Protección de datos y comercio electrónico: una revisión de los desafíos jurídicos para Colombia en el 2023[1]

Luisa Fernanda Díaz Barrientos[2]

Resumen: Este artículo tiene como objetivo abordar los desafíos del comercio electrónico y la protección de datos para el sistema jurídico colombiano en 2023. Para ello, se desarrolla una metodología cualitativa y descriptiva basada en la revisión de investigaciones previas, informes gubernamentales y académicos, artículos de investigación y normas jurídicas. Como resultado se obtiene que la protección de datos y el comercio electrónico, de forma independiente, están siendo ampliamente abordados desde lo normativo y lo jurisprudencial; no obstante, al tratarse de protección de datos en el marco del comercio electrónico no se cuenta con regulación específica que asegure la confianza de los consumidores en las entidades que manejan sus datos. Se concluye que el mayor desafío está en establecer una regulación específica que garantice una aplicación efectiva y sólida salvaguardia para los consumidores que confían sus datos personales en el entorno del comercio electrónico. Además, es crucial fomentar una cultura de protección de datos y conciencia entre los ciudadanos, promoviendo el conocimiento de sus derechos y deberes en este ámbito.

Palabras Clave: sociedad digital, habeas data, comercio electrónico, ciberseguridad, derecho tecnológico.

Abstract

This article aims to address the challenges of electronic commerce and data protection for the Colombian legal system in 2023. To do so, a qualitative and descriptive methodology is

[1] Artículo de revisión para optar por el título de abogada en la Universidad Católica Luis Amigó. En ejecución año 2023.

[2] Profesional en Negocios Internacionales. Universidad Católica Luis Amigo, Medellín, Colombia. 2015; Estudiante de décimo semestre de Derecho. Universidad Católica Luis Amigó, Medellín, Colombia. 2023. https://orcid.org/009-0009-2825-775X; luisa.diazba@amigo.edu.co

developed based on the review of previous research, government and academic reports, research articles. and legal norms. As a result, data protection and electronic commerce, independently, are being widely addressed from a regulatory and jurisprudential perspective; However, when it comes to data protection in the framework of electronic commerce, there is no specific regulation that ensures consumer trust in the entities that handle their data. It is concluded that the greatest challenge is establishing a specific regulation that guarantees effective application and solid safeguards for consumers who trust their personal data in the electronic commerce environment. Furthermore, it is crucial to foster a culture of data protection and awareness among citizens, promoting knowledge of their rights and duties in this area.

Keywords: digital society, habeas data, e-commerce, cybersecurity, technology law.

Introducción

La cuarta revolución industrial, la masificación del internet, las redes sociales y el metaverso traen consigo nuevas formas de relacionamiento social. En estos espacios virtuales las personas interactúan en charla, discusión, enseñanza, contratación, e incluso, el amor. Así, es como se consolida la sociedad digital, que cada vez rompe más límites de la distancia y le apuesta a la inmediatez que le ofrece la tecnología (Arteaga, 2023).

De acuerdo con Hootsuite y We Are Social (2020) para el 2020 la población mundial alcanzó los 7.8 miles de millones de personas, de los cuales 5.2Mm usan dispositivos móviles, 4.5Mm son usuarias de internet y 3.8Mm están activas en redes sociales. Colombia, con una población cercana a los 50.6 millones de personas tiene el 119% de conexión a teléfonos móviles y 35 millones de usuarios de internet (Campuzano et al., 2021).

No obstante, en un entorno de interconexión y digitalización como el expuesto se pueden acentuar la exclusión y desigualdad social. En este campo, estos fenómenos se manifiestan a través de la brecha digital, que se refiere a la inequidad en el acceso a las tecnologías de la información y la comunicación para poblaciones históricamente excluidas como discapacitados, migrantes y personas de bajos recursos (García et al., 2020).

Diversos autores han determinado que la brecha digital no solo se refiere a tener o no acceso a las nuevas tecnologías, sino que, para hacer frente a las desigualdades sociales, es importante hablar de alfabetización digital como el medio para el mejor uso y aprovechamiento de las TIC (Ragnedda, 2017).

De acuerdo con el Ministerio de Tecnologías de la Información y las Comunicaciones-MinTIC- (2022), en una escala de 0 a 1, en la que cero es la menor brecha digital y uno la mayor, Colombia obtuvo 0,4107 puntos en brecha digital para el 2021. Esto, teniendo en consideración las habilidades digitales, el acceso al material, el aprovechamiento y la motivación de la población frente a las TIC.

