EL PANORAMA LEGAL DEL COMERCIO ELECTRÓNICO Y ALGUNOS DE SUS RIESGOS

Estudio preliminar

Por:

Valentina Castrillón González

Manuela Restrepo Martínez

Asesor:

José Alberto Toro Valencia

Trabajo para optar al título de abogadas

Escuela de Derecho

Universidad EAFIT

Medellín, abril 2021

Índice

Resumen

Debido a el alarmante paso en que el uso de la Internet y las plataformas digitales ha crecido el presente trabajo de tesis tiene como objetivo realizar una investigación sobre el comercio electrónico. Esto con un análisis de los riesgos jurídicos asociados con las nuevas tecnologías, en específico, con las disputas de los dominios de internet, con la falsificación y la infracción de marca comercial, y el fraude electrónico y la usurpación de identidad en los documentos digitales. Para ello se plantea un primer capítulo con una explicación del concepto del comercio electrónico, se expone un poco de su historia, formas y procesos.

En un segundo capítulo se procede a un estudio regulatorio del comercio electrónico*,* se lleva a cabo una recopilación normativa nacional e internacional sobre este y se brinda un esclarecimiento de su aplicación en la actualidad, por ende, se toman como base análisis doctrinales, jurisprudenciales y legislativos sobre el *eCommerce.* Así, en un tercer capítulo se ejecuta la introducción a cada riesgo y su regulación nacional e internacional, esto para detallar, oportunamente, la manera en que cada uno puede ser mitigado, de este modo, se finaliza con una conclusión.

Palabras clave: riesgo, comercio electrónico, disputas de dominio, infracción de marcas en internet, documentos electrónicos.

Abstract

Due to the alarming rate in which the use of Internet and digital platforms is being implemented in day to day basis this thesis aims to make a compilation of information about e-commerce, focusing in analyzing the legal risks associated with the use of new technologies and digital platforms in Colombia, concretely, the risks related with domain names in the internet, trademark infringement and passing off in the internet and the electronic fraud and identity usurpation in electronic documents. The first chapter will be an introduction and a definition of the concept of e-commerce, its history, the types of e-commerce and the processes involving its use.

In a second chapter a recompilation of the international and local legal framework of e-commerce will be developed, therefore a legislative analysis on e-commerce law. Will be explained; In a third chapter we will proceed to realize the introduction and analysis of each risk and the ways these can be mitigated, ending with a conclusion.

Key words: risk, electronic commerce, domain name disputes, trademark passing off, electronic document.

Introducción

La globalización, los tratados de libre comercio y los distintos convenios entre Estados para expandir sus economías han traído consigo la necesidad de implementar nuevos desarrollos tecnológicos. Esto debido a que la economía es impulsada por la Cuarta Revolución Industrial marcada por las convergencias de nuevas tecnologías digitales, físicas y biológicas en el mundo.

La Asamblea General de la Organización de las Naciones Unidas (2016), en la Resolución A/HRC/32/L.20, señaló el acceso a internet como un derecho humano que ha tomado un gran protagonismo en la actualidad y, en correspondencia con el estudio de “Securing the digital economy”, el nivel de dependencia de las personas a los medios digitales ha incrementado de un 28 % en el 2008 a un 100 % en el 2018 (Accenture,2019). Cabe resaltar que el virus SARS-CoV-2 llevó, a la gran mayoría de países, a instaurar diferentes medidas para tratar de evitar los contagios, como el confinamiento obligado, el aislamiento social o el cierre de colegios y otros espacios públicos, en consecuencia, la población ha permanecido más tiempo en sus casas; dicha realidad se traduce en un mayor uso de los medios tecnológicos de comunicación, concretamente, de las diferentes plataformas de internet; de conformidad con la plataforma de estadísticas Statista, el crecimiento del uso de plataformas electrónicas en los países ha acrecentado entre de un 19 % a un 108 % en la pandemia (2021).

> De acuerdo con el último informe sobre el índice de comercio electrónico de empresa a consumidor 2020, elaborado por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD, por sus siglas en inglés), los 152 países calificados en el ranking sumaron durante el último año US $ 4,4 billones, lo que representa un incremento de 7 % respecto al 2019. (La República, 2021, p. 3)

Además, ante la crisis mundial por el Covid-19, la Unidad Internacional de las Telecomunicaciones (UIT) estableció unas directrices para la elaboración y la aplicación de planes nacionales de telecomunicaciones de emergencia. En estas, se señalaron los lineamientos para que las autoridades competentes de cada Estado puedan garantizar el uso de las redes y telecomunicaciones antes, después y en una catástrofe. Conforme con lo consagrado en estas directrices, se busca que las comunicaciones tecnológicas ayuden a la población a superar la emergencia, esto conlleva a inferir que una de las soluciones identificadas por los organismos internacionales para mitigar los posibles daños de la emergencia sanitaria, de talla mundial, es la tecnología, pues esta podría aliviar las repercusiones económicas, por lo tanto, su dependencia va en aumento.

Con lo anterior es posible afirmar que las compras por internet también han acentuado, en gran medida, por el aislamiento de los individuos, en concordancia con el diario La República*,* respaldado en un estudio realizado por Kantar, el comercio electrónico ha crecido más de un 300 % en América Latina en la pandemia; estas cifras reflejan que los consumidores han cambiado sus hábitos de compra, por consiguiente, en el caso de Colombia, según la Cámara Colombiana de Comercio Electrónico, el comercio electrónico aumentó entre un 50 % a 80 % en la cuarentena. Igualmente, de

acuerdo con Adriana Ceballos, directora de desarrollo de programas del Centro de Análisis y Creatividad de las TIC (TicTac) de la Cámara Colombiana de Informática y Telecomunicaciones, el 2020 fue un año muy positivo en cuanto a transacciones digitales; en julio de 2020 se llegó casi a los $ 3 mil millones en transacciones de comercio electrónico, es decir, hubo un crecimiento de 130 %, en general, en el país.

En definitiva, el uso de internet se intensificó y esto implica que la utilización de plataformas de comercio electrónico también lo ha hecho. Así, por el crecimiento masivo, el mundo de los negocios tradicionales se revoluciona, pues cada vez más personas pretenden abrir un negocio por internet y más consumidores cambian sus hábitos de consumo, dejan atrás las tiendas físicas y optan por comprar en línea. Esto genera transformaciones profundas en la forma de adquirir ciertos bienes o servicios, puesto que se evita la presencialidad y se promueve la virtualidad. Dichos cambios requieren la implementación de regulaciones jurídicas al presentarse con ellos nuevos retos para los consumidores y para los que ofrecen los bienes o servicios, estos retos pueden suscitar riesgos jurídicos.

A pesar de que estas tecnologías llevan un tiempo en desarrollo, al incrementar su utilización, y volverse necesarias para el progreso de actividades cotidianas, comienza a ser oportuno que los individuos conozcan el alcance del comercio electrónico y algunos de los riesgos en el ejercicio de su actividad. Por ello, el presente trabajo de grado tiene como objetivo realizar una recopilación de los modelos de regulación del comercio electrónico, para identificar los riesgos asociados a esta modalidad de comercio. Dentro de dichos riesgos se encuentran disputas de dominios, la infracción y falsificación de

marcas en internet, y el fraude electrónico y la usurpación de identidad en documentos electrónicos.

En el primer capítulo se indaga por el concepto de comercio electrónico. Para ello se exploran distintas definiciones del mismo, su historia, y los tipos de comercio electrónico que existen. En el segundo capítulo se hace una compilación de las distintas regulaciones sobre el comercio electrónico tanto nacionales como internacionales, con la finalidad de identificar si se adoptan patrones similares entre ellas y si se hace uso de la ley modelo de la CNUDMI (Comisión de Naciones Unidas para el Derecho Mercantil Internacional). En el tercer capítulo se efectúa un análisis sobre los riesgos relacionados con el comercio electrónico. Dentro de los riesgos se encuentran la usurpación de nombres de dominio, la falsificación e infracción de marcas en internet, el fraude electrónico y la usurpación de identidad en documentos electrónicos. Es por esto que resulta importante realizar un estudio de las distintas regulaciones del comercio electrónico y los riesgos mencionados, con ello se pretende informar y alertar a las personas sobre el contexto en el que se encuentran actualmente, brindarles un mayor conocimiento y seguridad frente a esta materia para pueda proporcionarles soluciones y mecanismos para mitigar e identificar dichos riesgos.

Por otro lado, es fundamental analizar el impacto que esto tiene en el derecho, al identificar los riesgos se puede acudir a herramientas jurídicas para mitigarlos, también es importante aprender a distinguirlos, en vista de que, en algunos casos, por ejemplo, en los riesgos relacionados con la infracción de marcas en internet, el derecho proporciona herramientas para prevenirlos; en tal sentido, si algunos de estos se presentan, como el del secuestro de nombre de dominio, esto podría afectar al negocio

al que le fue robado el nombre de dominio y a los consumidores, estos perderían su dinero al realizar compras a través de dicho nombre. Para finalizar, es elemental ejecutar una estructuración y recopilación de información sobre el comercio electrónico y sus riesgos, en virtud de que frente a estos todavía hay ciertos vacíos legales de los que es importante hacer al lector consciente y lograr suministrarles una mayor seguridad y conocimiento respecto a estos temas; el uso del internet y de plataformas digitales para la realización de actividades de la cotidianidad va en aumento y es cada vez más necesario para el ser humano.

Capítulo 1. ¿Qué es el comercio electrónico?

En principio, es importante identificar que en Colombia el comercio electrónico se encuentra consagrado en un marco constitucional y legal, de esa manera, está justificado en la Constitución Política de Colombia en el Artículo 15 que señala el derecho a la intimidad y al buen nombre, de donde se deriva el *habeas data*; asimismo, en el Artículo 20 indica la libertad de expresión, una de las principales garantías del comercio electrónico, y en el Artículo 333 se plantea que la actividad económica y la iniciativa privada son libres dentro de los límites del bien común. Por otra parte, el marco legal es la Ley 527 de 1999 como ley de comercio electrónico, esta proyectó el principio de equivalencia funcional entre la firma electrónica y la autógrafa, y entre los mensajes de datos y los documentos escritos.

De acuerdo con lo mencionado, Colombia cuenta con la Ley 527 de 1999 que consagró la regulación de la firma digital en el territorio nacional. Este estudio se denominó como una forma de identificar, inequívocamente, al firmante y asegurar la integridad del documento firmado, esto para analizar qué metodologías debe adoptar una entidad pública o privada al momento de distinguir a un individuo que utilice el comercio electrónico, y tener una verificación de su identidad y datos.

En lo relativo con la recolección de datos personales de los sujetos que hacen uso de la herramienta del comercio electrónico, es necesario tener en cuenta que en cuanto a su protección existe un marco normativo amplio, este busca generar confianza en las personas y garantizar el derecho de *habeas data*; igualmente, se debe considerar que

uno de los elementos relevantes para llevar a cabo estas actividades y tener pruebas son los documentos electrónicos, pues el Artículo 299 de la Ley 1 de 2000 ideó la eficacia de cualquier documento derivado del proceso en una plataforma electrónica o que se transfiera electrónicamente. Así, se debe verificar que el contenido de estos documentos cumpla con lo oportuno y tenga validez jurídica, es decir, surta los efectos legales y jurídicos.

1.1 Definición del comercio electrónico

No hay una definición absoluta y globalmente aceptada sobre qué es el comercio electrónico, este puede ser definido de muchas formas puesto que no está enmarcado en una única definición; a continuación, se exponen algunas de las conceptualizaciones más empleadas del comercio electrónico.

Para la OMC (Barchetta et al., 1998), el comercio electrónico está compuesto por instrumentos como el fax, el televisor, los pagos electrónicos, las transferencias electrónicas, el intercambio de datos electrónicos y el internet; esta definición es muy extensa y abarca muchos conceptos, pero la empleada en este trabajo de grado comprende, únicamente, las transacciones de bienes y servicios que se hagan por una plataforma electrónica de internet. La CNUDMI (1998) utiliza una definición más cerrada del comercio electrónico, lo refirió como el uso alternativo de métodos de comunicación y almacenamiento de información al papel, donde es pertinente resaltar que, en dicha descripción, no están incluidos ni el teléfono ni el fax, sino que esta gira en torno al internet.

Para Anteportamlatinam (2014), el comercio electrónico está ligado a las Tecnologías de la Información y Comunicación (TIC) que permiten el desarrollo de actividades empresariales. Esta definición es muy abierta, no aluden a una conceptualización de las tecnologías, por lo tanto, puede abarcar muchísimas definiciones de esta. En otro orden de ideas, de acuerdo con Paul Todd (2005), el comercio electrónico se entiende como cualquier transacción que involucre bienes o servicios, en donde las comunicaciones electrónicas y digitales desempeñan una función esencial, es importante recordar que este es transfronterizo, por esto, depende de políticas establecidas entre territorios dentro de un mismo país o diferentes países en tiempo real.

Conforme con lo señalado por la enciclopedia de negocios de Shopify (Shopify Business Encyclopedia, 2020), el comercio electrónico se refiere a la compra y venta de bienes y servicios, ejecutado esto mediante internet, y las transacciones de dinero y data que se realizan para dichas compraventas. En concreto, para integrar los diferentes conceptos de comercio electrónico, se entendió, para efectos de este trabajo de grado, como una función del comercio que se efectúa por medios digitales o electrónicos, y se puede dar desde diferentes territorios para intercambiar bienes y servicios.

1.2 Antecedentes históricos

El comercio electrónico se hizo posible gracias al desarrollo del EDI (*Electronic Data Interchange*). Este era un modelo que se basaba en el intercambio de documentos de negocios de un computador a otro en un formato estándar. Fue creado a mediados de los años sesenta, cuando las compañías de transporte y algunas industrias de venta

al por menor tenían la intención de instaurar oficinas “libres de papel”, en este sentido, en 1970 el EDI fue formalizado por el Comité de estándares acreditado de representantes de la industria de los Estados Unidos. Después de esto, en las décadas de los setenta y ochenta, varias compañías lo empezaron a adoptar.

En 1980, la Internet mantenía su naturaleza no comercial, y los que lo usaban eran, en su mayoría, científicos e ingenieros que trabajaban para el Gobierno de los Estados Unidos y universidades. Gracias al desarrollo de una forma interfaz de usuario, se les posibilitó a los usuarios interactuar con dispositivos electrónicos con iconos gráficos e indicadores de audio y no por textos. La segunda generación del comercio electrónico se caracterizó por la transacción de bienes y servicios a través del internet, lo que empezó como una herramienta de búsqueda evolucionó y se convirtió en una herramienta comercial.

Lo anterior se remonta a 1960, cuando *Advanced Reserch Project Agency Computer Network* (ARPANET), el precursor de la Internet. ARPANET se estableció para investigar en áreas de alta tecnología. El término internet no fue utilizado sino hasta 1982, cuando el número de *hosts* en ARPANET rozaba los 213; luego, en 1983, el protocolo de internet, o *internet protocol* (IP), se convirtió en el único modo aprobado para transmitir datos en la red, esto con la habilitación de todos los computadores para intercambiar información por igual.

En 1986, la Fundación Nacional de Ciencia, agencia del Gobierno de Estados Unidos, lanzó la *National Science Foundation Network* (NSFNET); con el propósito de proporcionar comunicaciones más rápidas entre centros de supercomputadoras en dicho

Estado, donde la columna vertebral del NSFNET se convirtió en la piedra angular del internet, basado esto en el Protocolo de Control de Transmisión /Protocolo de Internet (TCP/IP).

Por consiguiente, la denominada *World Wide Web* (WWW) cambió la naturaleza del uso del internet y, en 1990, con la creación del lenguaje de marcado de hipertexto HTML empleado para la elaboración de páginas web, con especificaciones para localizadores uniformes de recursos (URL), la dirección específica asignada a cada uno de los recursos disponibles en la red para que puedan ser localizados, se logró desarrollar el internet que se conoce actualmente (Zwass, s.f.). En tal óptica, para Anteportamlatinam, (2014), el comercio electrónico surgió por la necesidad de las empresas de utilizar la tecnología de los medios electrónicos para mejorar la relación con los clientes, y se originó en 1991 cuando el internet ingresó al comercio. Por otra parte, este autor también señaló cuatro generaciones del comercio electrónico, estas son las siguientes (Zwass, s.f.).

- Primera generación de 1993, se creó la web y solo indicó información de la compañía.
- Segunda generación, en esta comenzaron a darse las compras por internet.
- Tercera generación, esta automatizó el proceso de selección de productos, se habilitaron métodos de pago digitales y se realizó el *marketing* por red.
- Cuarta generación, esta mejoró la seguridad de los sitios y los métodos de pago se hicieron más seguros.

Con la primera generación del comercio electrónico, el EDI les permitía a las compañías intercambiar información, ejecutar órdenes y hacer transferencias

electrónicas de fondos a través de computadoras, sin embargo, la expansión de este modelo era lenta, y muy pocas compañías de Europa y EE.UU. lo habían adoptado debido a los grandes gastos en que se debía incurrir para estar conectado y algunos problemas técnicos. En 1991, cuando la NSFNETA decidió levantar las restricciones comerciales de uso de la red, y abrió paso a que el comercio electrónico se empezará a desarrollar sin limitaciones. La clasificación señalada demuestra el modo en que el comercio electrónico evoluciona a lo largo de los años, se minimizan riesgos y aumentan, significativamente, las compras por los medios electrónicos (Anteportamlatinam, 2014).

1.3 Tipos de comercio electrónico

De conformidad con Anteportamlatinam, (2014) y Espinosa (2020), existen diferentes tipos de comercio electrónico, estos se clasifican en valoración a distintos factores ¿quién interviene?, ¿de qué manera?, ¿qué tipo de intercambio realizan? Con base en lo anterior, existen las siguientes clasificaciones.

- B2C: se da cuando quien vende es una empresa y quien compra es un consumidor.
- B2B: se materializa cuando el vendedor y el comprador son empresas.
- C2C: sucede cuando el vendedor y el comprador son consumidores.
- C2B: se da cuando el consumidor le vende a una empresa.

No obstante, para el presente trabajo la clasificación más relevante es B2C, esto por el desarrollo que ha tenido, es el supuesto que se puede llevar a cabo con mayor facilidad en la cotidianidad y los riegos tienen más probabilidades de materializarse; por

lo mencionado, es preciso enfocarse en esta clasificación con la explicación expuesta a continuación.

Business to consumer (B2C)

Son las actividades que se dan, tradicionalmente, por medios electrónicos y digitales entre empresas y sus clientes, donde se ofrecen productos con una promoción de estos a partir de alguna herramienta digital; dicha herramienta puede ser una página web, esto hasta que se realice la transacción en la que se intercambia el bien o servicio por una contraprestación económica. En este caso, se le denomina al consumidor como "ciberconsumidor", este consta de varios modelos de acuerdo con *Shopify Business* (*2020*), estos son los siguientes.

- Vendedores directos: son tiendas en línea donde el creador del producto (la empresa) realiza la transacción con el consumidor.
- Intermediarios en línea: son herramientas electrónicas que ayudan al vendedor y al comprador a contactarse para que celebren el negocio.
- Basados en la publicidad: es una herramienta para que el consumidor ingrese al sitio web de la empresa.
- Basados en la comunidad: es un mecanismo para que las comunidades digitales ayuden a las empresas a publicitar sus bienes o servicios.
- Basados en una cuota: son medios digitales que le cobran una cuota al consumidor para acceder a su contenido.

Por consiguiente, estos modelos entre una empresa y un consumidor son los que tienen más probabilidades de que se materialicen los riesgos, y requieren de más cuidado al tratarse con clientes.

