bloque regional y del MERCOSUR en sí.

7ª. Conocimos el Reglamento eIDAS, el marco jurídico para la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado único europeo el cual cambió todos los paradigmas existentes en materia

digital, paradigmas que consideramos, promovía la falta de interoperabilidad transnacional en el mercado digital de la U.E.

Este reglamento no solo armoniza las firmas electrónicas, sino que va más allá, introduciendo el reconocimiento de identidades electrónicas, los servicios de confianza, todos ellos armonizados y enmarcados en la legislación más disruptiva y evolucionada del mundo en esta materia.

8ª. También identificamos los aspectos y elementos principales del Reglamento eIDAS, por un lado, la identificación electrónica, y por el otro, los servicios de confianza, que engloban las firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o la creación, verificación y validación de certificados para la autenticación de sitios web.

9ª. Determinamos el grado de adopción de la firma electrónica en la U.E. con Reglamento eIDAS, y demás servicios de confianza. El reglamento en la U.E permitió el florecimiento del ecosistema a nivel digital europeo en uno de los más avanzados, seguros y prósperos mercados digitales del mundo.

10ª. Determinamos que el grado de adopción e implementación en el MERCOSUR es muy bueno, pero si miramos el trabajo realizado en la U.E en la materia, este queda un poco rezagado en muchos aspectos. Esto se traduce en barreras que dificultan el desarrollo pleno del comercio electrónico debido a la falta de un avance muchísimo mayor en legislación relativa a la firma digital y herramientas digitales.

En línea con estas ideas, dentro de las últimas normas emanadas por el MERCOSUR, el Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del MERCOSUR, el “Reconociendo” que establece

> RECONOCIENDO que, debido a la asimetría de los marcos jurídicos nacionales sobre la materia, es necesario suscribir acuerdos con estándares internacionales a fin de promover un entendimiento de las estructuras legales y técnicas de las Partes en la materia, puesto que se logrará garantizar la seguridad jurídica en el contexto de la utilización más amplia posible del procesamiento automático de datos (anexo).

11ª. Gracias a la anterior conclusión, establecemos que existen barreras que dificultan el desarrollo óptimo del comercio electrónico debido a la falta de

armonización legislativa relativa a la firma electrónica, o mejor dicho no existe un marco de referencia general transfronterizo y multisectorial para la interoperabilidad de identificación, autentificación y firma electrónica más que la Decisión N° 11/19 del Consejo Mercado Común: Reconocimiento mutuo de los certificados de firma digital y la Decisión N° 15/2021 del Consejo Mercado Común: Acuerdo sobre comercio electrónico.

La Decisión N° 11/19 del Consejo Mercado Común, establece el Reconocimiento mutuo de los certificados de firma digital, el cual dice lo siguiente

> Que el desarrollo continuo de las tecnologías de la información y de la comunicación se encuentra al servicio de la consolidación y del desarrollo de una sociedad de la información inclusiva que promueva el mejor aprovechamiento socio-económico de los bienes inmateriales. Que un número creciente de operaciones internacionales usan métodos de comunicación, almacenamiento y autenticación de la información sustitutivos de los que utilizan papel (considerandos).

Por su parte la Decisión 15/2021 del Consejo Mercado Común: Acuerdo sobre comercio electrónico establece lo siguiente

> Que, en el ámbito de MERCOSUR, los Estados Partes han profundizado el desarrollo de normas tendientes a aplicar mecanismos que faciliten y promuevan los intercambios a través de tecnologías de la información.
> Que, en complemento a la iniciativa MERCOSUR Digital, al Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del MERCOSUR y a otras normas relativas a la materia, resulta necesario que el MERCOSUR cuente con un instrumento común que represente la importancia que los Estados Partes asignan al comercio electrónico.
> Que es conveniente contar con un marco jurídico que consagre las normas y principios relativos al comercio electrónico en el MERCOSUR, con el objetivo de aprovechar el potencial económico y las oportunidades proporcionadas por el comercio electrónico (considerando).