Además de la brecha digital, en tiempos de interconexión y digitalización social se han presentado amplios desafíos para los gobiernos mundiales a fin de regular las relaciones que se dan en el espacio virtual y, así como se extiende el ejercicio de los derechos a esos entornos, ampliar su protección. De ahí el origen del derecho informático como la rama del derecho que busca regular todas las conductas que se desarrollen por medio de los sistemas informáticos (Arteaga, 2023).

Las mayores transformaciones de la tecnología en la historia se han enmarcado en cuatro revoluciones. La primera se caracterizó por la producción mecánica; la segunda, por los avances en la industria química, eléctrica y automotriz; la tercera, por el surgimiento del internet y el desarrollo de las Tecnologías de la Información y la Comunicación (TIC). La cuarta revolución inició con el siglo XXI y se ha caracterizado por la digitalización, el manejo de altos volúmenes de información (Big Data), la Inteligencia Artificial (IA), la robótica y la biotecnología (Martínez et al., 2020).

La cuarta revolución se caracteriza por la convergencia de diversas tecnologías digitales, físicas y biológicas. Entre ellas se encuentran la IA, la inteligencia aumentada, la robótica, la impresión 3D, el *cloud computing*, el *big data*, el "internet de las cosas" y la nanotecnología (Rose, 2016). Esta convergencia da lugar a lo que se conoce como redes ciberfísicas, que ya se encuentran presentes en diversos ámbitos laborales, financieros y de entretenimiento, y poseen la capacidad de autorregularse y tomar decisiones de manera autónoma, con una mínima o nula intervención de seres humanos (Escudero, 2018).

En esa línea, la tecnología ha permeado todos los ámbitos de la vida y las relaciones humanas, lo que ha hecho necesario que el derecho se adecúe a través del sistema jurídico para ampliar su regulación y protección de la vida en sociedad. En las relaciones comerciales, la tecnología se manifiesta a través del comercio electrónico, que se refiere a toda clase de transacciones comerciales que se den en medios electrónicos (Knight y Liesh, 2016).

Según Moreno (2014) el comercio electrónico es un paso fundamental para avanzar en la globalización, ayuda a las pequeñas empresas a ser más competitivas y a aspirar al comercio mundial. La pandemia del Covid-19 repotencializó las compras por internet para dinamizar la economía de los países, lo que, además de beneficios económicos, representó desafíos legales para los gobiernos, especialmente, en la protección de los derechos de los consumidores (Limas, 2020).

A la par del auge de la tecnología y de su incursión en campos como el comercio, se han incrementado las conductas contra derecho en la red. La delincuencia se ha trasladado a los entornos digitales, sistemas informáticos, programas, aplicaciones, redes sociales, etc., esto es lo que se conoce como ciberdelincuencia (Arteaga, 2023).

El ciberdelito se materializa cuando un individuo hace uso de las TIC para facilitar la realización de una conducta típica, antijurídica y culpable, puede involucrar acciones de varia índole como ataques a equipos, uso de computadores para difundir códigos maliciosos, obtención de información ilegal y robo de datos personales con fines fraudulentos (Mejía et al., 2023).

Según Mejía (2021) los tipos de ciberdelincuencia están estrechamente relacionados con el uso de datos para fines ilegales, por lo que se ha hecho necesario implementar estrategias y políticas públicas para su protección. En ese contexto surge el habeas data como el derecho de todo titular de datos personal de exigir el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de sus datos, así como la facultad de prohibir su divulgación, publicación o cesión (Gil, 2017).

Al considerar que las nuevas tecnologías han dado paso a la sociedad digital, en la que se dan nuevas formas de interactuar, comunicar y realizar actividades desafiando los límites de la distancia y priorizando la inmediatez, es importante ahondar en los esfuerzos

del sistema jurídico para contextualizarse a esta realidad y satisfacer las nuevas necesidades de la sociedad.

En ese sentido, el objetivo de este artículo es analizar los desafíos jurídicos del comercio electrónico y la protección de datos para Colombia en 2023, teniendo en cuenta que son ámbitos importantes para el desarrollo de la vida en sociedad y que, por tanto, han exigido una amplia regulación internacional y nacional a fin de extender la protección de bienes jurídicos al espectro tecnológico.

En este artículo se abordan los esfuerzos jurídicos del sistema colombiano, específicamente en las áreas de: protección de datos (habeas data) y comercio electrónico, teniendo en cuenta que son campos interrelacionados y que se han visto impactados significativamente por el auge de las nuevas tecnologías. Esto, con el fin de brindar un panorama de los impactos de la tecnología en sistema jurídico de Colombia y vislumbrar los desafíos que aún están pendientes.