1.4 Procedimiento del comercio electrónico

Es necesario hacer la respectiva división de los procedimientos del comercio electrónico, uno es el que la empresa debe ejecutar para tener una herramienta digital y ofrecer sus productos o servicios, y otro lo hace el consumidor para adquirir el respectivo producto. La empresa que quiere ofrecer y publicitar por medios electrónicos debe seguir los siguientes pasos según (Trabado, 2018).

- Crear el mecanismo *online* con un respectivo nombre y el dominio de este, es decir, la dirección de la página web.
- Seleccionar los productos o servicios que se buscan comercializar en la plataforma.
- Contratar un *hosting* que busca garantizar una buena conexión y tener un buen posicionamiento en los buscadores.
- Elegir una plataforma tecnológica.
- Definir las pasarelas de pago por parte del consumidor, estas pueden ser tarjetas de crédito o débito, PayPal, pago aplazado y transferencia *online*.
- Se debe tener un servicio de envío del producto.
- Señalar unos plazos de entrega.

Por otra parte, conforme con lo señalado por la página Equipo Woko (2018), el proceso del consumidor para obtener los productos o servicios deseados es el siguiente.

- Buscar el producto que se desea, esto con el acceso a sus funcionalidades y características.
- Indicar, en el carrito de compra, el producto que se quiere adquirir.

- Llenar el respectivo formulario para realizar la compra donde se debe señalar la información personal.
- Determinar el método de pago para finalizar con la orden de compra.

Cada procedimiento corresponde a los implicados en el negocio jurídico que se celebra con el comercio electrónico: el de la empresa que ofrece los bienes o servicios y consta de crear una página web, generar un catálogo de los productos, gestionar una pasarela de pagos y realizar el envío del producto. El del usuario que quiere adquirirlos, en el que se elige el producto, se llena el formulario con sus datos para la factura y el envío, y se procede con el pago; en este orden de ideas, cada uno de los dos procedimientos puede tener ventajas y desventajas para las partes implicadas.

1.5 Ventajas y desventajas del comercio electrónico

Al mencionar las ventajas y las desventajas del comercio electrónico, se busca indicar cuáles son los riesgos que más se deben tener en cuenta a la hora de hacer uso de las plataformas digitales y electrónicas. En concordancia con Peña (2019), las ventajas son mucho mayores frente al comercio tradicional, por lo que supone un asunto competitivo y una oportunidad de negocio; entre muchas otras están las siguientes.

- Superación de limitaciones geográficas.
- Obtención de mayor número de clientes por la visibilidad.
- Costo menor al negocio tradicional.
- Mayor facilidad, por parte de la empresa, de mostrar sus productos.
- Mayor facilidad y rapidez para encontrar productor por parte del consumidor.

No obstante, Malca (2001) planteó que, entre las desventajas que interesan en el presente trabajo de grado, se encuentran las expuestas a continuación:

- La seguridad de la información se puede ver comprometida.
- La empresa puede no contener una buena política de tratamiento de los datos de las personas.
- La empresa debe tener convenios con los bancos para realizar los pagos electrónicos por las pasarelas de pago señaladas.
- Falta de confianza en la recepción y devolución de los productos.

A modo de cierre del presente capítulo, es importante mencionar que para esta investigación se empleó la definición contenida en el Programa de Trabajo sobre el Comercio Electrónico adoptado por la OMC en 1998: “la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos”; en consecuencia, después de haber identificado una definición al término de comercio electrónico, sus tipos, ventajas y desventajas, fue preciso realizar una recopilación de la normatividad de esta institución, esto es desarrollado en el segundo capítulo. Esta recopilación normativa contiene la regulación nacional colombiana, la regulación internacional y expone cómo se despliega el comercio electrónico desde el derecho comparado; lo anterior con el propósito de observar el proceso que esta figura tiene en el marco normativo a nivel nacional e internacional, y así delimitar qué riesgos han sido tratados, o no, y regulados por estas (Herreros, 2019).

Capítulo 2. Regulación internacional y nacional del comercio electrónico y sus ámbitos de aplicación

Ahora bien, en consideración con los conceptos generales del comercio electrónico, en este acápite se procede con un análisis de la normatividad vigente a nivel nacional e internacional; lo primero que se revisó fue el marco jurídico expedido en Colombia y que regula este tema en específico, asimismo, se examinó el marco normativo a nivel internacional. En concordancia con esto, en un primer lugar se indagó la regulación internacional de América Latina y el Caribe, y, consecuentemente, algunos acuerdos multilaterales y un análisis de derecho comparado entre distintas jurisdicciones; así, esto se efectuó para distinguir cómo se ha regulado el comercio electrónico en el mundo y en los distintos órganos jurisdiccionales y de derecho comunitario.

2.1 Normatividad nacional

Fundamentalmente, se debe plantear la regulación constitucional que ofrece garantías y establece límites del comercio electrónico, consagrados estos en las siguientes normas de la Constitución Política de Colombia.

- Artículo 15: señaló el derecho a la intimidad personal y familiar, y a su buen nombre, de esto se deriva el *habeas data*.
- Artículo 20: indicó la protección de la libertad de expresión, uno de los pilares del comercio electrónico.

- Artículo 333: consagró que la actividad económica y la iniciativa privada son libres dentro de los límites del bien común, e ideó que, para su ejercicio, solo con la autorización de la ley alguna persona podrá exigir permisos previos o requisitos.

En este sentido, a continuación, se presenta la regulación legislativa y reglamentaria.

- Ley 222 de 1995, fue la primera en mencionar los medios electrónicos, esbozó que los accionistas de las sociedades podían realizar su reunión ordinaria por medios digitales.
- Ley 270 de 1996, esta se ocupa de que la administración de justicia pueda hacer uso de la tecnología por cualquier medio para el cumplimiento de sus funciones.
- Ley 527 de 1999, esta fue nombrada la ley del comercio electrónico, mediante ella se estableció el principio de equivalencia constitucional entre la firma electrónica y la autógrafa, y a los mensajes de datos y los documentos escritos; a su vez, indicó los requisitos para la certificación de firmas digitales y la existencia de unas entidades de certificación; esta ley fue reglamentada con el Decreto 2364 de 2012, donde se desarrolló el mecanismo de firma electrónica y se aclaró su alcance.
- Ley 633 de 2000, consagró que las páginas web y sitios de internet de naturaleza comercial, financiera o de prestación de servicios, que tengan como origen a Colombia, deben ser inscritos en el Registro Mercantil y suministrar a

la Dirección de Impuestos y Aduanas Nacionales (DIAN) la información que esta entidad requiera.

- Ley 962 de 2005, esta buscó la utilización de medios electrónicos en los procesos de facturación.
- Ley 1150 de 2007, reglamentó la Ley 80 de 1993, se instituyó el sistema electrónico de contratación pública (SECOP).
- Ley 1266 de 2008, determinó la protección del *habeas data*, dirigido este para los servicios financieros, señaló la relevancia de tener seguros los datos para calcular el riesgo crediticio de las personas; esto fue reglamentado por el Decreto 1727 de 2009 y el Decreto 2952 de 2010.
- Ley 1331 de 2008, indicó que la factura es un título valor, por lo tanto, en cuanto a la facturación electrónica se expidió el Decreto Reglamentario 2242 de 2015, con el fin de recalcar la interoperabilidad de esta.
- Ley 1273 de 2009, se ocupó de las consecuencias en el ámbito penal, con la búsqueda de la seguridad entre los usuarios de las plataformas digitales.
- Ley 1480 de 2011, con esta se creó el Estatuto del Consumidor y se desarrolló lo concerniente con las transacciones electrónicas para amparar a los consumidores.
- Ley 1581 de 2012, estableció el Régimen General de Protección de Datos Personales regulado con el Decreto 1377 de 2013 y el Decreto 886 de 2014.
- Decreto 1078 de 2015, es el Decreto Único Reglamentario del sector de las TIC, fue modificado por el Decreto 1008 de 2018 que instauró los elementos

fundamentales para el desarrollo de esta, busca la confidencialidad, la integridad, la disponibilidad y la privacidad de los datos.

- Ley 1955 de 2019, con esta se señaló el Plan Nacional de Desarrollo de 2018-2022, en su Artículo 147 consagró la inclusión y la actualización permanente de políticas de seguridad y confianza digital.

De acuerdo con el catálogo de normas mencionado anteriormente, se seguirá la explicación de cada una de las normas señaladas de una manera cronológica y teniendo en cuenta su relevancia para el tema del comercio electrónico, esta explicación estará conformada de un análisis que se le hizo a cada una de las normas, identificando así sus puntos más importantes para este trabajo.

La Ley 527 de 1999 es la ley del comercio electrónico, esta desarrolló temas muy importantes para el comercio electrónico, regula todo lo que tiene que ver con los documentos y la firma electrónica, mensajes de datos, su reconocimiento jurídico, además, cómo esta información puede acarrear una celebración de un contrato por medios digitales, entre otros temas de gran relevancia. Esto deja a Colombia como un país pionero en América Latina en esta temática, pues la ley se expidió con sustento en la Resolución 51/162 de 1996 de la Asamblea General de Naciones Unidas, en consideración con las discusiones realizadas en la Comisión de Naciones Unidas, donde se contempló el derecho mercantil internacional y se crearon mecanismos para su implementación en Colombia (Flórez, 2014).

Ahora bien, se estudiaron los diferentes principios que la Ley 527 dictó, al igual que la equivalencia funcional para darle la validez, indicada con anterioridad, a los mensajes de datos; estos son los siguientes.

- El principio de neutralidad tecnológica: alude a que no interesa la fuente tecnológica por la que se expide el mensaje de datos, puesto que todas tienen igual trascendencia, lo fundamental es su cumplimiento con los requisitos señalados en la ley para su validez jurídica; esta noción adquiere relevancia hacia el futuro, cada vez el hombre crea nuevas tecnologías mejoradas e innovadas. Este principio también fue delimitado en la Sentencia 662 de 2000 de la Corte Constitucional con Magistrado Ponente Fabio Morón Díaz, donde se indicó que los mensajes de datos no eran definidos por una determinada tecnología, por lo tanto, se tuvo en cuenta el desarrollo de nuevas TIC, para potenciar este elemento principal del comercio electrónico.

  Esta sentencia estableció el carácter constitucional de la Ley 527 de 2000, y fue esencial para el comercio electrónico, hizo énfasis en la recomendación de la Ley Modelo sobre el Comercio Electrónico (LMCE) de la Comisión de Naciones Unidas para el Desarrollo del Derecho Mercantil; lo anterior precisó que su implementación es modelo para volver más ágil las relaciones comerciales internacionales.
- El principio de equivalencia funcional sobre los documentos electrónicos, este otorga un reconocimiento jurídico, se le concede la validez jurídica que tiene un documento, de esta manera, se le asemeja con los documentos escritos, con una seguridad jurídica para quienes hacen uso de estos mecanismos a la hora de

celebrar un negocio. Asimismo, se emplean unos requisitos para estos documentos, estos son los presentados a continuación.

- La confiabilidad en la forma en que fue generado, archivado o comunicado el documento con el mensaje de datos, es decir, la credibilidad de que el documento no ha sido alterado desde su emisión y tiene la trazabilidad de quien lo tramitó, para así adquirir este carácter de seguridad, eficacia y validez. También es importante resaltar que se deben tener medidas de seguridad para la autenticación del sujeto que transmitió el documento, como lo puede ser una firma digital debidamente certificada; no obstante, se deberá tener en cuenta que el juez es quien determina la fiabilidad del mensaje de datos, esto con los elementos indicados y el caso objeto de análisis.
- La integridad de la información, en otros términos, que no haya sido alterado después de su emisión por el sujeto de derecho; en la Sentencia de Sala de Casación Civil del 16 de diciembre de 2010, con Magistrado Ponente Octavio Munar Cadena, se hizo alusión a este requisito con el argumento de que este documento electrónico debe permanecer con la información integral con la que fue emitido, sin ningún tipo de adición o alteración. El documento, al no coincidir con el original, no es jurídicamente seguro, por lo tanto, no es válido; en otro orden de ideas, se trata la autenticación digital del sujeto que emite el mensaje de datos por alguna herramienta digital.
- El requisito de identificación del emisor del mensaje de datos, en vista de que la autenticación de la identidad del sujeto que transmitió el mensaje de datos es vital, al ser identificado el documento adquiere mucha más seguridad jurídica y

confiabilidad para los jueces, en caso de que tengan que determinar su equivalencia funcional, y para la otra parte con la que se celebró el negocio jurídico, o simplemente a quien fue dirigido dicho mensaje de datos. Para este punto, se pueden emplear muchos métodos digitales que corroboren la identidad del sujeto, lo más importante es que sean lo suficientemente eficaces para cumplir a cabalidad con este requisito.

- Por último, de acuerdo con Suñe (2006), desde la doctrina puede llegar a existir un cuarto requisito basado en la confidencialidad de la información emitida. En este requerimiento, la información solo podrá ser conocida por el destinatario, porque se puede tratar de información altamente valiosa para el emisor.

En tal marco, se debe tener en cuenta la diferenciación entre la firma digital y la electrónica, pues ambas están cobijadas con la validez otorgada por la Ley 552; la firma digital es aquella que es concedida por una entidad pública certificada para estos fines, la encargada de realizar la verificación de que quien firme un documento sea efectivamente el dueño de la firma digital, esto con unos medios de seguridad y con lo consagrado en la Sentencia 662 de 2000 de la Corte Constitucional sobre la importancia de la identificación de un individuo como emisor de un documento electrónico o mensaje de datos. Esta herramienta de firma digital emana certidumbre para los usuarios de las tecnologías, y aún más para el destinatario de dicho documento, destaca la importancia de tener un mecanismo de tecnología que autentique, digitalmente, a la persona que emite el mensaje de datos.

Ahora bien, la firma electrónica, tal y como lo señaló dicha ley, instituye, generalmente, el requisito de firma que los documentos tienen y el mecanismo requerido

para distinguir al emisor. No es precisamente la firma digital con su respectivo certificado, este es un método de firma electrónico, es decir, solo uno de los tantos mecanismos de autenticación de identidad que se pueden efectuar con la tecnología como medio confiable. Asimismo, el Decreto 2364 de 2012 desarrolló el mecanismo de firma electrónica y aclaró su alcance; indicó lo siguiente sobre los mecanismos: *"*códigos, contraseñas, datos biométricos o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos" (Artículo 1).

Como se puede observar en el aparte citado, se promueven herramientas para utilizar la firma electrónica que aporta validez al documento jurídico; por otro lado, también es necesario indicar que, en el Decreto 2364, se esbozó la potestad de los implicados de convenir diferentes métodos de firma electrónica, comunicarse, enviar mensajes de datos, realizar documentos electrónicos, o cualquier actividad relacionada a un ámbito tecnológico y digital. En esta normatividad se señalaron algunos requisitos para que esta firma electrónica sea confiable, en correspondencia con Flórez, (2014) estos son los siguientes.

a) Los datos con los que se crea la firma son los datos personales del emisor y firmante.
b) Existe la forma hallar, si es el caso, una alteración del mensaje de datos después de firmado.

Igualmente, es inevitable resaltar la Ley 1341 de 2009, que, si bien tiene un enfoque general, es muy importante para el comercio electrónico, mediante esta se expidieron los principios sobre la información y la organización de las TIC; uno de sus aspectos más relevantes es ser el sustento para el sector de la tecnología que impulsa

la libre competencia y la protección de los derechos de los usuarios, así como se fundan limitantes para el desarrollo de políticas públicas en este ámbito. Por otra parte, se considera necesario exteriorizar el marco normativo de las TIC que ha estado en los últimos años en proceso, esto gracias a la constante actualización tecnológica que aumentan los mecanismos para celebrar negocios jurídicos, esto materializa la figura del comercio electrónico.

Las normas con todo lo relacionado con las TIC son las siguientes: la primera a tener en cuenta es la Ley 222 de 1995, esta reglamentó la junta de accionistas de una sociedad por medios electrónicos, con esto se comenzó a notar, en el ámbito de las comunicaciones a nivel societario, la presencialidad de sujetos de derecho a través de la virtualidad. La segunda es la Ley 1150 de 2007, esta decretó la Ley 80 de 1993, y estableció el SECOP; conforme con Vásquez y Valencia, (2019), es una de las primeras leyes donde se tratan conceptos propios de comercio electrónico con una vinculación entre el derecho de las TIC y el administrativo.

En tal marco, una tercera norma a sobresalir es la regulación, desde el punto de vista penal, por intermedio de la Ley 1273 de 2009, esta busca la seguridad de los usuarios de las plataformas digitales en las que se celebran negocios jurídicos, tipifica delitos informáticos, y tutela el bien de protección de la información y de los datos. Desde esta Ley se comenzó a fijar la relevancia de los datos personales de los sujetos, y su relación con el comercio electrónico.

De conformidad con lo establecido en la Ley 222 de 1995, otra de las regulaciones en este ámbito del comercio electrónico ha sido la facturación electrónica, y, según la Ley 962 de 2005, como bien lo desarrollaron Vásquez y Valencia, (2019), busca la

utilización de medios electrónicos en los procesos de facturación de un documento electrónico. Por consiguiente, surgió la Ley 1331 de 2008, esta planteó que la factura electrónica es un título valor, por lo tanto, se expidió el Decreto 2242 de 2015 en cuanto a la facturación electrónica, recalcó la necesidad que esta se desarrolle con la herramienta de interoperabilidad; cabe mencionar que este es un tema altamente concerniente con el comercio electrónico, es otro de los mecanismos favorecedores del intercambio de bienes y servicios por esta plataforma, esto hace más ágiles estos procesos sin requerir ningún tipo de contacto físico.

Adicionalmente, el derecho de los titulares frente a sus datos personales, consagrado en los Artículos 15 y 20 de la Constitución Política, cobró gran importancia en los últimos años, se logró ver que la información es un activo económico para las entidades públicas y privadas, entonces, con la Ley 1266 de 2008 se creó el *habeas data*, empero, dicha ley se enfoca, principalmente, en datos de carácter financiero o comercial, historial crediticio o de servicios. Análogamente, se encuentra la Ley 1521 de 2012 y su respectivo Decreto Reglamentario 1377 de 2013, esta es fundamental al encargarse de desarrollar el derecho constitucional de *habeas data*. La ley trajo consigo 7 definiciones para tratar las demás temáticas, dichas conceptualizaciones se muestran a continuación.

a) Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
b) Base de datos: conjunto organizado de datos personales y objeto de tratamiento.

c) Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

d) Encargado del tratamiento: persona natural o jurídica, pública o privada, que por sí misma, o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable de este.

e) Responsable del tratamiento: persona natural o jurídica, pública o privada, que por sí misma, o en asocio con otros, decida sobre la base de datos y/o el tratamiento de estos.

f) Titular: persona natural cuyos datos personales sean objeto de tratamiento.

g) Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, el almacenamiento, el uso, la circulación o la supresión.

Similarmente, la ley implica unos principios que deben orientar el tratamiento de los datos personales, estos son los expuestos a continuación.

- Principio de legalidad en materia de tratamiento de datos: el tratamiento de la presente ley es una actividad reglada, sujeta a lo establecido en ella y en las demás disposiciones que la desarrollen.
- Principio de finalidad: el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, esta debe ser informada al titular.
- Principio de libertad: el tratamiento solo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

- Principio de veracidad o calidad: la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- Principio de transparencia: en el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- Principio de acceso y circulación restringida: el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley; los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme con la presente ley.
- Principio de seguridad: con la información sujeta a tratamiento por el responsable o encargado de este, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. (Ley Estatutaria 1581 de 2012, Artículo 2)

Por último, es muy significativo el tema de las políticas de tratamiento de datos, estos son documentos que deben ser elaborados por los responsables del tratamiento y contienen toda la información asociada a este. Es necesario valorar que, en materia jurisprudencial, se han regulado situaciones que se pueden presentar en la plataforma digital, tal y como se observa en la Sentencia SU 420 de 2019, con la que la Corte Constitucional estableció pautas para delimitar el ejercicio de la libertad de expresión en las redes sociales, donde el juez debe intervenir, excepcionalmente, en caso de ser preciso, para proteger los derechos de la honra y buen nombre.