Concluimos, que nuestro trabajo de investigación, nuestro planteo del problema y nuestros objetivos, se encuentran en línea con la última Decisión en materia de firma digital del MERCOSUR.

12ª. Determinamos también que la legislación Argentina, el MERCOSUR y sus países integrantes, no contienen dentro de sus artículos algún vestigio de autoridades de creación, verificación y validación de sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados

relativos a estos servicios, creación, verificación y validación de certificados para la autenticación de sitios web, preservación de firmas, sellos o certificados electrónicos relativos a estos servicios a excepción de la República del Paraguay. Tampoco existe avance alguno en materia de reconocimiento de identidades electrónicas tal como se plantea con el eIDAS.

Sin embargo, el art. 17 de la LFD, menciona la posibilidad de que se brinden otros servicios de certificación relacionados con la firma digital, entre los cuales se puede incluir a los servicios de confianza que menciona el Reglamento eIDAS. Los acuerdos y decisiones del MERCOSUR van por el mismo camino, no existen otros servicios de confianza o servicios de certificación relacionados a la firma electrónica a excepción de la firma electrónica en sí entre los países miembros, así como tampoco existe artículo alguno en materia de estandarización o armonización en materia de Identificación electrónica de los ciudadanos de los estados miembros.

13ª. Consideramos que hemos puesto a prueba nuestra hipótesis.

Tal como expusimos se continúa acentuando la falta de armonía que venimos advirtiendo a lo largo de nuestro trabajo en el ámbito del MERCOSUR. Por un lado, el bloque regional sigue sin contar con un marco normativo como el Reglamento eIDAS de la U.E.

Por otro lado, la República del Paraguay con su novedosa Ley 6822, “De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos” del año 2022, establece en materia de aspectos internacionales que: Los servicios de confianza prestados por los prestadores de servicios de confianza establecidos fuera del país serán reconocidos como legalmente equivalentes… (art. 7).

Esto significa claramente que la anterior legislación de este miembro del MERCOSUR, al igual que las de los demás miembros, no se encuentran armonizadas dificultando el desarrollo del comercio y del gobierno electrónico debido a la falta de armonización legislativa.

II. Propuestas y recomendaciones

En definitiva, lo que proponemos es eliminar las barreras existentes entre países miembros del MERCOSUR, asequible a través de la armonización de la firma electrónica (y demás servicios de confianza en el caso de que se adopten) lo que sin duda supondrá un avance en el impulso de la economía digital, el comercio electrónico y la implantación más efectiva de la administración pública electrónica.

El art. 1 del Tratado de Asunción para la Constitución del MERCOSUR en su último párrafo establece lo siguiente: “El compromiso de los Estados partes de armonizar sus legislaciones en las áreas pertinentes, para fortalecer el proceso de integración”. No dudamos que el aporte de esta investigación claramente coincide con los objetivos fundacionales del MERCOSUR, y por esa razón sugerimos a través de la redacción de pautas o lineamientos que veremos a continuación, promoverá la existencia de una mejor armonización legislativa en el MERCOSUR y en sus países miembros.

Por un lado, de acuerdo a los alcances y características de las Decisiones del MERCOSUR (arts. 38, 39 y 40 del Protocolo de Ouro Preto). Aprobadas las normas por los órganos decisorios del mismo, pueden ser obligatorias y cuando sea necesario, incorporadas a los ordenamientos jurídicos nacionales mediante los procedimientos previstos por la legislación de cada miembro del bloque.

Reconocemos la influencia de las pautas y lineamientos y que las mismas se basan en el Reglamento eIDAS. Sin embargo, mencionamos que los reglamentos de la U.E (tal como sucede con el eIDAS) se aplican de manera automática y uniforme en todos los miembros desde su entrada en vigor, sin necesidad de incorporación al derecho nacional los cuales son obligatorios, en todos sus elementos, en los Estados miembros.

Resaltamos que un marco legal de estas características debe ser neutral en lo que se refiere a la tecnología. Los efectos jurídicos que otorga deben poder lograrse por cualquier medio técnico, siempre que se cumplan los requisitos que se establezcan.