Para ello, se propone desarrollar este artículo en cuatro partes: introducción al contexto del habeas data y el comercio electrónico en Colombia; la metodología propuesta para la investigación cualitativa y documental; resultados sobre la protección de datos y el comercio electrónico de forma independiente y el tratamiento de la protección de datos en el marco del comercio electrónico. Finalmente, se presentan las conclusiones sobre el gran desafío de establecer una regulación específica que garantice una aplicación efectiva y sólidas salvaguardias para los consumidores que confían sus datos personales en el entorno del comercio electrónico.

El apartado de los resultados y las conclusiones se relacionan y estructuran de acuerdo con los objetivos investigativos: 1) examinar la normativa y el estado del arte de la protección de datos en Colombia hasta el 2023; 2) abordar la normativa y estado del arte del comercio electrónico en Colombia hasta el 2023; y 3) relacionar el comercio electrónico y la protección de datos desde los hallazgos normativos y académicos en Colombia hasta el 2023. Y a partir de estos objetivos específicos, se cumple con el objetivo general del artículo sobre analizar los desafíos jurídicos del comercio electrónico y la protección de datos para Colombia en 2023.

Metodología

Esta investigación se enmarca en el enfoque cualitativo de carácter descriptivo. Es un estudio documental que se basa en la revisión de investigaciones previas, informes gubernamentales y académicos, artículos de investigación y normas para lograr el objetivo propuesto. Según Hernández (2018), este es un estudio que se caracteriza por su énfasis en la interpretación, la comprensión profunda, el análisis de contenido y la atención al contexto, todo ello con el objetivo de generar conocimiento significativo a partir de fuentes documentales. Así, el aporte de este artículo se circunscribe en su enfoque, reflexiones, análisis y conclusiones.

La revisión documental se llevó a cabo por medio de la búsqueda en las bases de datos GoogleScholar, Scopus, Scielo, Redalyc, LexBase, Corte Constitucional de Colombia, Congreso de la República de Colombia, y otras gubernamentales como el Ministerio de Tecnologías de la Información y Comunicación de Colombia (MinTIC).

Después de acotar la revisión documental a través de las palabras clave: “Habeas data”, “Comercio electrónico”, y otras relacionadas con el objeto de estudio planteado, siempre en el contexto colombiano. Se excluyeron los documentos no relacionados con estas categorías de análisis, con el fin de mantener el marco investigativo establecido por el objetivo formulado. Para, finalmente, obtener 12 informes, 17 artículos de investigación, 8 normas jurídicas y 15 sentencias judiciales.

Gracias a la información recolectada se da desarrollo a los objetivos específicos planteados: 1) examinar la normativa y el estado del arte de la protección de datos en Colombia hasta el 2023; 2) abordar la normativa y estado del arte del comercio electrónico en Colombia hasta el 2023; y 3) relacionar el comercio electrónico y la protección de datos desde los hallazgos normativos y académicos en Colombia hasta el 2023. Y a partir de esto, se cumple con el objetivo general del artículo sobre analizar los desafíos jurídicos del comercio electrónico y la protección de datos para Colombia en 2023.

Resultados

Protección de datos en Colombia

En el contexto colombiano, la regulación del tratamiento de datos personales ha sido abordada a través de la legislación, la jurisprudencia de la Corte Constitucional y la doctrina.

La primera normativa en abordar el tratamiento de los datos en Colombia fue la Ley 1266 (2008), en la cual se regula el uso de los datos personales exclusivamente en asuntos crediticios, financieros, comerciales y de servicios. Allí se estableció que el tratamiento de datos es la actividad reglada para manejar la información tecnológica en el marco de la legalidad y la constitucionalidad.

Posterior a la Ley 1266 (2008), que limitó al sector financiero y de servicios, surgió la Ley Estatutaria 1581 (2012), y con ella, el abordaje del tratamiento de datos en el marco de tres principios fundamentales: transparencia, en cuanto el titular puede acceder a sus datos en cualquier momento y sin restricción; seguridad, ya que los datos deben ser manejados con las medidas técnicas, humanas y administrativas necesarias para la seguridad del titular; y confidencialidad, puesto que se debe garantizar la reserva de los datos y su uso exclusivo en el desarrollo de actividades autorizadas por la constitución y la ley.