En tal marco, la Ley 1480 de 2011 es relevante para el comercio el electrónico, regula el Estatuto del Consumidor y la protección de los consumidores cuando están en una relación de consumo, sus derechos y deberes, al igual que las obligaciones de los proveedores de los bienes y servicios, asimismo, en su Artículo 49, instauró una definición de comercio electrónico, conexa esta con la acogida en el presente trabajo de grado. También, uno de los puntos más relevantes de esta norma es la potestad del consumidor para cancelar o revertir el pago en las siguientes situaciones.

- Cuando este haya sido objeto de un fraude.
- Cuando el cobro se base en una operación que no solicitó.
- Cuando no haya recibido el servicio o bien contratado.
- Cuando el bien o servicio, objeto del negocio jurídico celebrado sea diferente al entregado o prestado.

De este modo se ve regulado el comercio electrónico, cada vez tiene más requisitos y materias para tener en cuenta a la hora de ofrecer bienes y servicios por plataformas digitales, y su incumplimiento acarreará las sanciones dispuestas en el

ordenamiento jurídico. Ahora bien, después de todo lo analizado, se debe resaltar la expedición del CONPES 3995 de 2020, con el que se determinó la importancia de una política nacional de confianza y seguridad digital con objetivo de establecer medidas para ampliar y mejorar dicha confianza y seguridad, esto porque en el sector público y privado se debe actualizar el marco de gobernanza para aumentar el desarrollo y la efectividad de las plataformas digitales.

A lo largo del estudio ejecutado en el presente documento, se logró evidenciar que el nivel de dependencia de los ciudadanos colombianos al internet es alto, sin embargo, su nivel de confianza es bajo, y, aunque se demuestra la implementación de políticas en el pasado para mejorar esta situación, estas no han sido efectivas, Colombia se encuentra por debajo del promedio global en la evaluación sobre el índice de evolución digital, lo que afecta el intercambio de bienes y servicios. Las políticas mencionadas se basaron en la legislación y en el desarrollo de capacidades gubernamentales, no obstante, no generaron progreso en otros sectores ni directamente con los ciudadanos, en vista de que estas partes interesadas no se vieron involucradas con el proceso de las anteriores políticas. Debido a lo anterior, con el CONPES 3701 del año 2011 que fijó *"*lineamientos de política para ciberseguridad y ciberdefensa*",* se llevó a cabo lo proyectado a continuación.

Se crearon los siguientes entes.

- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT).
- El Centro Cibernético Policial (CECIP).
- El Comando Conjunto Cibernético (CCOCI).

- Se realizó una capacitación especializada para las instituciones del Gobierno Nacional.
- Se fortaleció la legislación.
- Se promovió la colaboración internacional.

Pero estas políticas, al enfocarse, principalmente, en el desarrollo de capacidades gubernamentales, no suscitaron progresos en otros sectores o con los ciudadanos. También es pertinente hacer alusión a la existencia de un ente privado, la Cámara Colombiana de Comercio Electrónico, esta promueve el comercio electrónico en Colombia con el uso y desarrollo de nuevas TIC, ayuda a la implementación de buenas prácticas y a la generación de confianza en los usuarios.

Análogamente, con el CONPES 3854 del 2016 que señaló la *"*política nacional de seguridad digital*"*, se desarrollaron estrategias que establecieron un marco institucional de seguridad digital (con base en la gestión de riesgos) y se creó el Coordinador Nacional de Seguridad Digital. Esta política, al dirigirse, especialmente, al Gobierno, conllevó a que no hubiera gestión frente a los convenios y los acuerdos de cooperación e intercambio de información con las partes interesadas; en esta línea hay que tener en cuenta que, con el Decreto 1008 del 2018, se instituyeron lineamientos de la Política de Gobierno Digital, esto para la seguridad de la información como uno de los elementos fundamentales para el desarrollo de esta, con la confidencialidad, la integridad, la disponibilidad y la privacidad de los datos. Además, en la Ley 1955 de 2019 se diseñó el Plan Nacional de Desarrollo de 2018-2022, y en su Artículo 147 decretó la inclusión y la actualización permanente de políticas de seguridad y confianza digital.

En el CONPES 3995 se entiende como confianza la probabilidad suficientemente alta de que un actor externo realice una acción beneficiosa y no perjudicial, por lo tanto, la confianza digital es la calidad de interacción basada en la seguridad, la privacidad, la transparencia y las buenas prácticas efectivas que pueden llegar a ser exigibles. Este tema es vital, pues, a medida que las plataformas y la tecnología avanzan, se dan los ciberataques y las vulnerabilidades tecnológicas donde los ciudadanos, las empresas y las entidades públicas se ven expuestos a amenazas de seguridad digital.

En Colombia se pueden generar diferencias sociales de seguridad digital para los grupos poblacionales más vulnerables, en virtud de que, al tener una baja interacción con la tecnología, tienen menos posibilidades de prevenir estas situaciones, por ende, el CONPES determinó la necesidad de desarrollar políticas que tengan en cuenta todas estas problemáticas plasmadas, donde se busque la adopción de modelos, estándares y marcos de trabajo que no entorpezcan la aparición de nuevas tecnologías en el futuro, y permitan al Estado enfrentar amenazas y ataques de alta complejidad y sofisticación. En tal óptica, se fijó un plan de acción y seguimiento en el que participaran todas las entidades competentes, esto para fortalecer las capacidades de seguridad digital en el sector público y privado, y actualizar el marco de gobernanza. Así, se patentiza cómo, a lo largo de los años, las tecnologías han adquirido importancia y generando riesgos para los usuarios de plataformas digitales, donde el ordenamiento jurídico ha tenido que ejecutar un seguimiento minucioso para mitigar los riesgos que perjudican a los implicados en este ámbito.

2.2 Regulación internacional del comercio electrónico

En esta sección se realiza una recopilación de la regulación internacional del comercio electrónico, se hace una pequeña introducción acerca de la LMCE considerada como un pilar de la regulación del comercio electrónico internacional; luego se efectúa una compilación de la regulación internacional de América Latina y el Caribe, con el fin de proceder a un marco jurídico multilateral que se ha creado como moderador de las temáticas que giran en torno al comercio electrónico. Por consiguiente, se describe la regulación que la Unión Europea (UE) tiene frente al comercio electrónico, esta es un organismo de derecho comunitario que ha avanzado mucho frente a esta temática; después se alude a la Convención de Roma en la ley aplicable a las obligaciones contractuales, y se finaliza con unos comentarios sobre derecho comparado y una conclusión del capítulo.

En tal óptica, en 1996 se creó la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), esta publicó una LMCE (Naciones Unidas, s.f.), luego enmendada por la Convención sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2005 (Naciones Unidas, 2005). Esta ley buscó establecer un conjunto de reglas internacionales encaminadas a eliminar los obstáculos jurídicos que se presentan en el comercio electrónico, esto con normas para la formación y la validez de los contratos realizados por los medios electrónicos.

2.2.1 Regulación internacional en países en América Latina y el Caribe

Algunos de los países de América Latina que han promulgado una legislación doméstica, basada en la Ley Modelo, son: Colombia, El Salvador, Guatemala, Honduras, Panamá, Paraguay, República Dominicana y Venezuela.

Esta ley trata los 4 pilares fundamentales de las transacciones de comercio electrónico que son: (a) equivalencia de datos, (b) equivalencia de documentos, (c) equivalencia de formalidad, (d) paridad contractual (Ferrari, 2017). Según Rengifo, 2000), 5 pilares primordiales integran la LMCE, estos son los proyectados a continuación.

- Facilitar el comercio entre países y al interior de cada uno de ellos.
- Validar las operaciones efectuadas con las nuevas tecnologías de la información.
- Fomentar y estimular la aplicación de nuevas tecnologías de la información.
- Promover la uniformidad del derecho.
- Apoyar las prácticas comerciales. (p. 32)

Ahora bien, un organismo de derecho comunitario que se ha encargado de regular las relaciones internacionales de comercio electrónico en América Latina es la Comunidad Andina de Naciones (CAN), que ha expedido las siguientes normas:

- Decisión 486, Régimen Común sobre Propiedad Industria: esta entró en vigor a partir del 1 de diciembre del 2000; en su Artículo 233 regula aspectos relacionados con las marcas comerciales y los nombres de dominio de internet.

- Decisión 691, de la CAN, del 13 de agosto del 2008, estadísticas sobre las TIC: en esta decisión se estableció un marco para la producción de estadísticas sobre el uso de las TIC.

Similarmente, la Alianza del Pacifico en el Protocolo Comercial, suscrito en 2014 y vigente desde 2016, incluyó un capítulo sobre comercio electrónico, este sigue de cerca el modelo del Tratado Integral y Progresista de Asociación Transpacífico (CPTPP), en vigencia, entre 6 de sus 11 signatarios, en diciembre de 2018; ello no resulta sorprendente, pues 3 miembros de la AP (Chile, México y Perú) son también signatarios del CPTPP. Por lo tanto, se debe tener en cuenta lo señalado por Herreros (2019).

El Mercado Común Centroamericano también dispone de un marco normativo básico para el comercio electrónico, establecido en el capítulo respectivo del tratado de libre comercio entre los Estados Unidos, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y la República Dominicana (conocido como DR-CAFTA, por su sigla en inglés). Este acuerdo, suscrito en 2004, es de naturaleza plurilateral, su capítulo sobre comercio electrónico establece la no imposición de aranceles a los productos digitales transmitidos electrónicamente. El capítulo no contiene compromisos vinculantes sobre el entorno regulatorio del comercio electrónico (protección de datos personales, protección del consumidor, firma electrónica, entre otros), si bien se señala que las partes compartirán información y experiencias sobre esos temas. Al igual que en la AP, estimula al sector privado a desarrollar mecanismos de autorregulación. (p. 32)

En este orden de ideas, Mercosur (Mercado Común del Sur) es un bloque económico conformado por varios países sudamericanos y creado con el objetivo de

aumentar la eficiencia y la competencia entre las economías incluidas; actualmente está integrado por Argentina, Brasil, Paraguay, Uruguay, Venezuela y está en proceso de adhesión Bolivia. Los países constituyentes suscribieron el Acuerdo sobre Comercio Electrónico luego de la serie de discusiones dentro del subgrupo de trabajo N. 13 comercio electrónico.

El Acuerdo sobre Comercio Electrónico del Mercosur es el primer ordenamiento normativo del bloque en materia de comercio electrónico multilateral. Busca garantizar las condiciones para la transferencia transfronteriza de información por medios electrónicos, la ubicación de las instalaciones informáticas, la protección de datos personales, la protección al consumidor en línea, el acceso y uso de internet para el comercio electrónico, autenticación y firmas digitales, comunicaciones comerciales directas no solicitadas, facilitación del comercio electrónico y cooperación. (MIC, 2020, p. 2)

Este acuerdo implica la expansión del horizonte de oportunidades para todo tipo de empresas de los distintos sectores, y en consecuencia la generación de un importante valor agregado, permitiendo a los países del Mercosur ampliar la escala de negocios con la eliminación de restricciones a las transacciones comerciales. (MIC, 2020, p. 3)

2.2.2 Marco normativo multilateral

En relación con la normatividad internacional, se inició con la LMCE de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional

(CNUDMICNUDMI) de 1996. Este documento representó las bases de regulación del comercio electrónico. Esta Ley Modelo tiene los siguientes 2 objetivos.

- Ofrecer a los legisladores de los ordenamientos jurídicos un conjunto de reglas internacionales, esto para crear un ambiente legal más seguro para el comercio electrónico y facilitar su uso.
- Mejorar el tratamiento igualitario entre los usuarios de la documentación en papel y los que usen documentación electrónica o digitalizada.

Otro tratado multilateral es el Centroamérica - Asociación Europea de Libre Comercio (AELC), en su Artículo 1.8 apuntó al comercio electrónico y cómo las partes reconocen el creciente rol de este. Por otra parte, se realizaron las negociaciones plurilaterales sobre comercio electrónico lanzadas en enero del 2019 en la OMC, donde los países participantes fueron Argentina, Brasil, Chile, Colombia, Costa Rica, El Salvador, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Uruguay. A continuación, se señalan los acuerdos preferenciales suscritos que regulan el comercio electrónico internacional.

a) Con Estados Unidos existen seis acuerdos suscritos que consagran la prohibición de cobrar aranceles a los productos digitales transmitidos electrónicamente, estos de primera generación con Chile, Colombia, Perú, Centroamérica y Panamá entre 2003 a 2007. Asimismo, en el 2018 se suscribió un acuerdo con más obligaciones que indicaron una mayor regulación de estos.
b) El Acuerdo 38 de 2012, suscrito entre la UE, Colombia y Perú, contiene muy pocas disposiciones sobre comercio electrónico, estas constan de protección

de información personal, publicación y aceptación digital de documentos relacionados con el comercio, y adopción de medidas de protección para el consumidor que use plataformas digitales.

Similarmente, la CNUDMICNUDMI-CNUDMI expidió una Ley Modelo de la firma electrónica que fue adoptada el 5 de julio de 2001, su propósito fue facilitar el uso de las formas electrónicas. Específicamente, en el contexto de actividades comerciales internacionales, pero no otorgó ninguna norma de derecho destinada a la protección de consumidores. Por su parte, la Organización para la Cooperación y el Desarrollo Económico (OCDE) creó, en 1998, una Guía del Comercio Electrónico (*Guideline of Electronic Commerce*), donde se determinaron las bases para la regulación de este en consideración con la materia de privacidad, la autenticación, la protección al consumidor y la fiscalidad, esta normatividad tampoco tuvo fuerza vinculante en Colombia. Estos documentos fueron decretados por el Comité de políticas de consumidor que representó el foro principal para la regulación del comercio electrónico a nivel global; dicha guía reglamentó lo siguiente.

Esta Guía fijo lineamientos que constituyen una recomendación dirigida a los gobiernos, empresarios, consumidores y sus representantes, sobre las características esenciales que debe contener una efectiva protección al consumidor en el comercio electrónico. Sin embargo, nada de lo que establecen los lineamientos debe restringir cualquier regulación que exceda sus disposiciones, ni impedir que los países miembros conserven o aprueben previsiones más estrictas para proteger a los consumidores en línea. En general, el propósito de los lineamientos es proporcionar un marco de referencia, así como un conjunto de principios que orienten: i) a los gobiernos para la

revisión, formulación e implantación de leyes, prácticas, políticas y regulaciones en materia de consumo, para lograr una efectiva protección del consumidor en el contexto del comercio electrónico; ii) a las asociaciones empresariales, grupos de consumidores y organismos autor regulatorios, proporcionándoles la orientación relativa a los principios básicos que deben considerarse en la formulación e instrumentación de esquemas de autorregulación en el contexto del comercio electrónico. iii) De manera individual a los empresarios y consumidores involucrados en el comercio electrónico, proporcionándoles una clara guía sobre las características fundamentales que debe contener la información que se difunda por este medio, así como de las prácticas comerciales equitativas que los empresarios deben realizar y que los consumidores tienen derecho a recibir en el contexto del comercio electrónico. (Organización para la Cooperación y el Desarrollo Económico , s.f., p. 2 - 3)

En el marco de la Organización Mundial del Comercio (OMC) se han negociado algunos acuerdos multilaterales que abarcan temas conexos con el comercio electrónico, estos se presentan a continuación.

- Acuerdo sobre Tecnología de la Información (ATI) de 1996, por el que 82 miembros de la OMC se comprometieron a no aplicar aranceles aduaneros a los productos del sector de las TIC.
- Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT).
- Acuerdo General sobre el Comercio de Servicios (AGCS).
- Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC).
- Acuerdo sobre Facilitación del Comercio, este entró en vigor en el 2017.

Estos acuerdos son considerados “tecnológicamente neutrales”, esto quiere decir que sus disposiciones se aplican independientemente del medio con el que se comercian los bienes o servicios, por ende, sus disposiciones son, en principio, plenamente aplicables al comercio electrónico (Wu,2017; OMC,2018). Pese a estos desarrollos en los acuerdos, al ser tan antiguos, cabe añadir que no logran solucionar las controversias y los retos generados con los nuevos modelos de negocio de los últimos años, por ejemplo, las enormes plataformas digitales y la inteligencia artificial; actualmente, la OMC no ha implementado ni realizado un nuevo programa de trabajo sobre el comercio electrónico, ni ha ejecutado una enmienda de los acuerdos existentes, y la creciente digitalización del comercio mundial hace que cada vez esto sea más urgente.

La LMCE, elaborada, en 1996, por la CNUDMI, es la base de las leyes sobre esta materia en 150 jurisdicciones y en 71 países, incluidos 22 de la región. A pesar de ser una Ley no vinculante, es uno de los primeros textos legislativos que adoptó principios fundamentales como la no discriminación, la neutralidad tecnológica y la equivalencia funcional, fundamentales estos en el comercio electrónico (CNUDMI, 2018); tal y como se mencionó, esta es la base de toda la normatividad colombiana. También se debe resaltar que esta ley contiene varias disposiciones importantes para tratar el comercio electrónico transfronterizo, esto en valoración con el reconocimiento jurídico de los mensajes de datos y la validez de la firma electrónica; posteriormente, estos conceptos fueron adoptados en la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales en el 2007.

Otra ley esencial es la Ley Modelo de la CNUDMICNUDMI, del 2017, sobre registros transferibles electrónicos, esta reconoció efectos jurídicos a documentos electrónicos permutables que sean equivalentes funcionales para instrumentos transferibles, esto para dar seguridad jurídica, puesto que estableció requerimientos para el uso de estos documentos, tales como las letras de cambio, los pagarés, los certificados de almacenamiento de depósito, entre otros. Así, la Organización Mundial de la Propiedad Intelectual (OMPI) expidió 2 instrumentos de relevancia denominados “tratados sobre internet”.

- Tratado sobre derechos de autor.
- Tratado sobre interpretaciones o ejecuciones y fonogramas.

Ambos tratados tienen como objetivo la aplicación de acuerdos como la Convención de Roma y el Convenio de Berna, los temas que se tratan en estos están relacionados con la revolución digital.

2.2.3 Unión Europea

Es necesario efectuar una recapitulación de la regulación que la Comisión de la UE ha realizado frente a el comercio electrónico, este es un organismo pionero en la protección de los consumidores de plataformas electrónicas; asimismo, conforme con lo señalado en el documento “comercio para todos, hacia una política de comercio e inversión más responsable”, dictado por la Comisión de la UE, se menciona lo siguiente.

> La UE es el mayor exportador e importador mundial de bienes y servicios considerados en su conjunto, el mayor inversor extranjero directo y el destino más

> importante de inversión extranjera directa (IED). Esta envergadura convierte a la UE en el mayor socio comercial de unos ochenta países y en el segundo socio más importante de otros cuarenta. La UE debe utilizar esta fortaleza en beneficio tanto de sus propios ciudadanos como de los de otras partes del mundo, especialmente los de los países más pobres. (Malmström, 2015, p. 1)

Debido a esto, fue de gran importancia hacer una explicación extensa de los avances regulatorios de este organismo, puesto que se ha encargado de romper las barreras que se generan en línea entre sus países miembros, esto para los individuos puedan disfrutar el acceso a todos los bienes y servicios que se ofrecen a través de la web; lo anterior ha logrado terminar con estas barreras trasfronterizas injustificadas y facilitar los envíos, esto ha suscitado una mayor protección a los consumidores, sus derechos y ha conseguido que se promueva el acceso a contenido *online*. Por estos motivos, cuenta con varias directivas reguladoras de estos temas específicos, estas se plantean a continuación.