A continuación, se encuentran las pautas o lineamientos para que haya una mayor armonización legislativa en el MERCOSUR.

a. Establecer el objeto, siendo su objetivo garantizar el correcto funcionamiento del comercio electrónico aspirando al mismo tiempo a un nivel de seguridad adecuado de las firmas electrónicas.

Establecer las normas para las firmas electrónicas y establecer un marco jurídico común para las firmas electrónicas dentro del MERCOSUR con el reconocimiento jurídico de los métodos de autenticación y firmas electrónicas de sus miembros (de sus certificados digitales).

b. Establecer el ámbito de aplicación.

c. Establecer a los efectos del marco legal, las definiciones de los términos o definiciones más relevantes que en él se apliquen.

d. Establecer el tratamiento, la protección de datos y la confidencialidad. (Capítulo V. VI. C de la tesis)

e. Incorporar de ser posible los “servicios de confianza”: estos incluyen las ya conocidas firmas electrónicas, además de incorporar a los sellos electrónicos, el sellado de tiempo, la entrega electrónica certificada, y la autenticación web. Para esto, además se debe establecer la figura de los prestadores de servicios de confianza dentro del MERCOSUR. (Capítulo V. VIII de la tesis).

Como ya desarrollamos en la presente tesis los servicios de confianza tienen como objetivo garantizar la confianza, la seguridad y la seguridad jurídica en las transacciones electrónicas, algo más que necesario en la actualidad y en el ámbito del MERCOSUR.

f. Establecer los aspectos internacionales.

El Reglamento elDAS armoniza en este sentido a través del art. 14 al establecer que la U.E garantizara la validez de los certificados digitales de los países miembros en materia de servicios digitales de acuerdo a determinadas circunstancias.

Un interesante ejemplo de un miembro del bloque del MERCOSUR lo hace el Paraguay con el art. 7 de la Ley 6822 titulado “aspectos internacionales (Vemos también influencia del Reglamento elDAS) cuando establece que

> Los servicios de confianza prestados por los prestadores de servicios de confianza establecidos fuera del país serán reconocidos como legalmente

> equivalentes a los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la República del Paraguay si los servicios de confianza son reconocidos en virtud de acuerdos de reconocimiento mutuo celebrado entre autoridades normativas de cada país o con organizaciones internacionales de conformidad a la reglamentación correspondiente (art. 7).

g. Establecer los efectos jurídicos de las firmas electrónicas. Conforme a la presente tesis, concluimos que en el MERCOSUR contamos con certificados de firma electrónica avanzada, por lo que no deben ser denegados sus efectos jurídicos como prueba en procesos judiciales solo por ser electrónicos.

El principio de equivalencia funcional debe estar presente en todo momento, teniendo los mismos efectos jurídicos que la firma ológrafa. Recordemos lo establecido por la Ley Modelo sobre Firma Electrónica de la CNDMI en el art. 12, bajo el título “el reconocimiento de certificados y firma electrónica”, en donde se establece el principio de no discriminación, tratando de dar validez jurídica a una firma o certificado, con independencia de donde se haya expedido, siendo su fiabilidad técnica el factor que determine su efecto jurídico.

El reconocimiento mutuo de los certificados de firma electrónica avanzada por parte de los estados miembros del MERCOSUR es fundamental. Se deben garantizar las condiciones para que las firmas electrónicas funcionan entre distintos miembros del MERCOSUR.