La Ley 1581 (2012) incorporó disposiciones generales para el almacenamiento de datos para garantizar los derechos fundamentales a la intimidad y al buen nombre, protege integralmente cualquier clase de datos de personas naturales y jurídicas que se encuentren en bancos de información.

Para cumplir con la protección que se espera en la Ley 1581 (2012, art. 19) se designó a la Superintendencia de Industria y Comercio como la encargada de vigilar el cumplimiento de las disposiciones consagradas en la norma, como consecuencia puede ordenar medidas de cumplimiento como el bloqueo de datos.

En cuanto al tratamiento de datos, según la Ley 1581 (2012), los comerciantes pueden recolectar datos personales, pero deben obtener el consentimiento informado y previo de los titulares de los datos (Ley 1581, 2012, art. 2). Pueden realizar el tratamiento

de datos personales con fines comerciales, siempre y cuando respeten los principios de finalidad, necesidad y proporcionalidad.

Además, los comerciantes pueden utilizar los datos personales recopilados para llevar a cabo actividades comerciales y de mercadeo, siempre que se ajusten a los propósitos previamente informados y autorizados por los titulares. Sin embargo, es importante que cumplan con todas las disposiciones establecidas en la Ley 1581 para garantizar la protección adecuada de los datos personales y la privacidad de los individuos.

Existe un tipo de datos con los que el comerciante o administrador de bases de datos debe tener especial cuidado, estos son los datos sensibles, que son aquellos que afectan la intimidad del titular y por su uso indebido se puede dar discriminación o vulneración de garantías fundamentales. De este tipo son aquellos datos que revelen "origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos (…) datos relativos a la salud, a la vida sexual y los datos biométricos" (Art. 5, Ley 1581, 2012).

Para la Corte Constitucional (2002; 2012a; 2020) los datos, en general, son aspectos exclusivos y propios de una persona natural, que permiten identificarla; son de su propiedad y plena disposición, por lo que están sujetos a reglas y principios especiales. De esa aproximación conceptual se derivan tres dimensiones o reglas de los datos: 1) el titular y el dato tienen un vínculo inquebrantable, por lo que puede solicitar acceso, rectificación, actualización, exclusión y certificación a quien administra la información; 2) el titular puede limitar la difusión de su dato; y 3) el titular puede exigir a quien administra su dato que se sujete estrictamente a los límites constitucionales y legales del tratamiento de información (Sentencia T-058 de 2015).

Además, en Sentencias C-748 de 2011 y T-238 de 2018, la Corte Constitucional (2011; 2018) clasificó los datos en: privados, que tratan de información personal a la que solo se puede acceder por autoridad judicial; semiprivados, que a pesar de no ser privado o sensible tampoco es público, ya que su conocimiento y divulgación puede interesar a su titular y un sector específico como el financiero; reservados o sensibles, que versa sobre información personal relacionada con derechos fundamentales a la dignidad, intimidad y libertad, por lo que no puede accederse a ella ni siquiera con autoridad judicial; públicos, ya

que es información general que se puede obtener sin reserva alguna; y semiprivada, porque para acceder a ella se presenta un grado mínimo de limitación de acceso.

En el contexto contemporáneo, en el que el avance tecnológico y la rápida transmisión de vastas cantidades de información son predominantes, la Corte Constitucional (1992; 1999) enfatiza que aquellos individuos con la capacidad de adquirir, recopilar y divulgar datos adquieren un "poder informático", por lo que es crucial controlar y restringir este poder en beneficio de la ciudadanía.

El poder informático es un tipo de dominación social que se ejerce sobre el individuo a través de la acumulación ilimitada de información para hacerle seguimiento y difundirla como mercancía (Sentencia T-729 de 2002). Así, quien tiene el poder informático puede representar un riesgo para el titular del dato en derechos fundamentales como la intimidad, el buen nombre, el debido proceso, entre otros (Sentencia T-307 de 1999).

Este poder informático, en Colombia, se identificó inicialmente en la asimetría de información en el ámbito financiero. Debido a problemas de interpretación de la ley, en este sector, se presentan ausencia, error y falta de oportunidad en el manejo de la información, lo que se traduce en conflictos con los derechos fundamentales de los titulares de los datos (Devis et al., 2019).

Con el transcurrir del tiempo, y con el desarrollo tecnológico, la asimetría de información no solo se hizo presente en el sector financiero, sino que se extendió a los demás sectores económicos y sociales. Fue a partir del relacionamiento entre la asimetría de información y los derechos fundamentales que en Colombia se empezó a hablar de tratamiento de datos y habeas data.