1. Directiva del comercio electrónico de 2000/31/EC: esta comisión tiene como propósito proveer una infraestructura legal que facilite el funcionamiento del mercado del sistema interno europeo, y asegurar que los negocios y los consumidores sean beneficiados con el principio de libertad de circulación, libertad de establecimiento y libertad de servicios. Aun así, se debe recalcar que la directiva no estableció normas de derecho internacional privado de acuerdo con el Considerando 23 y el Artículo 1, apartado 4 de la Ley de Comercio electrónico.

De esta manera, las normas de derecho internacional privado de la UE influyeron en la redacción de esta Ley Directiva basada en el Artículo 49 del Tratado de la UE, así como en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, en este se instauraron los principios de control cuando se da un litigio comercial, donde el país de origen y el reconocimiento mutuo de las leyes son pilares elementales del mercado interior, esto en función del ordenamiento jurídico. Igualmente, se estableció, como principio de origen, la ley aplicable, esta adicional a una excepción en los contratos con los consumidores, donde estos tienen permitido demandar, en sus propios países, con la aplicación de la ley. No obstante, la directiva no interfiere con la liberad de las partes de elegir la ley, el foro aplicable y la aplicación, o no, del Reglamento 44 de 2001 de Bruselas del Consejo que regula la competencia, el reconocimiento, la ejecución en materia civil y asuntos comerciales, y la Convención de Roma de 1980 a la hora de celebrar un negocio jurídico (Rizzi, s.f.).

Esta directiva solo se aplica en las actividades de los proveedores de servicios dentro de la UE, empero, esta apunta que, con la dimensión global del comercio electrónico, se debe garantizar que las normas comunitarias sean coherentes con las internacionales (Rizzi, s.f.). Algunas acciones de la UE para que se facilite el uso de plataformas de servicios en internet son las siguientes.

- Crear normas que regulen los servicios de pago y de paquetería transfronterizos, esto mediante su Reglamento 644 del 2018.
- Diseñar nuevas reglas para detener el geobloqueo injustificado con su Reglamento 302 del 2018.

- Se crearon nuevas normas de impuesto al valor agregado (IVA) para las ventas *online* de bienes y servicios que entrarán en vigor a partir del 1 de julio del 2021, en vista de que, por las medidas tomadas en la pandemia, la aplicación de las nuevas reglas de IVA en el comercio electrónico se pospuso por 6 meses, esto para darle a los Estados miembros tiempo para prepararse. El IVA será simplificado para las compañías que llevan a cabo transacciones transfronterizas de bienes y servicios; estas nuevas normas garantizarán que los suministros se paguen de acuerdo con el principio de tributación en el Estado de destino.

La UE tiene reglas para eliminar el geobloqueo injustificado que previene a los usuarios de comprar a través de una página web de otro Estado miembro, por esto, para dicha prevención se ejecutaron las siguientes acciones.

- Por intermedio de la UE entró en vigencia el Reglamento de Bloqueo Geográfico 302 del 2018, este termina la discriminación con las plataformas digitales por la nacionalidad o al lugar de residencia, esto suscita que no hayan unas barreras infundadas, tales como ser redireccionado a la página web de cada país o pagar, únicamente, con tarjeta de crédito desde algunos países, también se consagró que los vendedores por internet deberán tratar a los consumidores de la UE por igual sin interés de dónde decidan comprar.
- Reglamento 2394 de 2017 sobre la cooperación entre las autoridades nacionales responsables de la aplicación de la normatividad en materia de protección de los consumidores.

- Reglamento sobre Servicios de Paquetería Transfronteriza 644 del 2018, este tiene los siguientes objetivos: 1) mejorar la supervisión regulatoria de los servicios de entrega de paquetes, 2) aumentar la transparencia de determinadas tarifas de una sola pieza con la publicación en un sitio web y 3) evaluar las tarifas de los servicios de paquetería transfronteriza.

En esta línea, se expidió el Reglamento de Protección de los Derechos de los Consumidores 2161 del 2019, este entró en vigor en 2020 y modificó la Directiva 13 CEE de 1993 del Consejo, y las Directivas 6 CE de 1998, la 29 CE de 2005 y la 83 UE de 2011 del Parlamento Europeo y del Consejo, esto en lo concerniente con la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la UE. El propósito de esta directiva es buscar la armonización de los Estados miembros para la seguridad jurídica de sus consumidores, por ende, fijaron unas sanciones más gravosas, es decir, de mayor cuantía, en caso de que se incumplan las normas por parte de los comerciantes, lo que implica para estos mayores obligaciones a la hora de realizar las transacciones, y genera un reconocimiento y protección a los consumidores en línea.

2. Directiva 7 OJ de ventas a distancia del 1997 (L 144), esta protege a los consumidores en materia de contratos celebrados a distancia, específicamente, las transacciones B2C. Para lo anterior es necesaria la cooperación entre Estados y organizaciones internacionales, con el fin de lograr armonía y regulación, y posibilitar las actividades comerciales por la red.

Cada vez que la tecnología avanza, el comercio electrónico también debe evolucionar, y conduce a que los Gobiernos y las entidades competentes para regular estas materias monitoreen, constantemente, estos desarrollos para adaptarse a futuras

reglas de cambio. Para esta directiva existe información básica que debe ser otorgada a los usuarios antes de que el contrato a distancia sea celebrado, estos datos son los siguientes.

- Tener el nombre y la dirección del proveedor.
- Las principales características de los bienes y los servicios.
- El precio de los bienes o servicios con impuestos.
- Los costos de envío.
- Arreglos para el pago de envíos y rendimiento.
- Posibilidad de aplicar el derecho de retracto.
- Duración del contrato.

En esta directiva se tiene como principal foco el tema de protección al consumidor y la ley aplicable a las obligaciones contractuales, el consumidor no puede renunciar a un derecho conferido por una directiva adherida a la legislación nacional; por consiguiente, es preciso que los Estados miembros tomen medidas para garantizar esta protección. Esta directiva fue modificada por la nueva Directiva (UE) 1995 del Consejo, aprobada esta el 21 de noviembre del 2019, esta transformó la Directiva 112 CE del 2006 en lo relativo con las disposiciones de las ventas a distancia de bienes y las entregas nacionales de estos; esta norma desarrolla los siguientes temas.

- Las situaciones donde se consideran las plataformas electrónicas que facilitan la compra y venta de bienes y servicios entre los usuarios, en esta medida, detallan la información que deben conservar estos negocios. También indica que los mercados en línea, en cuanto a las entregas de bienes, no están obligados al pago de un importe de IVA.

- Estas medidas simplifican el régimen del IVA vigente como el previsto para el comercio transfronterizo dentro de la UE, este consta del principio de tributación en el Estado miembro de destino, busca evitar los problemas que en cuanto a fraude, asimismo, reduce los costos de cumplimiento para las empresas.
- Por esta directiva es ineludible una actualización de programas informáticos de contabilidad y facturación, por lo tanto, se deberá tener en cuenta una inversión en el futuro en cuanto a la formación profesional para que se conozca acerca del nuevo sistema.

3. Directiva 93/EC de la firma electrónica 24 del 1999, esta facilita el comercio electrónico y asegura el funcionamiento del mercado interno con la posibilidad del uso de la firma electrónica avanzada, esta no se limita a una firma digital y es equivalente a una física, contribuye a su reconocimiento legal; en tal marco, se reglamentó toda una identificación y servicios de confianza para las firmas electrónicas. También, tal y como se observó en la normatividad colombiana, se efectuó una diferenciación entre firma electrónica y digital, donde la primera puede ser cualquier símbolo o marca originada electrónicamente con la intención de autenticar una acción, y la segunda emplea la criptografía de clave pública para garantizar la integridad de un documento durante su transmisión, estos se envían después de ser firmados y encriptados con una clave privada que solo el firmante posee.

Esta directiva fue derogada por el Reglamento del Sistema Europeo de Reconocimiento de Identidades Electrónicas 910/2014 (eIDAS) el 1 de julio del 2016; en

este reglamento se enmarcan un conjunto de normas destinadas a la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado europeo. Por otra parte, se estableció en el Reglamento 910/UE del Parlamento Europeo y del Consejo del 23 de julio de 2014, relativo esto con la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Este proporcionó el entorno regulatorio para los siguientes aspectos relacionados con las transacciones electrónicas.

- La firma electrónica avanzada: Es una firma que está vinculada al firmante de una forma única e intransferible permitiendo así su identificación, esta es creada utilizando personales y del exclusivo control de la persona quien firma, esta debe de estar ligada a los datos firmados en el documento impidiendo modificaciones posteriores. (Electronic identification, 2020).
- La firma electrónica cualificada: Tiene las mismas características de una firma electrónica avanzada el hecho diferencial es que en la firma electrónica cualificada se utiliza un dispositivo cualificado de firmas electrónicas para su creación. (Electronic identification, 2020).

Otro asunto que resulta esencial es la responsabilidad tratada en el Artículo 6 de la directiva, los Estados miembros deben asegurar que, si usan el servicio de un servidor certificado de certificación de firmas, este proveedor asumirá la responsabilidad por los daños causados a una entidad o persona jurídica o natural que, responsable y diligentemente, confió en dicha certificación. Por lo tanto, a ninguna firma electrónica se

le negará los efectos jurídicos o la admisibilidad en los tribunales por el mero hecho de no ser una firma electrónica avanzada o cualificada.

4. Directiva 46 de protección de datos 46 del 24 de octubre del 1995, esta se encargaba de la protección de personas naturales en cuanto a tratamiento de datos personales y a la libre circulación de los estos. Fue sustituida en el 2016 por el Reglamento General de Protección de Datos (RGPD) que entró en vigencia el 25 de mayo del 2016 y su cumplimiento se volvió obligatorio el 25 de mayo del 2018, este aplicado a todas las entidades con sede en un país miembro de la UE que procesen datos personales, por esto, no importa donde se encuentra ubicada la empresa, aplica el reglamento solo por el hecho de usar analíticas digitales para medir la navegación y los comportamientos digitales de un titular que se encuentra en la UE.

Para esta protección se despliegan varias actividades y conceptos, la evaluación de impacto sobre la privacidad es uno de los más importantes, en vista de que se deben determinar los riesgos específicos que supone tratar con ciertos datos de carácter personal y que prevén medidas para mitigarlos, y la protección reforzada de datos sensibles, principalmente, los genéticos y biométricos, pues sus infracciones pueden acarrear responsabilidad penal. Con respecto a la protección para los ciudadanos, las organizaciones, a la hora de tratar datos personales, deberán proporcionar más información y hacerlo de modo sencillo y entendible, esto para que la toma de decisiones de los ciudadanos sea más fácil, y se le dé el correcto cuidado a los datos personales de los menores de edad.

En este orden de ideas, el consentimiento debe ser claro, inequívoco, libre y revocable (este se puede revocar en cualquier momento, se puede solicitar la eliminación de los datos contenidos en redes sociales o buscadores de internet) al tratar los datos de carácter personal, y no se admiten los consentimientos tácitos. También es posible, para el ciudadano o consumidor, solicitar que los datos sean transferidos de un proveedor de servicios de internet a otro. Así como presentar denuncias a través de asociaciones de usuarios y solicitar indemnizaciones de daños y perjuicios derivados de tratamiento ilícito de datos personales.

5. Reglamento 44/EC del Consejo del 2001, este es sobre la competencia, el reconocimiento y la ejecución de sentencias en materia civil y mercantil, fue sustituido por el Reglamento de Bruselas número 1215 del 2012 que entró a regir a partir del 10 de enero del 2015. Este nuevo reglamento se aplica, únicamente, a las acciones judiciales ejercitadas, a los instrumentos auténticos formalizados o registrados, o a las transacciones judiciales aprobadas o celebradas a partir del 10 de enero de 2015. El Reglamento 44/2001 se sigue con su aplicación a las sentencias dictadas en acciones judiciales ejercitadas, a los instrumentos auténticos formalizados o registrados y a las transacciones judiciales aprobadas o celebradas antes del 10 de enero de 2015.

Lo anterior se da debido a que en el crecimiento del comercio electrónico ha generado conflictos entre ordenamientos jurídicos y preguntas de derecho internacional privado, por ejemplo, cuál es la jurisdicción competente, la responsabilidad contractual que rige el contrato celebrado, la extracontractual, el reconocimiento y ejecución de sentencias extranjeras. En tal marco, existe una ausencia de normas legales y convenios

internacionales que traten, específicamente, sobre estos temas, por lo que deben ser abordados con las normas pertinentes de cada jurisdicción; para estos efectos se expidió el reglamento señalado, donde las transacciones celebradas antes del 2015 serán regidas por este con sus reglas generales de jurisdicción relevantes para estas transacciones electrónicas entre un comerciante y un consumidor, ahora, los negocios jurídicos celebrados después del 2015 regirán por el Reglamento de Bruselas I.

6. La directiva 31/CE del Parlamento Europeo y del Consejo, 8 de junio del 2000, en esta se fijaron aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interno.

Esta directiva ayudó a garantizar la libre circulación de los servicios de la sociedad de la información entre los Estados miembros, y regula temáticas relacionadas con los servicios de la sociedad de la información relativos con el mercado interior, el establecimiento de los prestadores de servicios, las comunicaciones comerciales, la responsabilidad de los intermediarios, los contratos vía electrónica, los acuerdos extrajudiciales para la solución de controversias, entre otros.

7. La directiva 29/CE del Parlamento Europeo y del Consejo, 22 de mayo del 2001, esta es sobre la armonización de algunos aspectos del derecho de autor y derechos conexos en la sociedad de la información. Mediante esta directiva se logró que cada Estado estableciera una protección jurídica adecuada contra la elusión de cualquier medida tecnológica cometida por una persona con la intención de causar daño, y también se instituyó una protección jurídica frente a la fabricación, la importación, la distribución, la venta, el alquiler, la publicidad para la venta o el alquiler, o la posesión con fines comerciales de cualquier

dispositivo y producto, esto con una protección a la prestación de servicios dados por intermedio de una promoción, de una publicidad.

8. La directiva 22/CE del Parlamento Europeo, 7 de marzo del 2002, esta alude al servicio universal y a los derechos de los usuarios en las redes y los servicios de comunicaciones electrónicas. Con esta directiva se aseguró la existencia de servicios de comunicaciones electrónicas disponibles para el público.
9. La Resolución del Consejo del 18 de febrero del 2003, esta refiere un enfoque europeo orientado a una cultura de seguridad de las redes y de la información. Igualmente, trata temáticas conexas con la seguridad y su importancia para el buen manejo del Gobierno y el sector privado.
10. La Decisión 752/CE de la Comisión, 24 de octubre de 2005, esta es acerca de la conformación de un grupo de expertos en materia de comercio electrónico. Dicha decisión permitió que la Comisión pudiera contratar a un grupo de individuos expertos para consultar cuestiones del comercio electrónico.
11. La Resolución C 68/01 del Consejo, 22 de marzo de 2007, esta apuntó a una estrategia para una sociedad de la información segura en Europa. Esta resolución mejoró la seguridad de los programas y la capacidad de adaptación de las redes sistemas de información de los Estados miembros.

Similarmente, la *New Deal for Consumers*, una iniciativa adoptada por la Comisión Europea en abril del 2018. Esta busca una mayor transparencia en los mercados digitales europeos, iguales derechos para los consumidores de servicios digitales “gratuitos”, una mejor clasificación de ofertas, transparencia sobre las opiniones de los

consumidores y la prohibición de revender entradas para eventos comprados a través de *bots.*

2.2.4 Convención de Roma en la ley aplicable a las obligaciones contractuales

Con este convenio se establecieron unas normas referentes con la ley aplicable a las obligaciones contractuales en la UE, este se aplica en situaciones que impliquen conflictos entre leyes nacionales de los Estados miembro, inclusive, en casos donde la ley pactada y designada entre las partes es la de un ordenamiento jurídico no contratante; no obstante, esto tiene unas excepciones que son los temas vinculados con lo siguiente.

- Estado civil o la capacidad física de las personas.
- Obligaciones contractuales adquiridas en testamentos, celebraciones de matrimonio, en general, todas las familiares.
- Obligaciones derivadas de instrumentos negociables, es decir, títulos valores.
- Convenios de arbitraje y de elección de foro.
- Regulaciones de derecho de sociedades, asociaciones y personas jurídicas.
- Si está permitido en el ordenamiento juicio que un tercer obligue por un sujeto.
- Si un órgano de una sociedad, de una asociación o una persona jurídica puede obligarse frente a terceros a esta.
- La Constitución y cuestiones de la organización.
- La regulación de los contratos de seguros que cubran riesgos en los territorios de los países de la UE (se excluyen los contratos de reaseguros).

Las partes de un contrato podrán pactar una ley que le aplique a la totalidad o a una parte de este, también pueden pactar el tribunal competente en caso de litigio y

podrán modificar, de común acuerdo, la ley aplicable siempre que consideren sustentarse en el principio de libertad de elección. Es necesario revisar los casos donde las partes no pacten una ley, pues el contrato se regirá por la normatividad del país que tenga más relación con el negocio jurídico, por ejemplo, el lugar donde se encuentra el establecimiento principal del proveedor. Empero, cuando en el contrato se haga referencia a un bien inmueble, la ley aplicable será la del país donde se encuentre este, y cuando indique un transporte de mercancía, la ley aplicable será determinada por el lugar de carga o descarga de esta o el establecimiento principal del proveedor.

Cabe añadir que existen muchas reglas que dependen del supuesto de hecho del caso, este deberá ser estudiado para poder determinar su regulación aplicable en caso de no ser pactada por las partes. Asimismo, en cuanto al suministro de bienes muebles corporales o a la prestación de servicios, se busca proteger a los consumidores con el beneficio del principio de protección de la parte más vulnerable y se regirán por la ley del lugar de residencia del consumidor, a menos de que las partes pacten lo contrario en el contrato, esto en valoración de que la ley aplicable acordada no puede ser perjudicial para el consumidor u ofrecerle menos protección a la de su país de residencia; se debe resaltar que estas normas no se pueden aplicar a contratos de transporte ni a los de suministro de servicios en un país distinto del de residencia del consumidor. Acerca de los contratos de trabajo la aplicación de la normatividad es la siguiente.

- La ley del país donde el trabajador realiza, habitualmente, el trabajo.
- La ley del país donde se encuentra el empleador.
- La ley del país con el que el contrato de trabajo tenga más relación.

Si las partes deciden elegir otra ley aplicable al contrato, esta elección no podrá hacerse en función de la protección del trabajador. Así, el impacto de esta convención fue la posibilidad solucionar temáticas de conflictos entre leyes nacionales, esto es muy positivo y esclarece problemáticas, en virtud de que el Artículo 3 planteó que las partes son libres de elegir la ley aplicable. Vale la pena recordar que, en ausencia de una elección, el Artículo 4 conducirá a la determinación por el tribunal y a la aplicación de la ley más vinculante con el contrato (Rizzi, C. (s.f.).)

2.2.5 Comité de Asuntos Fiscales de la OCDE

El Comité de Asuntos Fiscales de la OCDE ha desarrollado un plan de trabajo detallado con el objetivo de hacer prosperar el comercio electrónico, por lo tanto, se produjeron unas condiciones marco tributarias que fueron introducidas por los ministros en la conferencia “un mundo sin fronteras: cómo aprovechar el comercio electrónico” en 1998. Este plan tiene como base unos principios que deberían ser aplicados en el comercio internacional, estos son los siguientes.