Acerca de esto último, el Reglamento elDAS nos da la pauta en el art. 24 cuando trata los “Efectos jurídicos de las firmas electrónicas”:

> 1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada. 2. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita. 3. Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros. (art. 25).

h. Establecer los requisitos para las firmas electrónicas avanzadas. Conforme a la presente tesis y de modo que lo hace el Reglamento elDAS (Capitulo V. XIII y XII

de la tesis), pudimos ver los diferentes requisitos para que una firma electrónica pueda considerarse una firma electrónica avanzada, cosa que debería quedar manifiesta en el marco legal.

i. Establecer las especificaciones técnicas y los niveles de seguridad (también para el caso de que sean incorporados los servicios de confianza). Conforme a la presente tesis pudimos constatar los diferentes métodos técnicos, criptográficos y sus diferentes niveles de seguridad, los cuales deben ser tenerse en cuenta. Todos los estados miembros del MERCOSUR deben seguir estas especificaciones y sus requisitos para garantizar un nivel de seguridad equivalente.

j. Establecer las condiciones en que los Estados miembros deberán reconocer las normas para las firmas electrónicas (también para el caso de que sean incorporados los servicios de confianza). Conforme a la presente tesis, observamos como el GAD del MERCOSUR ya ha avanzado en este punto, estableciendo normas para el reconocimiento de las firmas electrónicas avanzadas dentro del MERCOSUR.

Bibliografía y fuentes de información

A. Bibliografía

Altmark, R., y Molina Quiroga, E. (2012). *Tratado de derecho informático.* La Ley.

Bibiana, L. C. (2006). *Ley de firma digital comentada.* Nova Tesis Editorial Jurídica.

Bielli, G., y Nizzo, A. (2017). *Derecho Procesal Informático*. La Ley.

Camps, C. (2015). *Tratado de Derecho Procesal Electrónico.* La Ley.

Caramelo, G., Picasso, S., y Herrera, M., (2015). *Código Civil y Comercial de la Nación Comentado* (1a. Ed.). Infojus. http://www.saij.gob.ar/nuevo-codigo-civil-y-comercial-de-la-nacion

Dates, L. E., y Maqueda, S. (2018, 3 de septiembre). Hacia una modernización (total) del procedimiento administrativo. *Abogados.com.ar* [online]. https://abogados.com.ar/hacia-una-modernizacion-total-delprocedimiento-administrativo/22064

De Luca, J. (2015). *La implementación de la firma digital en el sector público: mejoras en la gestión y en los procesos para lograr óptimos resultados.* Universidad de Buenos Aires. Facultad de Ciencias Económicas. Escuela de Estudios de Posgrado. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0390_DeLucaJC.pdf

Diffie, W., y Hellman M. E. (1976). New directions in Criptography [Nuevas direcciones en criptografía]. *Transcactions on information theory*

[Transacciones sobre la teoría de la información], *22*(6), 644-654. IEEE. https://www.documentcloud.org/documents/2730231-24.html

Fernández Delpech, H. (2014). *Manual de Derecho Informático*. La Ley.

García Mexía, P. (2018). *Criptoderecho: la regulación de Blockchain*. Wolters Kluwer.

Heinz Dietriech, H. (1996). *Nueva guía para la investigación científica.* Editorial Planeta Mexicana.

Hernández Sampieri, R., Fernández, Collado, C., y Baptista Lucio, M. P. (2014). *Metodología de la Investigación*. McGraw-Hill Interamericana.

La Nación. (2015). *Nuevo Código Civil: el impacto en la vida cotidiana de los argentinos* [diario online]. https://www.uba.ar/noticiasuba/nota.php?id=540

Llaneza González, P. (2018). *Reglamento eIDAS nuevos servicios de confianza, identificación electrónica, y sus prestadores.* Comares.

Mason, S. (2017). *Electronic Signatures in Law* [Firmas electrónicas en la Ley] (4th ed.). University of London.

Merchán Murillo, A. (2016). *Firma electrónica. Funciones y problemática. (Especial referencia al reglamento (UE) nº 910/2014, relativo a la identificación electrónica por la que se deroga la directiva 199/93/CE).* Aranzadi.