En ese sentido, la Corte Constitucional (1992; 1994; 1995; 2008); ha desarrollado ocho importantes reglas jurisprudenciales para el tratamiento de datos. La titularidad del dato personal es exclusiva de la persona y no del administrador de la base de datos (Sentencia T-414 de 1992); el procesamiento y la difusión de datos debe tener un fin constitucional y legalmente legítimo (Sentencia C-1011 de 2008); debe existir autorización del titular del dato para acceder a él en las centrales de información (Sentencia SU-082 de

1995); la información personal almacenada en las bases de datos debe ser la estrictamente necesaria para el cumplimiento de los fines de esta (Sentencia SU-082 de 1995).

Además, la información debe cumplir con una función determinada en las bases de datos (Sentencia C-1011 de 2008); quienes recolectan, tratan y ponen en circulación los datos deben garantizar que sean veraces (Sentencia T-157 de 1994); la circulación de los datos se encuentra limitada por la autorización del titular y el principio de finalidad (Sentencia C-1011 de 2008); el dato negativo caduca y se da el derecho al olvido (Sentencia SU-082 de 1995).

Los principios y reglas para el tratamiento de datos expuestos son los que dan paso al habeas data. El habeas data hace referencia al derecho que tiene un sujeto de acceder y disponer de sus datos personales, aunque estén en poder de otro (Newman, 2015; Constitución Política de Colombia (CP), 1999, art. 15; Corte Constitucional, 2015). Es un derecho fundamental autónomo que busca proteger los datos personales y tiene, según la Corte Constitucional (2011; 2012a), cinco contenidos mínimos: por acceder a la información, poder incluir nuevos datos, poder actualizar la información, poder corregir la información, y poder excluir información de bases de datos.

Para la Corte Constitucional (1995) el núcleo esencial del habeas data se encuentra en el derecho a la autodeterminación informática y la libertad, en el sentido de que el titular del dato se encuentra facultado para autorizar su uso, conservación y circulación según el ordenamiento jurídico. El sujeto activo del derecho es toda persona física o jurídica con datos susceptibles a tratamiento; el sujeto pasivo es toda persona física o jurídica que use sistemas de información para el tratamiento de datos. Así, el sujeto activo tiene el derecho al habeas data: a autodeterminarse informáticamente en libertad.

El habeas data surge por la compleja relación entre los avances tecnológicos y la privacidad individual (Gil, 2017). En ese contexto, al habeas data se le ha atribuido una estrecha relación con la dignidad, la intimidad, el buen nombre, el acceso a la información, la libertad, la autodeterminación y la libertad informativa (Gómez et al., 2020). Por ello, el habeas data ha sido calificado como fundamental por la Corte Constitucional (2022a), lo que ha permitido que se use para equilibrar el poder entre el titular del dato y quien lo

recolecta, almacena, utiliza y transmite; y, además, que sea garantizado a través de la acción de tutela.

En ese marco, se han dado diversos pronunciamientos normativos y jurisprudenciales con la expectativa de proteger los datos en los diversos ámbitos tecnológicos, que se extienden y modernizan constantemente.

Pese a la existencia de estas normas de habeas data, los jueces han debido interpretar disposiciones internacionales y constitucionales en casos concretos que cada vez son más retadores por las implicaciones tecnológicas y jurídicas para la vida en sociedad. En Sentencia C-406 de 2022, la Corte Constitucional (2022a) tuvo que decidir sobre la exequibilidad de una disposición que permitía la vigilancia de la Policía Nacional a través de circuitos cerrados para garantizar la seguridad de las personas y bienes. En ese pronunciamiento, la Corte dictaminó que las acciones de vigilancia, para ser constitucionales y legales, deben representar una ventaja de seguridad proporcional a los derechos fundamentales que se ponen en riesgo como la intimidad personal y el habeas data.

Es decir, el argumento de la seguridad de las personas y lo bienes no es suficiente para vulnerar los derechos fundamentales a la intimidad personal y al habeas data, es necesario que las acciones sean proporcionales para representar el mayor beneficio y el menor perjuicio para los derechos de las personas.

En sentencia SU-139 de 2021, la Corte Constitucional, al decidir sobre la solicitud de antecedentes judiciales por una persona que se encontraba fuera del país, afirmó que administrar las bases de datos de antecedentes judiciales es una función pública de la policía y, por tratarse de datos negativos, su acceso y conocimiento por parte del titular se sujeta a la protección legal y constitucional del habeas data.