- Neutralidad
- Eficiencia
- Certeza y simplicidad
- Eficacia y equidad
- Flexibilidad

En el 2016 se le otorgó la aprobación a este Comité de Asuntos Fiscales de la OCDE en Colombia, donde este evaluó la política fiscal colombiana y el resultado fue que se encontraba al nivel de los 34 países miembros de la OCDE. Este comité se

encarga de establecer estándares internacionales en materia de impuestos, y de implementar los Planes de Acción Erosión de la Base y Traslado Artificial de Utilidades (BEPS), tiene las siguientes finalidades: atacar a los evasores y dar respuesta a los abusos de planeaciones fiscales agresivas mediante el intercambio de información entre Estados, corregir vacíos normativos en los distintos sistemas tributarios, impedir el traslado de utilidades a jurisdicciones de poca o nula tributación, donde la actividad económica desarrollada es nula. Las recomendaciones dadas por este comité a Colombia se han seguido en las reformas tributarias; esto se realiza con la finalidad de propiciar el crecimiento económico e incentivar la inversión extranjera (Moreno, 2019).

En las recomendaciones, a nivel subnacional, debe prevalecer la reasignación de responsabilidades y el financiamiento, esto para que se haga más fácil la interacción entre los diferentes niveles de la administración, esto no solo se logra con la coordinación entre los distintos niveles del Gobierno en temáticas subnacionales, sino que los planteamientos del Comité de Asuntos Fiscales de la OCDE para Colombia toman en cuenta la necesidad de buscar espacios de integración entre países. Lo anterior como base fundamental para la coordinación en materia tributaria entre los Estados, para incentivar la inversión, y que estas impliquen una mayor competitividad económica en donde haya una hacienda pública eficiente en el recaudo y responsable en el gasto (Moreno, 2019).

2.2.6 El comercio electrónico desde la óptica de la regulación de ciertos Estados

Contar con un negocio virtual que puede estar abierto las 24 horas del día ha generado cambios abruptos en la manera de llevar a cabo el comercio, es por ello que

es precisa la ejecución de una investigación y comparación del campo del derecho y las nuevas tecnologías, particularmente, en lo relacionado con el internet y las ventas a través de este. Lo anterior para una comparación de las modalidades en que distinto regímenes jurídicos, alrededor del mundo, manejan esta temática; se eligieron estas regulaciones jurídicas al valorar la relevancia de los avances dados.

En tal marco, se seleccionó a Brasil, este país representa la economía más grande de América Latina, pues, según datos de un estudio realizado en el año 2019 por Euromonitor International, Brasil posee el 42 % de todo el *eCommerce* B2C latinoamericano (Ecommerce News, 2020). De acuerdo con el último informe sobre el índice de comercio electrónico de empresa a consumidor 2020, elaborado por la UNCTAD, los consumidores de Brasil, México, Argentina, Chile y Colombia constituyen 92 % del total de compras electrónicas de toda la región latinoamericana.

Por otro lado, se eligió España, en concordancia con un informe del 2020, realizado por Google España, en las ventas por internet ha crecido un 70 % el número de consumidores. Se denotó que España se sitúa como el cuarto país europeo que efectúa más compras *online*, detrás de Reino Unido, Italia y Polonia, y el gasto medio anual de compras *online* casi se ha duplicado en menos de 10 años, alcanzó los 1 366 euros por comprador (Think With Google, 2020). El país ha implementado muchas de las directivas de la UE, un órgano de derecho comunitario reconocido por su avanzada regulación en el tema de comercio electrónico. Finalmente, se optó por Estados Unidos, este país es una de las grandes potencias mundiales y, conforme con un estudio llevado

a cabo, en el 2020, por Bussiness.com, es el segundo mercado más grande de comercio electrónico en el mundo después de China (Business.com , 2020), esto lo convierte en un ejemplo para otros países en lo referente con la innovación y los avances tecnológicos.

1. Brasil

La Ley 25.506 regula temáticas relacionadas con el valor jurídico y probatorio del documento digital, y las diferentes formas digitales, la Ley 25.326 aborda el *habeas data*, la protección de datos de carácter personal y la privacidad, y la Ley 26.338 transforma en delitos aquellas conductas en que la informática es utilizada como medio u objeto para su comisión, etc. En Brasil se sancionó, el 30 de noviembre de 2012, la Ley 12.737 que incorporó algunos delitos informáticos a su Código Penal, dicha norma planteó el delito de “invasión de un equipo informático ajeno”, la “interrupción o perturbación de un servicio de comunicaciones de utilidad pública” y la “falsificación de tarjetas de crédito” al existente delito de “falsificación de documentos”.

La normatividad brasilera, en virtud del principio de libertad de las formas, garantiza la validez de los contratos celebrados vía internet, puesto que el contrato por medios electrónicos logra satisfacer los requisitos y los presupuestos aplicables a los contratos tradicionales. Los contratos electrónicos de consumo están reglamentados por la normatividad del Código de Defensa del Consumidor. En este país se encuentran vigentes los principios de equivalencia funcional de los contratos electrónicos, así como los de neutralidad tecnológica, esto según la Ley Modelo de CNUDMICNUDMI. Respecto con el documento electrónico y la firma digital, Brasil ha emitido la “Medida provisoria 2.200-2”, del año 2001, basada en la Ley Modelo de CNUDMICNUDMI, en esta se

reconoció la validez legal de los certificados digitales formulados en terceros países, esto resulta de relevancia en materia del ecosistema del comercio electrónico transfronterizo.

El Marco Civil de Internet de Brasil, con la Ley 12.965, fue finalmente aprobado por el 23 de abril de 2014. Esta norma regló el uso de internet, la responsabilidad de los distintos actores, la protección de datos personales y los derechos civiles de los brasileños; en esta se instauraron los principios por los que se rige el uso de internet en el país, tales como la garantía de la libertad de expresión, la comunicación y la manifestación del pensamiento, la protección de la privacidad, la protección de datos personales, la preservación de la garantía de neutralidad de la red, y la preservación de la estabilidad, seguridad y funcionalidad de la red. Este Marco Civil brindó derechos y garantías a los usuarios de internet, protege su intimidad, asegura el derecho a su protección, y a la indemnización por el daño material o moral resultante de su violación; protege la privacidad de los usuarios y regula la responsabilidad de los proveedores de servicios de internet y de los proveedores de aplicación (Lisandro, 2019).

2. España

El ordenamiento jurídico español incorporó, en su sistema, la Directiva 2000/31/ce del Parlamento Europeo y del Consejo, relativa esta con determinados aspectos de los servicios de la sociedad de la información, y al comercio electrónico en el mercado interior. Por otra parte, incluyó, parcialmente, la Directiva 98/27/ce del Parlamento Europeo y del Consejo, esta alude a las acciones de cesación en materia de protección de los intereses de los consumidores. Igualmente, el Decreto 1163/2005, del 30 de septiembre, por el que se reglamentó el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, y los requisitos y el

procedimiento de concesión. Equivalentemente, la Orden EHA/962/2007, emitida, el 10 de abril, por el Ministerio de Economía y Hacienda, del 10 de abril, desarrolló disposiciones sobre facturación telemática y la conservación electrónica de facturas. Esta reguló cómo deben de ser remitidas las facturas y la remisión por medios electrónicos.

También con la Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información, divulgada el 28 de diciembre, se fijaron unas medidas de impulso para el uso de la factura electrónica y de los medios electrónicos, por ejemplo, volver la facturación electrónica en el marco de la contratación con el sector público. En tal marco, el Real Decreto 1671/2009 del 6 de noviembre, con este se desarrolló la Ley 11/2007, del 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Reguló temas acerca de la transmisión de datos, sedes electrónicas y punto de acceso general, identificación, registros electrónicos, comunicaciones, notificaciones, documentos electrónicos y copias.

3. Estados Unidos

En Estados Unidos, a los negocios por intermedio de internet se les demanda la obtención de una licencia de operación o un registro frente a las autoridades gubernamentales, las plataformas *online* deben asegurar que, en sus términos y condiciones, sean vinculantes, contractualmente, en su sitio web con sus clientes y los individuos que lo visitan. Esto se logra con la inclusión de mecanismos para que las partes contratantes puedan manifestar su consentimiento, por ejemplo, la norma Federal de Garantía Magnusson-Moss (MMWA) aplicable a todas las personas que provean una garantía escrita o implícita en relación con un producto de consumo; se le solicita a esta persona que divulgue la garantía en un lenguaje simple y fácil de entender, este acto

también prohíbe a los proveedores modificar las garantías implícitas a un consumidor en algunas circunstancia.

Las leyes federales y estatales en privacidad de datos obligan, a los negocio de comercio electrónico, a publicar políticas de privacidad claras y especificas antes de recolectar cualquier tipo de información, implementar las salvaguardias apropiadas para la protección de dicha información y disponer de los datos de una manera segura. Las problemáticas conexas con el contenido generado por los usuarios, el uso de marcas comerciales de terceros y el uso o reproducción de material publicitario son resueltas por las normas de propiedad intelectual.

La regulación de la Comisión Federal de Comercio (FTCA) prohíbe a los negocios de comercio electrónico implementar medidas de ciberseguridad insuficientes que, injustamente, puedan dañar a los consumidores en casi todos los estados de Estados Unidos, y sus jurisdicciones tienen adscritos estándares de seguridad responsable para los problemas de ciberseguridad. El estándar de seguridad razonable es relativo, en lugar de ser definitivo, emplea las acciones de ejecución pasadas como guía; el Instituto Nacional de Estándares y Tecnología público, en abril del 2018, un marco para mejorar la ciberseguridad y este fue ampliamente aceptado para establecer el estándar de seguridad razonable (ICLG, 2020).

Asimismo, la norma de Transacciones de Información por Computadora (UCITA) busca brindar uniformidad y certeza a las leyes que se aplican en las transacciones de las TIC, tal como lo hace el Código de Comercio Uniforme para la venta de bienes. Este acto creó un conjunto de reglas para regular temas de comercio electrónico tales como la concesión de licencias de software, el acceso *online* y otras transacciones de las TIC,

eso debido a que su potencial para debilitar las protecciones del consumidor no es una ley federal y solo ha sido adoptado en los estados de Virginia y Maryland.

La ley de este país ha evolucionado para enfrentar los desafíos del uso de las tecnologías para la realización de negocios, por ejemplo, la Ley de Firmas Electrónicas en el Comercio Nacional y Global, promulgada por el presidente Bill Clinton en el 2000, implementó un estándar nacional uniforme para todas las transacciones electrónicas, y fomentó el uso de las firmas electrónicas en los contratos y registros electrónicos. La Ley E-SIGN se encargó de reglamentar las transacciones de comercio interestatal y extranjero, no alteró la ley existente y definió la “firma electrónica” como un sonido, símbolo o proceso electrónico adjunto asociado, lógicamente, a un contrato u otro registro electrónico ejecutado por una persona, esto con la intención de firmar el registro.

Por esta regulación tan amplia es posible que los acuerdos de teclado electrónico, en donde se indica que se presione un numero para estar de acuerdo, cumplan, legalmente, como contratos electrónicos bajo la ley; por otro lado, a un contrato no se le puede negar su validez solo por el hecho de emplear una firma digital para certificarlo, pues esta ley también instauró requisitos de consentimiento del consumidor, de validez para las firmas, los registros y los contratos electrónicos, las reglas de notarización, con la finalidad de brindar protección a los consumidores. Con respecto al *marketing*, el Congreso de Estados Unidos promulgó la ley CAN-SPAM del 2003 (control del asalto a la pornografía y el *marketing* no solicitados), esta ley otorgó autoridad a la FTC para regular asuntos relacionados con el uso corporativo del correo electrónico para fines de *marketing*, esta fijó multas y sanciones penales (JUSTIA, s.f.).

En tal óptica, la ley Millennium Copyright Act determinó sanciones civiles y penales a los actos de piratería y los usos no autorizados de softwares, esto para dar protección a la propiedad intelectual y promover la posibilidad de entablar acciones civiles para conseguir indemnizaciones monetarias. También existen ciertos requisitos legales que se deben llevar a cabo al momento de crear un sitio web, se debe asegurar los derechos para usar el nombre de dominio que se elija, esto requiere registrar el nombre con un administrador de dominio acreditado por la *Internet Corporation For Assigned Names An Numbers* (ICANN) (Sttimel, Sttimel & Roeser, s.f.).

En conclusión, se encontró que en sede de legislación doméstica la UE y Estados Unidos están mucho más avanzados en sus regulaciones frente al comercio electrónico. América Latina, aun cuando tenga acuerdos internacionales y leyes propias sobre comercio electrónico, no ha avanzado en estos asuntos. También se puede afirmar que la regulación relacionada con la firma digital ha sido desarrollada satisfactoriamente en todos los estados; Se debe tener en cuenta que el tema del comercio electrónico requiere de una actualización constante de su marco regulatorios a nivel internacional, esto para suscitar la necesidad del fortalecimiento y la cooperación entre ordenamientos jurídicos, y lograr una regulación económica global que no sea obstaculizada, no tenga contradicciones y propicie el crecimiento. Cabe añadir que hace falta una regulación internacional que exija su aplicación coercitiva entre los Estados que tengan vacíos en sus leyes, esto ha llevado a que se presenten riesgos jurídicos para los usuarios y consumidores del comercio electrónico.

Capítulo 3. Los riesgos en el comercio electrónico y cómo mitigarlos

En el presente capítulo se abordan algunos de los riesgos que se pueden presentar en el comercio electrónico y se brindan alternativas de cómo mitigarlos. El enfoque se encuentra en riesgos relacionados con la propiedad intelectual, la propiedad industrial, y con el fraude electrónico y los documentos electrónicos, esto es preciso, pues no hay un desarrollo jurídico firme frente a ellos; los riesgos son los siguientes.

1. Riesgos relacionados con los nombres de dominio.
2. Riesgos conexos con la falsificación y la infracción de marcas.
3. Riesgos vinculados con el fraude electrónico y la usurpación de identidad en los documentos electrónicos.

3.1 Riesgos relacionados con los nombres de dominio

3.1.1 ¿Qué es un nombre de dominio?

Un nombre de dominio es la dirección de la página web que se escribe en el navegador, en el URL, para poder dicha página. El internet es una red de computadores conectados y comunicados entre sí a través de una red global de cables, y a cada uno se le asigna una dirección de IP (*internet protocol*), estos son números que lo identifican dentro de la red. De esta manera, los nombres de dominio fueron diseñados para no colocar los números del IP, en vista de que estos son extensos y difíciles de recordar, así, para ingresar a la página web se coloca el nombre de dominio en la barra de navegador en lugar del IP.

Lo anterior se realizó en 1988, inicialmente, por *Internet Assigned Numbers Authority* (IANA) y luego por la ICANN, se subcontrató la asignación de los nombres de dominio para países individuales. Así, el nombre de dominio corresponde solo a una página web, y es el medio por el que los consumidores de las compañías pueden encontrar dicha página. En valoración con lo anterior, existen 2 puntos importantes que aclarar sobre los nombres de dominio.

- No son necesarios, son convenientes para el libre desarrollo de la WWW, lo preciso es el IP y los números que lo identifican.
- No es ineludible que los nombres de dominio sean asignados por cuerpos particulares, es posible prever para competirlos. El sistema de dominio (DNS) funciona al permitir de que la ICANN y los órganos subsidiarios tengan acceso a los servidores raíz que mantienen bases de datos de direcciones; esta información es, en principio, susceptible de copia y de registros alternativos.

Por consiguiente, los nombres de dominio son empleados como identificadores comerciales, y su registro es ejecutado por administradores y registradores a nivel local o internacional. Ahora bien, cabe indicar que en Colombia el dominio es ".co", y es administrado por el Ministerio de Tecnologías de la Información y la Comunicaciones (MinTIC) con base en la licitación pública No. 002 de 2009, mientras que, a nivel internacional, el dominio ".com" es realizado por la ICANN (Superintendencia de Industria y Comercio, 2005).

Independientemente de que sea como empresa o persona natural, obtener una URL en internet es un asunto sin mayor asesoría especial. En el mercado existen múltiples registradoras como Godaddy.com en la red, o entidades como Publicar S.A.,

esta se encarga de su mantenimiento. Entonces, esta facilidad de registro en la red, que puede conseguirse desde US $ 10, se ha convertido en una problemática que genera muchos riesgos como los expuestos a continuación.

3.1.2. Tipos de riesgos relacionados con los nombres de los dominios

Secuestro de nombres de dominio (*domain name hijacking*): este se presenta cuando terceros redirigen a los visitantes de un sitio web de una empresa hacia sitios web falsos, esta acción se realiza, normalmente, con el fin de robar credenciales de acceso e información confidencial, lo que implica ataques de suplantación de identidad contra los clientes, consumidores o empleados. Se suelen usar los propios dominios de la empresa para que el ataque parezca legítimo, estas actuaciones constituyen un gran riesgo para la información de la empresa y de los usuarios, y pueden darse infracciones a la privacidad, especialmente, relativas con el RGPD. Para este caso, uno de los vendedores de nombres de dominio más grandes, Go Daddy, brindó algunas recomendaciones que se dan para mitigar el riesgo, estas son las siguientes.

1. Adquirir buenas prácticas de dominios seguros, DNS y certificados digitales como medidas generales de ciberseguridad.
2. Utilizar estrategias de defensa para proteger sus dominios, DNS y certificados digitales que el sujeto tenga en su propiedad, esto se puede efectuar con la selección de un proveedor empresarial para proteger los sistemas de gestión de dominios, controlar los permisos para todos los usuarios y aprovechar las características avanzadas de seguridad de dominios.

3. Identificar y utilizar las medidas de seguridad que sean adecuadas en sus principales nombres de dominio, el bloqueo de registro, extensiones de seguridad DNS, y autenticación de mensajes e informes basados en el dominio.
4. Consolidar su dominio con DNS y proveedores de certificados digitales con un proveedor de tipo empresarial.

Secuestro inverso de nombres de dominio(***reverse domain name hijacking***): es lo que hace el propietario de una empresa que busca volverse propietario de un dominio realizando falsas demandas de ciberocupación contra el legítimo dueño del dominio, intimidando a los propietarios del nombre de dominio para que estos transfieran la propiedad de sus nombres de dominio a los propietarios de marcas registradas para evitar que se levanten acciones legales en contra de ellos, esto sucede en su mayoría cuando esos nombres de dominio pertenecen a empresas pequeñas y la demanda se realiza por empresas más grandes; El secuestro inverso de nombres de dominio es un recurso legal utilizado para contrarrestar la práctica de la ocupación ilegal de dominios en la cual personas poseen muchos nombres de dominio registrados en los cuales se contienen marcas comerciales famosas de terceros con la intensión de lucrarse vendiéndolos a los propietarios de las marcas comerciales; Las demandas por ciberocupación son una estrategia defensiva para combatir la ciberocupación, sin embargo, tales demandas también pueden usarse como forma de forzar a los registrantes de nombres de dominio para que renuncien a nombres de dominio a los que el propietario de la marca comercial no tiene derecho (Todd,2005,p. 28).

Ciberocupación: “es el acto mediante el cual se registra un nombre de dominio con la mala fe para aprovecharse del potencial y prestigio que tenga una marca que pertenezca a otra persona o empresa” (Rodríguez, 2019, p. 5); existen los siguientes dos tipos.