Merchán Murillo, A. (2015). *Reconocimiento transfronterizo de la firma electrónica* (Tesis de Doctorado). Repositorio institucional UPO. https://rio.upo.es/xmlui/bitstream/handle/10433/2055/merchan-murillo-tesis15.pdf?sequence=1&isAllowed=y

Merchán Murillo, A. (2015). La cooperación judicial internacional digital. *Revista Iberoamericana de Derecho Informático, 25*-40. FIADI. http://fiadi.org/revista_fiadi/

Monroy, D. A. (2020*).* Entendiendo blockchain, su aplicación y sus implicaciones legales y técnicas. *Revista Iberoamericana de Derecho Informático, 1*(8), 53-69. FIADI. http://fiadi.org/revista_fiadi/

Núñez Miller, J. (2017). Criptografía y consenso aplicado a la blockchain. En A. Preukschat (coord.) *Blockchain: la revolución industrial de internet* (pp. 203-220). Centro Libros PAPF.

Ordoñez, J. (2020). *El expediente electrónico.* Hammurabi.

Rifkin, J. (2011). *La Tercera Revolución Industrial*. Paidós.

Ritto, G. (2019). *El gobierno abierto en la Administración Pública Nacional.* Rubinzal Culzoni.

Rolero, G. (2001). *Documento electrónico y firma digital.* Necesidad de una legislación específica. SAIJ. http://www.saij.gob.ar/doctrina/dacf010040-rolero-documento_electronico_firma_digital.htm

Rossi, J. R. (2001). *Documento y firma digital: para entrar en tema.* SAIJ. http://www.saij.gob.ar/doctrina/dacf080089-rossi-documento_firma_digital_para.htm

Schwab, K. (2016). *La cuarta revolución industrial.* Debate.

Schwab, K. (2016). *The Fourth Industrial Revolution: what it means, how to respond* [La cuarta revolución Industrial: qué significa, cómo responder]. World Economic Forum [Foro Económico Mundial]. www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Thill, E. (2011). *Modelo Social de la Agenda Digital Argentina: Inclusión Digital para la integración social 2003-2011.* Jefatura de Gabinete de Ministros. http://catalogoiigg.sociales.uba.ar/cgi-bin/koha/opac-retrieve-file.pl?id=172e2b01a742dbf75d403a9fde6c92c9

B. Fuentes de información

Acuerdo de reconocimiento mutuo de certificados de firma digital entre la República Argentina y la República de Chile. (2018). http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312884/res436.pdf

ALADI. (1996). *Acuerdo de Complementación Económica MERCOSUR - Chile N° 35*. https://www2.aladi.org/nsfaladi/textacdos.nsf/ca05a6ae01cc969583257d8100416d1e/85868e7a6308d7d70325776d005ad45a?OpenDocument

Argentina.gob.ar. *Gestión Documental Electrónica – GDE.* https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/gde

Cámara Nacional de Apelaciones en lo Civil y Comercial de La Plata. (2020, 29 de septiembre). Banco de la Provincia de Buenos Aires c/ Spindola Sabrina Lorena s/ cobro ejecutivo. SAIJ. http://www.saij.gob.ar/camara-apelacion-civil-comercial-nro-2-local-buenos-aires-banco-provincia-buenos-aires-

spindola-sabrina-lorena-cobro-ejecutivo-fa20010096-2020-09-29/123456789-690-0100-2ots-eupmocsollaf?

Cámara Nacional de Apelaciones en lo Comercial. Capital Federal, Ciudad Autónoma de Buenos Aires. (2008, 15 de mayo). Bieniauskas, Carlos c/ Banco de la Ciudad de Buenos Aires. SAIJ. http://www.saij.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

CLAD. (2007). *Carta Iberoamericana de Gobierno Electrónico.* https://clad.org/wp-content/uploads/2020/07/Carta-Iberoamericana-de-Gobierno-Electronico.pdf

CLAD. (2009). *Carta iberoamericana de Gestión Pública. Resolución 38 del Plan de Acción de Lisboa.* http://observatorioserviciospublicos.gob.do/baselegal/carta_iberoamericana_de_participaci%C3%B3n_ciudadana.pdf

Comisión Europea. (2011). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0206:FIN:es:PDF

Comisión Europea. (2012). *Tratado de funcionamiento de la unión europea.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:ES:PDF

Comisión Europea. (2013). Reglamento (UE) Nro 1316/2013 del Parlamento Europeo y del Consejo. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013R1316&from=en