Por otro lado, en Sentencia SU-086 de 2022, a raíz del caso de una persona que fue reportada en DATACRÉDITO por una entidad financiera y que, posterior al pago de su obligación, continuó con el reporte y una anotación de “cartera recuperada”, lo que le impedía obtener servicios financieros en otras entidades. La Corte Constitucional (2022b) unificó su posición frente a que los administradores de bases de datos deben asegurarse de que la información compartida en sistemas digitales sea clara y no deje lugar a diversidad

en interpretaciones por parte de autoridades administrativas u otras personas que tengan acceso a ella.

En Sentencia SU-191 de 2022, la Corte Constitucional (2022c) conoció el requerimiento de un ciudadano y periodista a la Arquidiócesis de Medellín para conocer datos sobre denuncias sexuales en contra de sacerdotes, lo que incluía información de los sujetos y de los procesos en curso. Ante la negativa de la entidad religiosa para brindar la información solicitada, el actor interpuso acción de tutela, la cual abrió la puerta para que la Corte Constitucional unificara su posición sobre los datos semiprivados y la restricción legal para el administrados de dichos datos.

En esta sentencia, la Corte (2022c) destacó que el habeas data le da la facultad al titular del dato de exigirle al administrador de la información que se limite su divulgación, publicación y cesión. Además, afirmó que la restricción legal para que los administradores difundan datos semiprivados sin autorización del titular no es absoluta, ya que debe ser ponderada en la medida en que en el ordenamiento jurídico no exista ningún otro medio para resolver la tensión que se deriva del requerimiento de acceso por terceros.

En el contexto jurisprudencial colombiano, la protección del habeas data se ha erigido como una clave para para el equilibrio entre la seguridad pública y la intimidad. Así, a pesar del poder informático que le asiste al Estado, se consolida el poder del titular del dato para controlar su uso, y se reconoce la necesidad de sopesar la restricción legal frente a otras alternativas en el marco jurídico.

Por lo expuesto, se infiere que el desafío actual de los jueces frente a la vaga normativa sobre habeas data se circunscribe en la administración de datos por parte del Estado y sus autoridades administrativas. Sin embargo, un reto futuro, que cada vez se hace más latente es el habeas data en la administración de datos por parte de empresas privadas en virtud del comercio electrónico.

Como lo señala Monsalve (2017), en la adquisición de bienes y servicios en la red, los compradores deben digitalizar sus datos personales, sin conocer qué pasará con su información luego de su incorporación en la red. Esto ha representado un reto de manejo y control por parte de autoridades y organizaciones internacionales. Ante la ausencia de lineamientos legales específicos, las empresas privadas toman distintos datos y su

tratamiento se lleva a cabo de forma incongruente con el derecho al habeas data (Gómez et al., 2020).

No obstante, para abordar los retos del habeas data en el comercio electrónico, es menester ahondar, primero, en la normativa y estado del arte del comercio electrónico en Colombia, tal y como se presenta en el siguiente apartado.

Comercio electrónico en Colombia

Según Campuzano et al. (2021), del total de usuarios de internet con edades comprendidas entre los 16 y 64 años en Colombia, un 80% realiza búsquedas de productos o servicios para su compra, un 90% ha visitado plataformas de comercio electrónico, un 74% ha efectuado compras en línea, un 36% ha realizado adquisiciones desde un ordenador y un 52% ha llevado a cabo compras utilizando dispositivos móviles.

Esto demuestra la gran relevancia del comercio electrónico o E-Commerce en la sociedad actual. De acuerdo con el Consejo Nacional de Política Económica y Social (CONPES) (2020), el comercio electrónico se refiere a la venta o compra de bienes y servicios por medio de redes informáticas.

Según las estadísticas de Statista (BlackSip, 2019), en el 2018 Colombia se ubicó como el cuarto país latinoamericano con ingresos por ventas de E-Commerce por 6.000 millones de dólares. Esto incrementó con la pandemia por el Covid-19 (Limas, 2020), lo que, además de representar beneficios, ha significado grandes retos y esfuerzos para el sistema jurídico colombiano en la regulación y la protección de los derechos de los consumidores electrónicos.

Según Ramírez (2021), economista senior de la Cámara Colombiana de Comercio Electrónico-CCCE-, en 2019, las ventas en línea fueron de 21,8 billones de pesos, pero en 2020 aumentaron significativamente a 28,4 billones de pesos, representando un crecimiento del 30,2%. Las transacciones también aumentaron de 101,4 millones en 2019 a 181,9 millones en 2020, un aumento del 79,4%. Este aumento se debió en gran parte a la pandemia, que impulsó la migración de actividades cotidianas al entorno digital y redujo las compras en el sector turismo, que tiene un alto valor unitario por compra.