A. ***Typosquatting:*** “en este tipo de ciberocupación, lo que se hace es que se registran dominios variando algún carácter de posición. Por ejemplo, registrar un dominio llamado goooogle.com, es muy parecido a Google.com pero le agregan una o” (Rodríguez, 2019, p. 6).
B. ***Bitsquatting****:* “es una técnica compleja por la cual los delincuentes logran redirigir a los usuarios a una página diferente a la que realmente quieren acceder” (Rodríguez, 2019, p. 7).

Se debe tener en cuenta que no es posible garantizar, totalmente, que no se sufrirá este tipo de ataque, no obstante, se puede reducir el porcentaje de materialización del riesgo si se siguen las siguientes sugerencias dadas por el vendedor de dominios Go Daddy.

- Asegurarse de escribir la URL correctamente antes de ingresar, si se comete un error se puede materializar algún riesgo que afecte el dispositivo con el que se ingresó.
- No abrir emails sospechosos y no entrar a las URL de estos.
- Se deben eliminar los focos vulnerables del dispositivo, sean aplicaciones instaladas, actualizaciones, entre otros.

- Se debe procurar instalar un software de seguridad en internet, y para que sea duradero debe actualizarse.

Frente a estos riesgos asociados a los nombres de dominio se pueden tomar 2 caminos para resolverlos, estos se proyectan a continuación.

Acudir a un arbitraje internacional regulado por la ICAAN: la ICAAN es un organismo que regula, a nivel mundial, el registro de dominios. La ICANN y la OMPI publicaron una Política Uniforme de Resolución de Disputas (UDRP) sobre nombres de dominio, en esta se estipularon los pasos que debe dar cualquier usuario de internet que cree o tenga pruebas sobre el uso ilegal de un nombre de dominio.

Acudir a la vía judicial: si se presentan algunos de los casos mencionados, se puede acudir a la vía judicial, esto también cuando, en la materialización de dichos riesgos, hayan ocurrido daños, perjuicios o delitos. A continuación, se explicarán los caminos que se pueden seguir.

A. Acudir a las políticas de arbitramento de la ICAAN

¿Qué es la ICAAN?

Esta es una entidad sin ánimo de lucro creada, en 1998, en Estados Unidos, con la finalidad de asumir la responsabilidad de administrar el sistema de nombres de dominio en internet y proporcionar mecanismos rápidos y económicos para resolver disputas que puedan surgir con respecto a estos. En 1999, la ICAAN aprobó la UDRP, a través de esta política los titulares de marca o de nombres de dominio pueden impugnarle registro o uso ilegítimo a un nombre de dominio, y solicitar que el dominio, objeto de infracciones, sea cancelado o transferido al titular de marca, para que esto se logre se deben demostrar las siguientes condiciones.

1. Que el nombre de dominio sea parecido o idéntico al de la empresa o marca del demandante.
2. El que demanda debe demostrar que no hay interés o derecho legítimo sobre el dominio.
3. Se debe expresar que se registró ese nombre de dominio con mala fe (la mala fe se debe exteriorizar en los casos de ciberocupación en los que se induce a un engaño a los consumidores, esto con la creación de la falsa creencia de que ese nombre de dominio está relacionado con una marca comercial cuando no es así).

Los procesos de transferencia de nombre de dominio tienen, normalmente, una duración de 60 días y son llevados a cabo por árbitros y no por jueces; el valor para acceder a la UDRP oscila entre los US $ 2 500 y los US $ 4 000, esto depende de si el demandante quiere que la decisión sea tomada por 1 solo árbitro o por un panel compuesto por 3 árbitros. Nominet es el encargado de los nombres de dominio del Reino Unido y muchas veces hace parte en las disputas de los nombres de dominio.

Tanto para ICANN como para Nominet se incorporó un procedimiento de resolución de disputas en el contrato, esto para vincular al propietario del nombre de dominio registrado. El procedimiento de ICANN es la UDRP, y el de Nominet es la Disputa Política de servicio de resolución (DRS). A diferencia de arbitraje comercial, no es obligatorio para el demandante acudir a la resolución de disputas, pues este es libre de asistir a los tribunales acción si así lo prefiere.

Los pros y contras de procedimientos de resolución de disputas.

- Los procedimientos de resolución de disputas son un método rápido, conveniente y económico de reasignar el nombre de dominio, generalmente están basados en la correspondencia y son independientes de la jurisdicción de las partes; pero hacer valer jurisdicción sobre un extranjero demandado puede ser complicado.
- Las normas de propiedad industrial varían entre jurisdicciones, mientras que los procedimientos de resolución de disputas no lo hacen.
- La reasignación es la única opción que se ofrece. Si el reclamante quiere, por ejemplo, exigir por daños económicos, deberá acudir a los tribunales.
- Nominet tiene el poder "para transferir, cancelar o suspender el dominio de registro de nombres", pero no se mencionan otros poderes, es decir, no tiene poder para regular reclamaciones por daños o perjuicios causados o por delitos cometidos; esto si lo posee la vía judicial.

B. Acudir a la vía judicial: la falta de normatividad

No existe una regulación clara sobre los derechos de propiedad alrededor de los nombres de los dominios en internet, especialmente, en Colombia, donde los casos suelen ser resueltos por un juez ordinario del circuito municipal, por ende, es preciso definir estrategias de protección de la compañía y de la marca, por ejemplo, con la implementación de un sistema de protección de marcas: *Trademark Clearinghouse* (Tmch) que, por un costo, le permite a las empresas inscritas tener prelación en la adquisición de los nuevos dominios y recibir notificaciones al registrarse un dominio con su marca. Existe una falta de una institución normativa encaminada a dar una protección a los nombres de dominio y los riesgos asociados a estos, mientras se logra dicha

evolución normativa, se debe hacer uso de los mecanismos en los que se podría enmarcar la protección jurídica a los nombres de dominio.

En un primer momento, se debe intentar encuadrarla con base en lo que se pactó en el contrato, esto si ese mecanismo no es efectivo, igualmente, se mirará el régimen de propiedad industrial y si se puede enmarcar una protección a los nombres de dominio con el sustento en dicho régimen. También se evaluará en el caso de que no se pueda cobijar en el régimen de propiedad industrial, pero si en el régimen de propiedad intelectual, o si se es posible aplicar las normas que regulan los signos distintivos y en qué caso se podrían emplear estas, y finalmente, se dará la opción de acudir a normas de derecho civil y penal cuando se generen daños o perjuicios.

3.1.3. Protección jurídica al nombre de dominio

En Colombia no existe una normatividad específica encaminada a regular los nombres de dominio, por lo tanto, a continuación, se exponen algunas opciones a las que se debe acudir cuando estas problemáticas se presenten.

- **Según lo estipulado en el contrato**

Lo primero a observar es si en el momento en que se registró el nombre de dominio se pactaron estipulaciones contractuales, en estas se dota al titular del nombre de dominio, de acciones jurídicas que protegen dicho nombre de ataques provenientes de otros nombres de dominio, derechos de propiedad industrial, derechos de autor, etc. Cabe añadir que los derechos conferidos al titular del nombre de dominio en el contrato de registro no son muchos, estos son conexos con el derecho de uso del nombre de dominio y el derecho de transferirlo y licenciarlo. En segundo lugar, en la generalidad de

los contratos existe una adhesión completa para la resolución de disputas en torno a los nombres de dominio, esta es la UDRP; en concreto, se prevé que dicha política se incorpora al contrato.

- **Según el régimen de propiedad industrial**

Los nombres de dominio pueden ser utilizados como identificadores comerciales en el mercado virtual de bienes y servicios, desarrollan funciones similares o iguales a la de los signos distintivos tales como las marcas o los nombres comerciales. En estos casos se puede obtener un derecho de exclusividad sobre ese nombre de dominio, esto mediante la acción de registro de una marca, con la Superintendencia de Industria y Comercio (SIC), o con la constitución de una sociedad y la inclusión de ese nombre de dominio como parte de su razón social.

Cuando un nombre de dominio se usa para distinguir servicios y productos de una persona o empresa de los de otra, lo que no es extraño si se emplea en relación con servicios que se ofrecen a través de la red, debe afirmarse en línea de principio la posibilidad de obtener una marca sobre el mismo, siempre que se cumplan los requisitos legalmente establecidos. (Carbajo, 2002, p. 323)

Este mecanismo ha sido empleado en Estados Unidos para conferir tal facultad al titular del nombre de dominio, que este cumpla con las condicione por la entidad encargada y “determinando en cada caso las clases oficiales de productos o servicios donde pueden incardinarse los distintos servicios o informaciones técnicas prestadas en Internet para poder ser registrados los nombres de dominio identificativos de los mismos como marcas” (Carbajo, 2002, p. 324). Estas acciones son un mecanismo de protección jurídica para una mayor seguridad jurídica, viabilizan que la actividad comercial,

desarrollada por intermedio de una tienda virtual, no sea objeto de registro como marca, como nombre de dominio similar, u objeto de cualquier otra actividad que podría llegar a generar confusión; si esto sucede, se contará con herramientas jurídicas aptas para defenderse.

- **Utilizar las protecciones que se le dan a los signos distintivos y aplicarlas al nombre de dominio**

Es viable aplicar, al nombre de dominio, la protección de los signos distintivos tales como las marcas o el nombre comercial, pero sin la necesidad de registrar el nombre de dominio como una marca o u nombre comercial, sino por las funciones que este desempeña, estas pueden llegar a ser similares a las de las marcas comerciales. En tal marco, la protección a los nombres de dominio podría darse a partir de la normativa aplicable a los signos distintivos en virtud del uso dado a dicho nombre. Algunas de las normas jurídicas que protegen los signos distintivos son las siguientes.

- **Decisión 486 de la CAN**

Esta posibilidad de protección puede ser problemática, puesto que en Colombia el derecho exclusivo y excluyente sobre las marcas se consigue a través del registro. El uso de las marcas no es, por regla general, un hecho constitutivo de derechos.

- **Consideraciones sobre la protección de los nombres de dominio en Colombia según el régimen de propiedad industrial**

A continuación, se efectúa una explicación acerca del régimen de propiedad industrial para efectos de la protección de los nombres de dominio en Colombia. La autoridad encargada de realizar el registro de marcas es la SIC, esta ha emitido conceptos que podrían ser de gran ayuda para poder entender la protección de los

nombres de dominio desde una óptica de la propiedad industrial aplicable para el caso de Colombia.

- Concepto 03087905 del 17 de diciembre del 2003: en este concepto la SIC diferenció los nombres de dominio de los signos distintivos. Frente a los primeros mencionó que son simples identificadores (tienen la facultad de envolver, o no, una actividad comercial), estos son entendidos como direcciones de la red global de internet expresadas en letras para la facilidad del usuario. En cuanto a la marca, con base en el Artículo 134 de la Decisión 486 de la CAN, afirmó que esta se constituye como el signo apto para distinguir productos o servicios en el mercado, en otros términos, ambos conceptos contienen ideas distintas; la marca es el signo para la protección de un producto o servicio, mientras que el nombre de dominio es un digno identificador de una dirección en la red global del internet.

  De acuerdo con esto, se puede concluir que para la SIC los nombres de dominio no constituyen marcas comerciales y no es un signo distintivo en sí, pero puede llegar a constituir la manifestación del uso de una marca. Otra conceptualización que ratificó esto es el concepto No. 2264 del 2004, este establece una distinción entre la marca comercial y el nombre de dominio, y que no es posible atribuirle un derecho de marca comercial a un nombre de dominio.
- Concepto 03004020 del 29 de agosto del 2003: en este concepto se concluyó que existe la posibilidad de que el nombre de dominio pueda constituir un uso marcario, pero se debe considerar cada situación independiente y analizar la

> naturaleza del bien o servicio identificado con el signo y el uso dado al respectivo nombre de dominio. La SIC planteó que la utilización de un nombre de dominio podría componer un uso marcario, en la medida en que reúna los requisitos fijados en el Artículo 166 de la Decisión 486 de la CAN; es importante mencionar que dicho uso solo estaría protegido bajo la óptica de la jurisdicción colombiana y dentro de la clase en la que fue concedido el correspondiente registro de marca, a menos que el nombre de dominio constituya la manifestación del uso de una marca notoriamente conocida.

Es claro que no hay una protección diseñada, específicamente, para el nombre de dominio, y la SIC no desea brindarle a esta igual protección que a una marca, por lo tanto, es recomendable lo siguiente.

La constitución e inscripción del correspondiente tipo societario ante la autoridad competente, a efectos de demostrar derechos legítimos sobre el nombre de dominio similar o idéntico a la denominación o razón sociales de este. Asimismo, se opta por el registro del establecimiento de comercio cuyo nombre comercial conforma el SLD del nombre de dominio, con idénticas finalidades a las anteriormente descritas; también y con mayor frecuencia que en los eventos anteriores, se procede al registro del correspondiente signo como marca, en este caso el conjunto de palabras o números, conforme con lo estipulado en la Decisión 486, que constituye el SLD del nombre de dominio que se registra, el cual a su vez distingue un producto o un servicio.

Se encuentra que la única posibilidad concreta, aunque remota de obtener protección propiamente dicha para el nombre de dominio en Colombia por medio del régimen de propiedad industrial, es a la luz de lo dispuesto en el artículo 166 de la

Decisión 486 de 2000 de la CAN, o sea, considerarlo un uso marcario, alternativa que se plantea incierta, puesto que la SIC ha dicho que la misma está sujeta al análisis de las situaciones concretas y no ha establecido aún las directrices específicas. (Parra, 2010, p. 310 - 311)

- **Según el régimen de competencia desleal**

Esto se da en los casos en que el nombre de dominio no está protegido como marca, desde tal óptica, es viable valorarlo como se proyecta a continuación.

Como prestación empresarial autónoma, que merece protección frente a actos ilícitos de mercado. Aunque también se le podría proteger como simple prestación empresarial autónoma en el mercado, dado su más que evidente valor estratégico para globalizar el valor o la imagen de una empresa en el nuevo mercado electrónico, recurriendo en tales casos a la competencia desleal frente a actos de confusión, imitación o aprovechamiento de la reputación ajena llevados a cabo por terceros, dentro y fuera de la red, en perjuicio de la posición competitiva de su titular, en tanto el dominio pueda ser considerado como una importante prestación empresarial con vistas al mercado electrónico desarrollado en Internet. (Carbajo, 2002, p. 330)

3.1.4. Posibilidad de protección jurídica del nombre de dominio en Colombia por medio del régimen de competencia desleal

La ley 256 de 1996, en su Artículo 8, argumentó lo siguiente.

> Considera desleal toda conducta que tenga como objeto o como efecto desviar la clientela de la actividad, prestaciones mercantiles o establecimientos ajenos,

siempre que sea contraria a las sanas costumbres mercantiles o a los usos honestos en materia industrial o comercial.

En función de esto se puede afirmar que es posible la aplicación de la Ley 256 de 1996 (Ley de Competencia Desleal) a los casos de conductas relacionadas con los ataques a los nombres de dominio. En primer lugar, porque estas conductas de ataques se pueden llegar a desarrollar en el mercado al internet y determinarse como un mercado virtual; en segundo lugar, es evidente que, en materia de nombres de dominio, los actos tendientes a aprovecharse de uno de ellos llevan la intención de incrementar la participación en el mercado virtual de quien realiza tal acto, en vista de que conductas como el secuestro del nombre de dominio o el secuestro inverso de dominio, entre otras, persiguen, ilícitamente, un aprovechamiento del renombre logrado por el nombre de dominio que, en este caso, tiene funciones de identificador comercial. Esta ley se aplica a los comerciantes o a cualquier otro participante en el mercado, en efecto, bastaría con probar la participación del actor en el mercado virtual con la prestación u ofrecimiento de un determinado producto o servicio.

Ahora, en cuanto al aspecto territorial, establece que se aplicará a los actos de competencia desleal cuyos efectos principales tengan lugar o estén llamados a tenerlos en el mercado colombiano, previsión que puede ajustarse para proteger el nombre de dominio, como quiera que el titular del mismo y actor mediante esta ley podría demostrar probatoriamente que producto del ataque, el cual pretende prevenir o que ya se consolidó, se causará o se causó una serie de efectos nocivos para la prestación por él ofrecida en el mercado virtual, especialmente con efectos sobre la clientela lograda vía internet en Colombia, lo cual se podría ver reflejado en una disminución de ventas,

acompañada de un aumento de las mismas de quien realizó el acto de competencia desleal. (Parra, 2010, p. 313)

De conformidad con lo anterior, cabe aseverar que se puede hacer uso de la norma de competencia desleal para efectos de la protección a los nombres de dominio.

- **Normas de responsabilidad civil**

En los casos en que los ataques a los nombres de dominio produzcan daños o perjuicios, los individuos podrían acudir a la jurisdicción civil; en un principio, el titular del nombre de dominio puede demandar al proveedor de nombres de dominio por responsabilidad contractual en caso de incumplimiento del contrato, o de que, en el marco de cumplimiento de este, se generen daños conexos con dicho contrato (1602-1617). Análogamente, los consumidores de los bienes y los servicios pueden demandar al dueño del dominio por los daños causados con este nombre de dominio, esto con la acción de responsabilidad extracontractual (2341, Código Civil de Colombia).

- **Normas penales en Colombia que protegen a afectados por ataques a los nombres de dominio**

Existen ocasiones en que los ataques a los nombres de dominio pueden constituir conductas tipificadas como algunos, dichos casos son los siguientes.

- Suplantación de identidad: delito de falsedad personal, Artículo 296 de la Ley 599 del 2000.
- Hurto por medios informáticos y semejantes, Artículo 269I de la Ley 599 del 2000.
- Suplantación de sitios web para capturar datos personales, Artículo 269G de la Ley 599 del 2000.

En suma, se evidenció que no existe una normatividad encaminada a regular las problemáticas suscitadas cuando se presentan riegos asociados con los nombres de dominio, entonces, la opción es remitirse a normas que regulan otras instituciones por analogía normativa, como lo es la Decisión 486 de la CAN encargada de los temas de las marcas comerciales, esta norma se aplica cuando un nombre de dominio infringe una marca comercial. Similarmente, las normas de competencia desleal (Ley 256 de 1996), también existen instituciones del derecho civil y del derecho penal que pueden proteger a las víctimas de los riesgos que conllevan los nombres de dominio; otro problema es que no en todos los casos aplica esta remisión por analogía normativa y dichos casos desprotegidos generan vacíos legales.

3.2. Riesgos relacionados con la falsificación y la infracción de marcas en internet

3.2.1. ¿Qué es una marca comercial?

El Artículo 81 de la Decisión 344 de la Comisión del Acuerdo de Cartagena contiene una definición de marca: la marca constituye un bien inmaterial representado por un signo perceptible a través de medios sensoriales y susceptible de representación gráfica, es decir, un signo distintivo para identificar, en el mercado, los productos o servicios producidos o comercializados por una persona de otros idénticos o similares, a fin de que el consumidor o usuario los diferencie, esto sin riesgo de confusión o error acerca del origen o la calidad del producto o servicio de que se trate. La marca protege el interés de su titular, le otorga un derecho exclusivo sobre el signo distintivo de sus productos y servicios, así como el interés general de los consumidores a quienes sea

destinada, garantiza a estos la certeza de origen del producto o servicio que el signo distingue, les permite, en consecuencia, valorar, diferenciar, identificar y seleccionar el respectivo producto o servicio sin riesgo de error o confusión acerca de su origen o calidad. La marca procura asegurar la transparencia en el mercado. (Noticiero Oficial, s.f., párr. 1)

A diferencia de las patentes o los derechos de autor, las marcas comerciales no se vencen después de unos años, pues su derecho está ligado a su uso; en este sentido, una marca comercial podría funcionar para siempre y cuando se mantenga en uso en el comercio. Las marcas se registran en categorías de uso relevante en el registro; también es posible impugnar un registro en el motivo de falta de dicha utilización. El registro de la marca comercial no es obligatorio, pero es conveniente, en vista de que, gracias a esto, se le puede brindar una protección jurídica a la marca.