Comisión Europea. (2014). *Agenda Digital para Europa*. http://dx.doi.org/10.2775/41368

Comisión Europea. (2014). *Reglamento (UE) Nro 910/2014 del Parlamento Europeo y el Consejo*. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&from=ES#d1e771-73-1

Comisión Europea. (2021). *REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0281&from=DA

Comisión Europea. (2015). Reglamento de ejecución 2015/1502 del Reglamento eIDAS. https://www.boe.es/doue/2015/235/L00007-00020.pdf

Comisión Europea. (2019). *Un Mercado Único Digital en beneficio de todos los europeos.* https://digital-strategy.ec.europa.eu/en/library/digital-single-market-benefit-all-europeans

Comisión Redactora del Anteproyecto de Ley de Firma Digital. *Informe de la comisión redactora.* https://web.archive.org/web/20010219001233/http://www.pki.gov.ar/PKIdocs/Informe.html

Comunidad Andina. (2004, noviembre 2). *Acuerdo de Complementación Económica MERCOSUR N° 59*. http://intranet.comunidadandina.org/Documentos/DInformativos/SGdi671.pdf

Decreto 1747/00. (2000), *por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4277

Decreto 182/2019. (2019). *Ley N° 25.506. Reglamentación.* http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/320735/norma.htm

Decreto 27/2018. (2018). *Desburocratización y Simplificación.* http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/305736/norma.htm

Decreto 434/2016. (2016). *Plan de Modernización del Estado.* http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259082/norma.htm

Decreto 436/011. (2011). *Reglamentación de Documento Electrónico y Firma Electrónica*. https://www.impo.com.uy/bases/decretos/436-2011/17

Decreto 561/2016. (2016). *Sistema De Gestión Documental Electrónica.* http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/260145/norma.htm#:~:text=DECRETA%3A,expedientes%20del%20Sector%20P%C3%BAblico%20Nacional.

Decreto 7369/11. (2011). *Reglamento General de la Ley 4017/10.* https://www.acraiz.gov.py/adjunt/Leyes%20y%20Decretos/decreto7369reglamento.pdf

Decreto Supremo N°1793. (2014). *Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación.*

https://www.bcb.gob.bo/webdocs/normativa/2013%20-%20DS%201793%20-%20Reglamenta%20la%20Ley%20N%C2%B0%20164.pdf

Diario Oficial de las Comunidades Europeas. (2000). *Carta de los Derechos fundamentales de la unión europea,* 364, 01-22. https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Directiva 1999/93/CE del Parlamento Europeo y del Consejo. (1999). *por la que se establece un marco comunitario para la firma electrónica*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A31999L0093

Electronic Signature in Global and Nacional Commerce Act [Ley de Firma Electrónica en el Comercio Global y Nacional]. (2000). http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

Firma electrónica (ICP-Brasil). (2018). https://enciclopediajuridica.pucsp.br/verbete/257/edicao-1/assinatura-eletronica-%28icp-brasil%29

Gesetz zur digitalen Signatur [Ley de Firma Digital]. *(Signaturgesetz - SigG).* (1997). http://www.iprecht.com/Lawyer/Contact/Download/signaturgesetz.pdf

Infoleg. (s. f.) *Normativa Sistema de Gestión Documental Electrónica – GDE.* http://www.infoleg.gob.ar/?page_id=149

La Nación. (2015) *Nuevo Código Civil: el impacto en la vida cotidiana de los argentinos.* https://www.lanacion.com.ar/sociedad/nuevo-codigo-civil-el-impacto-en-la-vida-cotidiana-de-los-argentinos-nid1814707/

Ley 13.666 de adhesión de la Prov. de Bs. As. a la ley 25.506. (2007). http://www.gob.gba.gov.ar/legislacion/legislacion/l-13666.html

Ley 164. Ley general de telecomunicaciones, tecnologías de información y comunicación. (2011). https://www.wipo.int/edocs/lexdocs/laws/es/bo/bo052es.pdf