En el año 2021, el comercio electrónico en Colombia continuó la tendencia del 2020. Durante el período de enero a septiembre de 2021, los niveles de ventas digitales se mantuvieron por encima de los niveles registrados antes de la pandemia. En el tercer trimestre de 2021, las ventas en línea alcanzaron valores cercanos a los 10 billones de pesos, lo que representa un incremento del 79,6% en comparación con las ventas del mismo trimestre en 2019, y un aumento del 31,7% en comparación con las ventas del tercer trimestre de 2020 (Ramírez, 2021).

Para el 2022, la CCCE (2022) reportó un crecimiento de 35,4% de las ventas en línea respecto del 2021, por lo que se espera que para el 2023 el progreso sea del 14% en contraste con el 2022. Estos datos no son más que la muestra de que la pandemia cambió la forma en que los colombianos adquieren productos y servicios, dando fuerza al comercio electrónico.

Teniendo en cuenta estas cifras de progreso del comercio electrónico en Colombia, se ha hecho necesario que tanto el sector público como el privado se esfuercen por visibilizar el desarrollo de este comercio, regularlo e implementar acciones para incentivarlo. En ese sentido, se han dictado múltiples normativas e informes, las cuales se abordan a continuación.

De acuerdo con la Ley 527 (1999) el comercio electrónico se refiere a toda relación comercial que se estructure a través de mensajes de datos u otro medio similar. Las relaciones comerciales se derivan de actividades como suministro e intercambio de bienes y servicios, operaciones financieras, consultorías, explotación o concesión de servicios públicos, entre otras consagradas en la normativa comercial.

En esta ley (527 de 1999) se reconoció validez jurídica a la información contenida en mensajes de datos (Arts. 5 y 14). También se estableció que la validez de la firma en mensajes de datos se determina por la posibilidad de identificar al iniciador del mensaje y que el contenido tiene su aprobación; además, que el método de firma sea confiable y apropiado según el mensaje generado (Art. 7).

Por otra parte, se consagró que la originalidad del documento por mensaje de datos se satisface cuando la información es accesible para la consulta; el documento se conserva en el formato en que se generó, envió o recibió para demostrar la exactitud de la

información; y que se mantenga toda información que vislumbre el origen, destino, fecha y hora de envío y recibido del mensaje de datos (Art. 12, Ley 527, 1999).

Así, esta norma reconoce la equivalencia funcional de los negocios jurídicos llevados a cabo a través de mensajes de datos con los físicos, tanto en su validez jurídica (Arts. 5 y 14) como en su fuerza probatoria en toda actuación administrativa y judicial (Art. 10).

Posterior a esta normativa, en Colombia se han adoptado distintas disposiciones legales para ampliar la vigilancia del comercio electrónico. La Ley 1231 (2008) fue la primera para implementar la factura electrónica como título valor para fortalecer el comercio electrónico en el país. Por medio de ella se facilitó la negociación y respaldo de las facturas, lo que ayudó a las MIPYMES a acceder a recursos financieros más fácilmente. También regula aspectos como la emisión, transmisión, endoso y protesto de las facturas, brindando un marco legal para su utilización como mecanismo de financiación.

Una de las normas más importantes para el comercio electrónico es la Ley 1480 (2011) o Estatuto del Consumidor, el cual es aplicable tanto para el comercio físico como electrónico. En ese estatuto se reglamentan los derechos y debes de productores, proveedores y consumidores de bienes y servicios. Además, incentiva el comercio electrónico adoptando un capítulo especial para los consumidores en ese entorno (Arts. 49-54).

Según el capítulo especial de protección al consumidor de comercio electrónico los proveedores deben proporcionar información clara, veraz, actualizada y completa de su identidad y de los productos o servicios que ofrecen, también deben dejar claro los medios de pago disponibles, el tiempo de entrega, el derecho de retracto y su procedimiento. Adicionalmente, se deben adoptar medidas de seguridad para proteger los datos personales de los consumidores. Finalmente, se establece que las controversias en el comercio electrónico son atendidas por la Superintendencia de Industria y Comercio (Ley 1480 de 2011).