3.2.2. ¿Qué es la infracción de marca?

Según *United States Patent Trade Mark Office* (USPTO), la infracción de marca comercial es el uso no autorizado de una marca comercial, de servicio, o en conexión con bienes y / o servicios, esto puede causar confusión, engaño o error sobre la fuente de los bienes y / o servicios. Con el surgimiento del internet, muchas de las marcas se han visto afectadas, algunos de los ilícitos marcarios en internet se dan por intermedio de los proveedores de servicio de este, estos se constituyen por plataformas digitales de compraventa *online;* es frecuente la comercialización de productos falsificado e identificados con una marca propiedad de un tercero y sin la debida autorización de este.

Es importante resaltar que, en Colombia, para presentar una demanda por infracción de marca se debe proceder con lo siguiente.

En Colombia, la utilización de una marca, sin el consentimiento de su dueño, constituye una infracción de derechos de propiedad industrial, pues, de conformidad con la Decisión 486 de 2000 de la CAN, el uso de los signos distintivos radica, exclusivamente, en cabeza de su titular. El Artículo 155 de la decisión regula lo relacionado con el registro de marca, este esbozó que, al registrarla, se le brinda el derecho a su propietario de impedir que terceros la utilicen sin su consentimiento, esto logra que dicha marca no se pueda emplear sobre otros productos o servicios.

Terceras personas no pueden copiar la marca, sus slogans o símbolos distintivos, ni usar en el comercio los signos idénticos cuando esto cause confusión o un riesgo de asociación con el titular, tampoco pueden utilizar un signo idéntico o similar a una marca conocida si esto genera, al titular del registro, un daño económico o comercial, y a la marca dilución de la fuerza distintiva del valor comercial o publicitario. Esto fundamental, puesto que, con el registro de la marca, nace, en cabeza del titular, el derecho exclusivo de impedir a los terceros disponer de una marca semejante o igual, por lo tanto, es recomendable registrarla y, de ser posible, antes de empezar a usarla. Otro asunto esencial es recordar que el registro de la marca solo se limita al país en el que se ha otorgado, por consiguiente, las marcas registradas en el extranjero no se reconocen en el territorio colombiano, ni las marcas colombianas se comprenden registradas en el extranjero.

3.2.3. Panorama legislativo de la infracción marcaria en internet en Colombia

Normatividad aplicable en Colombia

Partiendo de la Constitución Política de Colombia en su Artículo 333, encontramos que el sistema económico colombiano defiende la libre empresa e iniciativa privada, reconoce que la libre competencia económica es un derecho de todos, para Molina, (2003), este derecho significa que los particulares puedan ejercer una actividad comercial o industrial sin discriminación, sin prohibiciones, obstáculos o trabas institucionales al momento de comercializar bienes y servicios. Por su parte el Artículo 61 de la Constitución Política de Colombia, preceptúa que el Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley; sin embargo, tratándose de derechos de propiedad industrial en asuntos de marcas, la Decisión 486 en su Artículo 137, menciona que han de negarse las solicitudes de registro marcario cuando se tengan indicios razonables que permitan inferir la comisión de actos de competencia desleal. (García, 2019, p. 15)

Es de recordar que en Colombia la propiedad industrial está regulada en el Libro Tercero, de los bienes mercantiles, Título II del Código de Comercio, (Leal, 2011), el cual ha sido objeto de múltiples modificaciones históricas normativas, actualmente se aplica lo establecido por la Decisión 486 de 2000 del Acuerdo de Cartagena, para el caso particular de las marcas, lo preceptuado en su Título VI, Artículos 134 al 189, además de la Ley 178 de 1994, por medio de la cual se aprueba el Convenio de París para la Protección de la Propiedad Industrial, publicada en el Diario Oficial No. 41.656 del 29 de diciembre de 1994. (García, 2019, p. 15)

En cuanto a la competencia desleal, las normas especiales vigentes en Colombia están contenidas en la Ley 256 de 1996, de la que destaca una cláusula general de competencia desleal en su Artículo 7 y un catálogo de doce prácticas consideradas desleales contenidas desde el Artículo 8 al Artículo 19.

A su vez, las normas correspondientes a la acción por infracción de derechos están contenidas en el Titulo XV de la Decisión 486 de 2000, descrita en su Artículo 238, como una acción de la que goza el titular en contra de cualquier persona que infrinja su derecho exclusivo o que dé lugar a una inminente infracción. (García, 2019, p. 16)

3.2.4. Acciones procedentes para la protección de las marcas de usos no autorizados en internet

Debido a la facilidad para publicar y hacer circular contenido en internet, se ha incrementado la posibilidad de que se cometan violaciones a los derechos de propiedad intelectual, entre ellos, una infracción marcaria, sea porque un sitio web empleó la marca sin autorización, la falsificó o se hizo pasar por ella. En concordancia con la Ley 1648 de 2013, la infracción marcaria puede dar lugar a que retiren los productos de los canales comerciales e, incluso, ordenar la destrucción de los productos usados en la infracción; en correspondencia con el Decreto 2264 del 2014, la infracción marcaria promueve indemnizaciones que van desde los 3 hasta los 200 salarios mínimos legales mensuales vigentes, esto a cargo del infractor. En este orden de ideas, se puede concluir que el titular de una marca registrada en Colombia, cuando sea víctima de una violación del derecho exclusivo que tiene sobre esa marca, puede iniciar acciones administrativas, judiciales ordinarias o penales.

3.2.5. Acciones administrativas de protección al consumidor

Una violación a los derechos marcarios en internet, en la que se vean afectados los derechos de los consumidores, puede dar lugar a que se presente una queja con el fin de que se inicie una investigación administrativa en los términos del Artículo 61 de la Ley 1480 de 2011 - Estatuto del Consumidor (Burgos, 2015). La Decisión 486, en su Artículo 486 de la Comisión de la CAN, argumentó que el derecho de exclusividad sobre el uso de una marca en Colombia se adquiere mediante el registro de esta ante la SIC, dicho registro, como todos los actos administrativos, goza de presunción de legalidad; pero el Artículo 146 de la Decisión 486 brinda un plazo de 30 días siguientes a la fecha de publicación, en estos se puede presentar una oposición para desvirtuar el registro de la marca (Andina, 2000).

3.2.6. Acciones judiciales

Los Artículos 238 y 241 de la Decisión 486 de 2000 indicaron que se puede presentar una acción por infracción de derechos marcarios, esto en contra del individuo que infrinja un derecho de propiedad industrial de un tercero o que, con sus actos, pueda llegar a infringirlo inminentemente, independiente esto del medio de comunicación empleado, en el que se dar el uso indiscriminado de una marca por internet. Así, el Artículo 24 del Código General del Proceso dio potestad a la SIC para ejercer funciones judiciales en los procesos de infracción de derechos de propiedad industrial, pero es el afectado quien elige ante quien quiere adelantar esa acción, lo puede efectuar frente a los jueces civiles del circuito o ante la SIC.

3.2.7. Acción por competencia desleal

Cuando una infracción marcaria conduzca a sus consumidores a caer en un error sobre la identidad de la empresa de la que proceden los productos y servicios, con la presencia de un riesgo en la capacidad decisoria de estos por la confusión generada, es viable que se haya incumplido la conducta señalada en el Artículo 10 de la Ley 256 de 1996, por la que se dictaron normas sobre la competencia desleal. Asimismo, cuando las marcas son idénticas, o muy similares, se presume el riesgo de confusión, por ende, esta ley indicó lo siguiente.

"Actos de confusión. En concordancia con lo establecido por el punto 1 del numeral 3 del Artículo 10 bis del Convenio de París, aprobado con la Ley 178 de 1994, se considera desleal toda conducta que tenga por objeto o como efecto crear confusión con la actividad, las prestaciones mercantiles o el establecimiento ajenos" (Ley N° 256, 1996).

3.2.8. Acción ordinaria para la indemnización de daños y perjuicios

Si el titular de la marca sufre alguna afectación debido a que una persona natural o jurídica utiliza su marca registrada por medio de internet, y esta actuación perjudica la marca registrada por el titular, este tiene la posibilidad de iniciar una acción ordinaria de responsabilidad civil extracontractual para poder reclamar la indemnización de daños y perjuicios. En primer lugar, se identificar el daño sufrido por la víctima, para luego proceder con un examen de causalidad, este conduciría a establecer la imputación material del daño al hecho generado y probar la afectación al derecho subjetivo.

3.2.9. Acción penal

La usurpación de derechos de propiedad industrial en Colombia constituye un delito tipificado en el Artículo 306 de la Ley 599 de 2000, Código Penal Colombiano, este proyectó lo siguiente.

> El que, fraudulentamente, utilice nombre comercial, enseña, marca, patente de invención, modelo de utilidad, diseño industrial, o usurpe derechos de obtentor de variedad vegetal, protegidos legalmente o similarmente confundibles con uno protegido legalmente, incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26 66) a mil quinientos (1 500) salarios mínimos legales mensuales vigentes. (García, 2019, p. 19)

3.2.10. Requisitos para presentar una demanda por la infracción de una marca

Existe un requisito extraprocesal que consiste en realizar una citación para adelantar una audiencia de conciliación extraprocesal. Sin embargo, cuando el demandante solicite el decreto y la práctica de medidas cautelares, no será necesario agotar dicho requisito de procedibilidad. Con la demanda, es necesario probar lo expuesto a continuación.

- Que el demandante es titular de una marca vigente registrada en Colombia en la SIC.
- Que el demandado ha usado, sin consentimiento de su titular, la marca para amparar productos o servicios idénticos o conexos, de tal forma que se genere

> riesgo de confusión en el mercado. Para lo anterior se requiere aportar pruebas tales como: i. El certificado de registro de la marca; ii. Facturas, fotografías, propuestas comerciales, material publicitario, correos electrónicos, páginas web, etc. (Cardenas Vega, Propiedad Intelectual, 2020, p. 13)

3.2.11. Nombres de dominio y marcas comerciales

En algunas ocasiones no es obvia la relación existente entre las marcas comerciales y los nombres de dominio, estos últimos son simples direcciones, pero algunos tribunales alrededor del mundo, por ejemplo, en el Reino Unido, e incluso, en la legislación colombiana, se ha visto que los nombres de dominio pueden llegar a ser capaces de infringir las marcas comerciales de una empresa. Los nombres de dominio son únicos, en otras palabras, se es más estricto con la elección de un nombre de dominio que con la del nombre de una marca comercial, en vista de que hay, aproximadamente, 45 clasificaciones reconocidas de bienes y servicios para una marca ser registrada, y no hay razón, al menos en principio, por la que empresas con nombres idénticos no deban competir en categorías diferentes; cuando el tema es de nombres de dominio, solo una podría usar dicho nombre, pues no interesa la categoría en ese caso.

Para que una infracción de nombre de dominio pueda ser interpretada como una infracción de marca, el nombre de dominio debe de ser idéntico a la marca, y usarse en el curso de comercio de bienes o servicios idénticos, esto es complicado de darse. A pesar de que tienen similitudes, estos son distintos, en otros términos, los nombres de dominio tienen una función localizadora propia de una dirección electrónica, estos

constituyen un elemento del sistema de direcciones de internet; mientras que las marcas son una palabra, frase o símbolo que identifica una marca comercial de las otras.

3.2.12. Problemáticas con la globalización

El alcance transfronterizo del comercio electrónico contrasta con el carácter territorial y nacional, de las marcas. La territorialidad e independencia de estos derechos y la protección dentro de un mismo signo puede variar entre los diferentes estados, con excepción de la UE la cual en virtud del Reglamento (UE) 2017/1001 sobre la marca de la UE (RMUE) brinda una protección unitaria a las marcas. La coexistencia de derechos marcarios nacionales es un reto puesto que el entorno en que se da el comercio electrónico es un entorno transfronterizo es decir que produce efectos en distintos países, debido a esto pueden surgir conflictos relacionados con la coexistencia en internet de derechos de exclusiva de distintos países que recaen sobre un mismo objeto pero pertenecen a diferentes titulares, y se plantea, por ejemplo, si el uso por uno de ellos del signo como nombre de dominio o en el contenido de una página web infringe la marca de otro. (De Miguel, 2018, p. 2 - 3)

En este sentido, se puede presentar que en una relación de comercio electrónico, en una venta transfronteriza, la comercialización de los productos no infrinja derechos de un país, por ejemplo, en el del comerciante, pero si puede infringirlos en otro país como en el que residen los compradores. Por consiguiente, existe una recomendación conjunta relativa con la protección de las marcas y otros derechos de propiedad industrial sobre signos en internet del 2001, adoptada esta por la Asamblea de la Unión de Paris y la Asamblea General de la OMPI; en esta se señaló que quien utiliza un signo distintivo en

internet es responsable por la infracción de una marca nacional con la que entre en conflicto, esto solo si la utilización tiene un efecto comercial en ese país. Conforme con (Torrubia, 2009), como se citó en (García, 2019), se proyecta lo siguiente.

> La red aparte de ofrecer nuevas oportunidades para las empresas también entraña nuevos riesgos que pueden perjudicar las marca tales como la suplantación de marca en los motores de búsqueda, o el uso de imágenes o material protegido por propiedad intelectual o copyright sin autorización, falsificaciones de productos en *marketplaces.* (p. 10)

En suma, en internet se presentan problemáticas relacionadas con la infracción de una marca comercial, en muchos sitios web se emplean marcas de los productos y los servicios de otras empresas sin la debida autorización, y hay una falta de legislación frente a dicha problemática. Cada día son más los problemas que se producen por esto, sin embargo, en Colombia estos obstáculos han sido mitigados por las acciones administrativas, judiciales, ordinarias o penales pertinentes, en busca de proteger sus derechos como propietarios y de acuerdo con el fin perseguido.

3.3. Riesgos asociados con los documentos electrónicos

Al momento de expedir documentos electrónicos se deben seguir unos requisitos que varían según el tipo de documento, y, en algunos ámbitos, es más exigente esta situación, tales como los casos donde se requiere la firma digital certificada. No obstante, así haya una regulación para situaciones más rigurosas, esta no es la regla general, además de ser un mecanismo complejo en vista de que no todos los individuos incumplen los requisitos para tener una firma digital; esto deja una brecha para quienes quieren

realizar negocios jurídicos y no cuentan con esa herramienta, en tal marco, los riesgos que se pueden generar son los siguientes.

3.3.1. El fraude electrónico y la usurpación de identidad en documentos electrónicos:

En este riesgo hay unas modalidades específicas, de conformidad con (Gabaldón y Pereira, 2008) son las presentadas a continuación.

- Falsificación de tarjetas sin permiso de su propietario.
- Fraudes de tarjetas pérdidas o interceptadas.
- Fraudes por sustitución de identidad, donde el impostor utiliza datos falsos o reales para abrir una cuenta a nombre de otro individuo.
- Falsificación de documentos electrónicos.

Estos riesgos conllevan a una usurpación de identidad basada en que una persona suplanta a otra en la titularidad de un derecho, esto para obtener un beneficio sin autorización del titular. De esta manera, se debe tener en cuenta que este riesgo es uno de los más materializados y suscita grandes pérdidas para todas las personas suplantadas; se debe confirmar que quienes realizan el negocio jurídico son, efectivamente, dichos sujetos, esto se toma como un documento electrónico con plena validez jurídica, por lo tanto, quien debe probar que se trata de un fraude es la persona que fue suplantada, pero existe una posibilidad alta de ausencia de las herramientas para comprobar esta situación, esto produce un perjuicio.

El modo de mitigar este riesgo es configurar mecanismos de autenticación y certificación de identidad que sean obligatorios para la celebración de cualquier negocio jurídico por medios digitales, para que no sea suficiente con los datos de identificación de un sujeto (nombre, cédula, entre otros) para indicar que ha sido verificada su identidad, pues estos son datos públicos que, aun cuando no gocen de confidencialidad y protección, pueden ser adquiridos con más facilidad. Por ende, si existen herramientas que aseguren la identidad del comprador, poco a poco los usuarios de las plataformas de comercio electrónico tendrán más confianza de usarlas, y quienes ofrecen los bienes y servicios se sentirán seguros de no ser parte de una estafa.

Equivalentemente, se debe resaltar que, para que un documento electrónico tenga validez, se demanda una verificación de identidad, empero, esto no significa la existencia de una autenticación de identidad, se ejecuta una firma electrónica sin que medien reglas que comprueben que la información no es suplantada, esto suscita inseguridad jurídica para los usuarios que pueden llegar a ser suplantados con una firma electrónica, y para la parte que ofrece sus bienes y servicios. Lo anterior debido a que estos confían en el comprador sin identificar que los presupuestos de autenticación de identidad son nulos, por lo tanto, el asunto se traduce en que la veracidad de la información se encuentra siempre en duda.

Para ahondar en este tema, (Musa, 2019) indicó: la normatividad internacional es donde es importante tener en cuenta que la autenticación electrónica busca validar la identidad de una persona que efectúa algún trámite electrónico con una entidad pública o privada, y tiene el objeto de mitigar el riesgo de suplantación en función de la confianza en las entidades que hacen uso del comercio electrónico. Asimismo, se debe considerar

que, con este mecanismo de autenticación, no solo se puede verificar la identidad de un usuario, también se identifica que el mensaje de datos no haya sido modificado, es decir, que sea integral; de esta manera, la Comisión de Naciones Unidas ha distinguido diversos tipos de factores de autenticación electrónicos, estos son los siguientes.

- Los que se basan en lo que el receptor sabe, por ejemplo, las contraseñas, entre otros.
- Los sujetos en las características físicas del usuario, por ejemplo, la autenticación biométrica.
- Los que tienen por propósito la posesión de un objeto, por ejemplo, una tarjeta magnética con un código.

De esta manera, se puede deducir que existe más de una herramienta para realizar la autenticación electrónica, que son equivalentes a una firma electrónica por medio de la cual el usuario se obligue con la contraparte en el negocio jurídico celebrado. Sin embargo, se debe tener en cuenta que ningún mecanismo es cien por ciento seguro, la entidad deberá conocer qué tipo de mecanismo de autenticación le conviene de acuerdo con sus procesos y dependiendo del grado de seguridad que requiera ofrecerles a sus usuarios, así, se permite concluir con esto la relevancia que tiene la autenticación electrónica, en el ámbito internacional del comercio electrónico.

Por otra parte, en la normatividad a nivel nacional aunque está más avanzada que otros países latinoamericanos en cuanto a comercio electrónico y traiga consigo un principio de equivalencia entre los documentos físicos y los documentos electrónicos para potenciar el comercio por los medios digitales, se empezó a identificar la importancia y necesidad de la autenticación digital para la realización de actos jurídicos de entidades

públicas y privadas, donde a finales del 2020 se expide la Resolución 2460 del Ministerio de las Tecnologías de la Información y las Comunicaciones por medio de la cual se consagra que para la prestación de Servicios Ciudadanos Digitales se debe implementar la autenticación digital en todas las entidades públicas, y las privadas que quieran adquirir esta herramienta, fundamentándose en la Ley 527 de 1999 antes analizada, este proyecto tiene como enfoque la seguridad y la garantía de los datos remitidos, donde se refuerza que la identificación de quien está realizando el trámite o celebrando el negocio jurídico si sea quien dice ser y que el mensaje de datos no haya sido alterado después de su emisión; sin embargo, a hoy no se han desarrollado herramientas que le permitan a los sujetos identificarse por medios electrónicos, de manera segura y fácil, el proyecto mencionado aun requiere de un desarrollo arduo que para constatar su eficiencia y efectividad se deberá esperar a su implementación, y así determinar si cumple con los lineamientos internacionales antes mencionados que buscan proteger y asegurar las transacciones que se realicen vía electrónica, y a su vez, si todos los sujetos podrán acceder a los mismos ya sean entidades públicas o privadas teniendo en cuenta su costo, nivel de rigurosidad sencilla implementación en los procedimientos de comercio electrónico.