Ley 18.600. del Documento electrónico y Firma electrónica. (2009). https://www.impo.com.uy/bases/leyes/18600-2009/2

Ley 4017. De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico. (2015). https://www.bacn.gov.py/leyes-paraguayas/3550/ley-n-4017-de-validez-juridica-de-la-firma-electronica-la-firma-digital-los-mensajes-de-datos-y-el-expediente-electronico

Ley 6822. De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos. (2022). https://www.bacn.gov.py/leyes-paraguayas/10318/ley-n-6822-de-los-servicios-de-confianza-para-las-transacciones-electronicas-del-documento-electronico-y-los-documentos-transmisibles-electronicos

Ley 527 de 1999. (1999). http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Ley de Comercio Electrónico, Firmas y Mensajes de Datos. (2002). https://www.gob.ec/regulaciones/2002-67-ley-comercio-electronico-firmas-mensajes-datos

Ley de Firma Digital Argentina 25.506. (2001). http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Ley de Firmas y Certificados Digitales Ley 27.269. (2002). https://www.minjus.gob.pe/wp-content/uploads/2014/03/Ley27269.pdf

Ley de Gobierno Electrónico de 2002. (2002). https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno. (1996). https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce

Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001). https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_signatures

Ley sobre mensajes de datos y firmas electrónicas. (2001). http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-sobre-Mensajes-de-Datos-y-Firmas-Electr%C3%B3nicas.pdf

Medida provisional 2.200-2. (2002). https://legislacao.presidencia.gov.br/atos/?tipo=MPV&numero=2200-2&ano=2001&ato=21cAza610MNpWT1e4

MERCOSUR. (1991). Tratado de Asunción para la Constitución de un Mercado Común https://www.mercosur.int/documento/tratado-asuncion-constitucion-mercado-comun/

MERCOSUR. (1995). *Protocolo de Ouro Preto*. *Adicional al Tratado de Asunción sobre la Estructura Institucional del MERCOSUR*. https://www.mercosur.int/documento/protocolo-ouro-preto-adicional-tratado-asuncion-estructura-institucional-mercosur/

MERCOSUR. (2006). Res. No. 37/06 Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del MERCOSUR. http://servicios.infoleg.gob.ar/infolegInternet/anexos/120000-124999/120555/norma.htm

MERCOSUR. (2014). Decisión del Mercosur 24/2014. https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n-24-2014-250227/texto

MERCOSUR. (2017). Decisión del Mercosur 27/2017. Creación del Grupo Agenda Digital Mercosur. https://acortar.link/vleHa4

MERCOSUR. (2021). Decisión del Mercosur 15/2021 Acuerdo sobre Comercio Electrónico del Mercosur. https://acortar.link/mdaAh

MERCOSUR. (2021). Estatuto de la Ciudadanía del MERCOSUR. https://www.mercosur.int/estatuto-ciudadania-mercosur/

MERCOUR. (2019). Decisión del Mercosur 11/2019. *Acuerdo de Reconocimiento Mutuo de Certificados de Firma Digital del Mercosur*. https://acortar.link/QKZx77

Plan de Modernización del Estado. (2016). http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259082/norma.htm

Poder Judicial de la Nación. (2019, 24 de septiembre). Juzgado Civil y Comercial Federal Nº 5 Cap. Fed. Incidente sobre Medida Cautelar 4451/2019.

https://www.diariojudicial.com/public/documentos/000/086/428/000086428.pdf

Real Academia Española: *Diccionario de la Lengua Española.* (2021). https://dle.rae.es

Reglamento de la Ley de Firmas y Certificados Digitales Decreto Supremo Nº 052-2008-PCM. (2008). https://diariooficial.elperuano.pe/pdf/0030/ley-27269.pdf

The Electronic Signatures Regulations [El Reglamento de Firmas Electrónicas]. (2002). http://www.legislation.gov.uk/uksi/2002/318/contents/made

Unión Europea. (2020). *Discurso sobre el estado de la Unión.* https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

Unión Europea. (s.f.). *Principios, países, historia.* https://european-union.europa.eu/principles-countries-history_es