Teniendo en cuenta lo mencionado anteriormente, lo que se busca con la implementación de la autenticación digital en todos los actos jurídicos que se realicen en el comercio electrónico, es identificar al firmante de manera inequívoca y asegurar la integridad del documento firmado, y de esta manera analizar qué metodologías debe adoptar una entidad pública o privada a la hora de identificar a una persona que hace uso de las plataformas digitales, para así tener una efectiva verificación de su identidad

y sus datos, generando más seguridad y confiabilidad en general para la población colombiana para de esta manera ir potenciando la economía a través de los medios tecnológicos.

4. Conclusiones

Como se abordó en los capítulos antecedentes, es notable que la regulación colombiana es escasa en cuanto a comercio electrónico, a pesar de ser uno de los países latinoamericanos pioneros en el desarrollo de la normatividad en esta materia, la tecnología cada vez crece y progresa rápidamente, esto le exige, a cada ordenamiento jurídico, la expedición de un conjunto de normas que limiten y permitan una ejecución sencilla de estos medios digitales por parte de los usuarios y las personas que ofrecen sus bienes y servicios. Lo anterior sin que se vean sometidos a la exposición de unos riesgos que, al momento de materializarse, pueden producir un profundo daño, y poca confianza y seguridad de su utilización.

Ahora bien, en materia de regulación de nombres de dominio se ultimó que no hay una regulación específica, a nivel nacional e internacional, que prevenga los riesgos derivados de la aplicación de este mecanismo, estos pueden conllevar a perjuicios y finiquitar en la comisión de delitos para una mayor probabilidad de materialización. En efecto, se denotó la necesidad mundial de realizar una reglamentación en este tema para prevenir el riesgo y evitar que las personas sean defraudadas al celebrar negocios jurídicos fraudulentos, esto con la implementación de una protección.

Se pudo constatar que el riesgo de los documentos electrónicos es la falsificación de identidad para celebrar un negocio jurídico; es necesario tener en cuenta que, internacionalmente, sí se ha buscado el desarrollo de mecanismos que si bien no aseguran un 100 % de efectividad, reducen la posibilidad de materialización del peligro de suplantación de identidad con unos métodos de autenticación digital. Es preciso

destacar que, aun cuando en Colombia no se ha implementado un asunto relativo con esto, se tiene en la mira el progreso de procesos para la seguridad de los ciudadanos, esto con la autenticación de identidad por medios digitales como una meta a ejecutar a corto plazo. Empero, se deberá hacer un seguimiento de cómo desemboca esta iniciativa, en virtud de que puede no llegar a lograr el objetivo trazado, por lo tanto, aunque sobre este riesgo en la regulación nacional e internacional se sigue un buen camino de mitigación, se debe esperar a la implementación de herramientas para deducir su eficiencia.

Como un corolario más, cabe resaltar que no es una observación solo para Colombia, sino para los países latinoamericanos carentes de estas normas para ajustar los medios digitales con los que se prestan servicios de comercio electrónico; de este modo, cada vez más se hace necesaria una regulación internacional de derecho comunitario que aplique, a nivel mundial, estas normas del comercio electrónico, para garantizar los derechos y la seguridad de las personas que hacen uso de los mecanismos nacionales de comercio electrónico y de páginas que efectúan envíos en escala mundial. Esto para suscitar la confiabilidad por parte de las personas, y promover este método potenciado en los últimos años, especialmente, en el 2020 por la pandemia del Covid-19, para un crecimiento y cumplimiento de los protocolos que eviten el contagio del virus por el contacto físico.

Adicionalmente, se concluye que la regulación sobre la firma digital es mucho más uniforme desde una mirada global, y tal y como se indicó en los párrafos anteriores, Colombia está intentando estar a la par con otros países en cuanto a la regulación de esta haciéndola más segura por medio de la autenticación digital. Por otra parte, en

cuanto al tema marcario y de dominios al no haber unificación de definiciones en el derecho internacional, cuando se celebran transacciones transfronterizas que contengan estos riesgos o cuando los mismos se materialicen para participantes de estos negocios jurídicos, existe más dificultad en la solución de los conflictos para definir que normatividad es la que les es aplicable generándoles incertidumbre y desconfianza.

5. Bibliografía

Anteportamlatinam Valero, J. (2014). *Relevancia del E-commerce para la empresa actual.* [Tesis de grado. Universidad de Valladolid]. Repositorio Institucional Universidad de Valladolid. http://uvadoc.uva.es/bitstream/handle/10324/5942/TFG-O%20174.pdf?sequence=1&isAllowed=y

Bachetta, M., Low, P., Mattoo, A., Schuknecht, L., Wagerand, H. & Madelon, W. (1998). *Electronic Commerce and the Role of the WTO.* Ginebra: World Trade Organisation.

Nametribune (2019). *¿Qué es secuestro inverso de dominios? Conceptos básicos*. https://nametribune.com/que-es-secuestro-inverso-de-dominios/#:~:text=El%20secuestro%20inverso%20de%20nombres,leg%C3%ADtimo%20due%C3%B1o%20de%20un%20dominio

Business.com . (2020). *The 10 Largest E-commerce Markets in the World by Country*. https://www.business.com/articles/10-of-the-largest-ecommerce-markets-in-the-world-b/

Cabezudo, V. (2020). *España lidera el crecimiento europeo en comercio electrónico.* Actualidad: https://www.muycanal.com/2020/12/01/espana-europa-comercio-electronic

Carbajo, F. (2002). *Conflictos entre Signos Distintivos y Nombres de Dominio en Internet.* Madrid: Aranzadi.

Cardenas Vega Propiedad Intelectual. (2020). *¿Cómo presentar una demanda por infracción marcaria en Colombia?* https://cardenasvega.com/index.php/cardenas-vega/boletin-intelectual/item/como-presentar-demanda-infraccion-marca

Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación. (2020). *CONPES 3995.* h

CSC. (s.f.). *Secuestro de DNS*. https://www.cscdbs.com/es/amenazas-digitales/secuestro-de-dns/

De Miguel Asensio, P. (2018). *Comercio electrónico y protección de marcas: aspectos internacionales*. En: De Miguel Asensio, P. (Ed). Problemas actuales de deercho de la propiedad industrial. Madrid: Tecnos

Electronic Identification. (2020). *Qué es la firma electrónica avanzada y para qué sirve.* https://www.electronicid.eu/es/blog/post/firma-electronica-avanzada/es

Equipo Woko. (2018). *E-commerce:* cómo debe ser un proceso de compra. https://woko.agency/blog/ecommerce-como-proceso-compra/

Espinosa, R. (s.f.). *Comercio Electronico: tipos, plataformas y ventajas.* https://robertoespinosa.es/2020/04/13/comercio-electronico

Ferrari Zamora, V. (2017). *El comercio electrónico en colombia: barreras y retos de la actualidad.* [Tesis de grado, Pontificia Universidad Javeriana]. Repositorio institucional U. Javeriana. https://repository.javeriana.edu.co/bitstream/handle/10554/36499/FerrariZamoraVanessa2018..pdf?sequence=1&isAllowed=y

Flores, P. (2012). *El Marco Civil de Internet: Brasil protege la neutralidad de la red*. https://hipertextual.com/2012/08/marco-civil-brasil

Flórez, G. (2014). La validez jurídica de los documentos electroónicos en Colombia a partir de su evolución legislative y jurisprudencial. *Verba Iuris,* (31), 43-71.

Gabaldón, L. G., & Pereira, W. (2008). Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. *Sociologias 10*(20), 164-190. DOI: scielo.br/pdf/soc/n20/a08n20.pdf.

García, V. (2019). Publicación marcaria por internet en Colombia. https://repository.ucatolica.edu.co/bitstream/10983/23771/1/PUBLICACION%20MARCARIA%20POR%20INTERNET%20EN%20COLOMBIA.pdf

Herreros, S. (2019). *Comercio Internacional. La regulación del comericio electrónico transfronterizo en los acuerdos comerciales.* Santiago: CEPAL.

ICANN. (s.f.). *¿Qué hace ICANN?* https://www.icann.org/resources/pages/what-2012-02-25-es

ICLG. (2020). *USA: digital business laws and regulations 2020*. https://iclg.com/practice-areas/digital-business-laws-and-regulations/usa

Increnta Colombia . (2018). *Marco Regulatorio del eCommerce.* https://www.observatorioecommerce.com.co/marco-regulatorio-del-ecommerce/

Infonegocios. (2020). Acuerdo e-commerce Mercosur: “Estamos caminando hacia la movilidad libre de productos, que es lo que necesitamos para incrementar la facturación”. Plus: https://infonegocios.com.py/plus/acuerdo-e-commerce-mercosur-estamos-caminando-hacia-la-movilidad-libre-de-productos-que-es-lo-que-necesitamos-para-incrementar-la-facturacion

Justia. (2019). *E-Commerce*. https://www.justia.com/business-operations/managing-your-business/e-commerce/

La República. (2021). *A*mérica Latina se rajó en el índice de *e-commerce* de empresa a consumidor el año pasado. https://www.larepública.co/globoeconomia/latinoamerica-se-rajo-en-el-indice-de-e-commerce-de-empresa-a-consumidor-2020-3127132

Lisandro, L. (2019). *Regulación jurídica de internet. el marco civil en Brasil*. https://bitsgrafia.com/doctrina/regulacion-juridica-de-internet-el-marco-civil-en-brasil/

Malca, O. (2001). *Comercio electrónico.* Lima: Universidad del Pacifico.

Merino, P. (2017). *Brasil, la locomotora que tira del ecommerce en América Latina*. https://ecommerce-news.es/brasil-la-locomotora-tira-del-ecommerce-america-latina/

Merizalde, S. (2018). *Protección de nombres de dominio en internet*. Asuntos Legales: https://www.asuntoslegales.com.co/análisis/sara-merizalde-533166/proteccion-de-nombres-de-dominio-en-internet-2719986

Ministerio de Industria y Comercio del Paraguay. (2020). Suscriben “Acuerdo sobre Comercio Electrónico del Mercosur”. mic.gov.py/mic/w/contenido.php?pagina=1&id=1856

Ministerio de Tecnologías de la Información y Comunicaciones. (2020). Resolución 000161 del 5 de febrero de 2020. [Por la cual se modifican las Resoluciones 284 y 1652 de 2008, se establece la política de administración del dominio de internet de Colombia (ccTLD .co) y se dictan otras disposiciones]. Bogotá, D. C. , Colombia.

Montezuma, O. (s.f.). *Brasil y su «Marco Civil da Internet»: análisis y perspectivas desde Perú.* https://www.blawyer.org/2014/04/22/marcocivil/

Moreno, C. (2019). *Recomendaciones de la OCDE en materia fiscal: aproximación al caso colombiano.* Universidad EAFIT : https://repository.eafit.edu.co/bitstream/handle/10784/15661/CarlosAndres_MorenoAlzate_2019.pdf?sequence=2&isAllowed=y

Musa, N. (2019). *Mecanismos de validación de identidad y firma electrónica certificados en la adquisición de productos o servicios comercializados en medios electrónicos.* Universidad Externado de Colombia: https://bdigital.uexternado.edu.co/bitstream/001/2892/1/GGAAA-spa-2019-

Mecanismos_de_validacion_de_identidad_y_firma_electronica_certificados_en_la_adquisicion_de_productos

Naciones Unidas. (2005). *Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005)*. https://uncitral.un.org/es/texts/ecommerce/conventions/electronic_communications

Naciones Unidas. (s.f.). *Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996) con su nuevo artículo 5 bis aprobado en 1998*. https://uncitral.un.org/es/texts/ecommerce/modellaw/electronic_commerce

Nametribune. (2019). *¿Qué es secuestro inverso de dominios?* https://nametribune.com/que-es-secuestro-inverso-de-dominios/#:~:text=El%20secuestro%20inverso%20de%20nombres,leg%C3%ADtimo%20due%C3%B1o%20de%20un%20dominio

Noticiero Oficial. (s.f.). *Tribunal de justicia de la comunidad andina*. https://www.noticieroficial.com/noticias/definicion-de-marca-y-de-los-requisitos-para-su-registro-3/182128

OMPI. (2020). *La OMPI contra el abuso de las marcas en Internet*. https://www.wipo.int/pressroom/es/prdocs/1999/wipo_pr_1999_170.html

OMPI. (s.f.). *Segundo Proceso de la OMPI relativo a los Nombres de Dominio de Internet*.

Organización Mundial de la Propiedad Intelectual [OMPI]. (s.f.). *La OMPI contra el abuso de las marcas en Internet.* Prenshttps://www.wipo.int/amc/es/processes/process2/report/html/annex15.html

Organización Mundial de la Propiedad Intelectual [OMPI]. (2003). *Segundo seminario regional sobre propiedad intelectual para jueces y fiscales de américa latina.*

http://www.oepm.es/cs/OEPMSite/contenidos/ponen/sem_jueces_03/informes/comunidad_andina.pdf

Organización para la Cooperación y el Desarrollo Económico [OCDE]. (s.f.). Recomendación del consejo de la ocde relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico. https://www.oecd.org/sti/consumer/34023784.pdf

PagBrasil. (s.f.). *Brasil, una de las mayores oportunidades de e-commerce en el mundo.* https://www.pagbrasil.com/es/mercado-brasileno/

Parra, Á. (2010). La protección jurídica de los nombres de dominio. *Derecho y realidad, 8*(15). https://revistas.uptc.edu.co/index.php/derecho_realidad/article/view/4977

Peña, Y. (2019). Comercio electronico ventajas y desventajas. Universidad cooperativa de Colombia : https://repository.ucc.edu.co/bitstream/20.500.12494/16999/3/2019_Comercio_electronico_ventajas.pdf

Qaz Wik. (2020). *Secuestro de dominio inverso*. https://es.qaz.wiki/wiki/Reverse_domain_hijacking

Rizzi, C. (s.f.). *E-Commerce: Its regulatory legal framework and the law governing electronic transactions – The situation in Italy.* https://www.diritto.it/articoli/tecnologie/tesi_rizzi_1_15.pdf

Rodríguez, A. (2019). *¿Qué es el cybersquatting o la ciberocupación?* https://es.godaddy.com/blog/que-es-el-cybersquatting-o-la-ciberocupacion/

Shopify Business. (2020). *Encyclopedia e commerce: Shopify*. https://www.shopify.com/encyclopedia/what-is-ecommerce

SICE. (s.f.). *Comercio electrónico Alianza del Pacífico. Capítulo 13.* http://www.sice.oas.org/trade/pac_all/comercioelectronico.pdf

Shopify Business. (2020). *Encyclopedia e-commerce: Shopify*. https://www.shopify.com/encyclopedia/what-is-ecommerce

Sttimel, Sttimel & Roeser. (s.f.). *Laws Pertaining to Commerce on the Internet*. https://www.stimmel-law.com/en/articles/laws-pertaining-commerce-internet

Suñe Llinas, E. & Almuzara Almaida, C. (2006). *Tratado de Derecho Informático. Vol. II, Servicios de la sociedad de la información e innovación jurídica, firma digital, servicios de la sociedad de la información y comercio electrónico.* Madrid: Servicio de publicaciones Universidad Complutense de Madrid.

Superintendencia de Industria y Comercio. (2005). Propiedad industrial. https://www.sic.gov.co/recursos_user/documentos/compendio/Propiedad.pdf

Think With Google. (2020). *Retail en España: el presente y futuro de los consumidores y empresas.*

thinkwithgoogle.com/_qs/documents/9011/Retail_en_Espana__el_presente_y_futuro_de_los_consumidores_y_empresas.pdf

Todd, P. (2005). *E-Commerce Law.* Avingdon: Routledge-Cavendish.

Toro, J. (2021). América Latina se rajó en el Índice de e-commerce de empresa a consumidor el año pasado. Comercio: https://www.larepublica.co/globoeconomia/latinoamerica-se-rajo-en-el-indice-de-e-commerce-de-empresa-a-consumidor-2020-312713

Trabado, M. (2018). *8 pasos para crear un ecommerce de éxito asegurado*. Semrush: https://es.semrush.com/blog/pasos-crear-ecommerce-exito/

Unión Europea. (2015). *Comercio para todos.* LUxemburgo: Unión Europea.

United Nations . (1998). *UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998*. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

Universidad Externado de Colombia. (2017). *Documentos electrónicos transferibles: CNUDMI adopta legislación modelo*. https://dernegocios.uexternado.edu.co/

Vásquez, M., & Valencia, A. (2019). *Límites de la normatividad en materia de comercio electrónico en Colombia.* Universidad EAFIT: https://repository.eafit.edu.co/bitstream/handle/10784/13825/MariaIsabel_Vasquez_Aelajndro_Valencia_2019.pdf?sequence=2&isAllowed=y

Zwass, V. (s.f.). *Comercio electrónico*. Britannica: https://www.britannica.com/technology/e-commerce

Normas legislativas citadas

Asamblea Nacional Constituyente. (1991). *Constitución política de Colombia.* Legis.

Barchetta, M., Low, P., Mattoo, A., Schuknecht, L., Wager, H., & Wehrens, M. (1998).

Congreso de la República de Colombia. (1995). Ley 222 de 20 de diciembre de 1995. Diario Oficial No. 42.156. Bogotá, Colombia.

Congreso de la República de Colombia. (1996). Ley 256 de 15 de enero de 1996. Bogotá, Colombia.

Congreso de la República de Colombia. (1996). Ley 270 de 7 de marzo de 1996. Diario Oficial No. 42.745. Bogotá, Colombia.

Congreso de la República de Colombia. (1999). Ley 527 de 18 de agosto de 1999. Diario Oficial No. 43.673. Bogotá, Colombia.

Congreso de la República de Colombia. (2000). Ley 633 de 29 de diciembre de 2000. Diario Oficial No. 44.275. Bogotá, Colombia.

Congreso de la República de Colombia. (2005). Ley 962 de 8 de julio de 2005. Diario Oficial No. 46.023. Bogotá, Colombia.

Congreso de la República de Colombia. (2007). Ley 1150 de 16 de julio de 2007. Diario Oficial No. 46.691 . Bogotá, Colombia.

Congreso de la República de Colombia. (2008). Ley 1266 de 31 de diciembre de 2008. Diario Oficial No. 47.219. Bogotá, Colombia.

Congreso de la República de Colombia. (2008). Ley 1331 de 17 de julio de 2008. Diario Oficial No. 47.053. Bogotá, Colombia.

Congreso de la República de Colombia. (2009). Ley 1273 de 5 de nero de 2009. Diario Oficial No. 47.223. Bogotá, Colombia.

Congreso de la República de Colombia. (2011). Ley 1480 de 12 de ocrubre 2011. Diario Oficial No. 48.220. Bogotá, Colombia.

Congreso de la República de Colombia. (2012). Ley 1581 de 17 de octubre de 2012. Diario Oficial No. 48.587. Bogotá, Colombia.

Congreso de la República de Colombia. (2019). Ley 1955 de 25 de mayo de 2019. Diario Oficial No. 50.964. Bogotá, Colombia.

Presidencia de la República de Colombia. (2012). Decreto 2364 de 22 de noviembre de 2012 . Bogotá, Colombia.

Presidencia de la República de Colombia. (2015). Decreto 1078 de de 26 de mayo de 2015. Diario Oficial No. 49.523 . Bogotá, Colombia.