Para la Comisión de Regulación de Comunicaciones-CRC- (2017) el comercio electrónico se refiere a las actividades empresariales que se realizan a través de medios electrónicos, donde las empresas interactúan y llevan a cabo transacciones tanto con sus

clientes como entre sí, e incluso con entidades administrativas. Abarca desde la realización de pedidos y pagos electrónicos en línea de productos que luego son enviados por correo o servicios de mensajería, hasta la provisión en línea de servicios como publicaciones, software e información.

Por otro lado, Hernández y Hernández (2021) señalan que el comercio electrónico es un tipo de transacción comercial que se realiza mediante uno o varios medios electrónicos, tales como computadoras, tablets, teléfonos celulares, relojes, gafas inteligentes o televisores, con conexión a internet (p. 13). Según los autores, el crecimiento del comercio electrónico ha representado tanto progreso como dudas y retos para llevarlo a cabo.

Teniendo en cuenta el desarrollo progresivo del comercio electrónico, el ordenamiento jurídico colombiano ha ampliado su regulación con el fin de proteger, especialmente, al consumidor. Los documentos CONPES 3701 (Consejo Nacional de Política Económica y Social-CONPES-, 2011), 3854 (CONPES, 2016) y 3995 (CONPES, 2019) abordan acciones de ciberseguridad y ciberdefensa, establecen medidas de protección de pagos en el comercio electrónico y se crean estrategias de seguridad digital para generar confianza en la comercialización de bienes y servicios electrónicamente.

A pesar de los intentos por regular las actividades que se llevan a cabo en el comercio electrónico, el Observatorio eCommerce del MinTIc (2021) afirma que la reglamentación del comercio electrónico aún es muy dispersa, por lo que se hace necesario integrar ese marco normativo para reforzar la protección de los consumidores, especialmente, al momento de hacer pagos en línea.

Ante la dispersión normativa y de datos sobre el comercio electrónico en el sector público, se creó la Cámara Colombiana de Comercio Electrónico-CCCE-. Se trata de una entidad gremial, privada y sin ánimo de lucro que busca promover y fortalecer el comercio electrónico por medio de la centralización de datos sobre el comportamiento de este tipo de comercio en Colombia, e incidiendo en políticas públicas (CCCE, s.f).

De acuerdo con Castiblanco (2022) la CCCE evidenció un crecimiento del 26,6% en las transacciones en línea en Colombia. La entidad halló que las ventas en línea, solo en el primer trimestre del 2022, alcanzaron los 82,7 millones de transacciones, lo que

representó alrededor de 14 billones de pesos. Además, identificó que los sectores con mayor movimiento en el comercio electrónico fueron: otros servicios como arquitectura y contabilidad, servicios financieros y tecnología, deporte, moda y belleza.

Además de los informes trimestrales, la CCCE brinda perspectivas sobre el comercio electrónico en el país para impulsar acciones públicas que promuevan la confianza y el progreso de este tipo de comercio en el país (CCCE, s.f).

Considerando lo expuesto en este y el apartado anterior, es preciso realizar un abordaje de la relación entre la protección de datos y el comercio electrónico en el sistema jurídico colombiano, teniendo en cuenta que en el desarrollo de este tipo de comercio se tratan grandes cantidades de datos personales de los consumidores.

La protección de datos del consumidor en el comercio electrónico en Colombia

En el comercio electrónico, cuando los usuarios realizar compras, solicitan servicios o descargan aplicaciones en línea se ven en la necesidad de proporcionar y registrar sus datos personales en la plataforma digital. Posteriormente, las empresas almacenan esta información en sus bases de datos para generar un valor adicional a través de su uso, lo que hace necesario que se garantice la protección de estos datos tal y como lo argumenta López (2011).

Según Niño (2022) el valor adicional que obtienen las empresas con el uso de los datos de los consumidores del comercio electrónico es tener un acercamiento asertivo hacia ellos, puesto que conocen sus intereses y necesidades. Las organizaciones, a partir de los datos que les proveen los consumidores, pueden crear perfiles para capturar la atención de los usuarios e incentivar la necesidad de compra.

Esto ha llamado la atención de las autoridades y organizaciones internacionales y nacionales, especialmente porque, una vez ingresados en la red, el manejo y control de los datos deja de estar al alcance del titular, así que se ignora el uso que puedan hacer las empresas de esta información (Monsalve, 2017).

Para el Observatorio eCommerce (2019), uno de los pilares fundamentales del comercio electrónico son los datos personales del consumidor, puesto que con ellos se hace posible que las empresas detecten perfiles de consumo para segmentar el mercado y

estructurar la oferta de sus productos y servicios con mayor eficiencia. Así, la mayor preocupación está en que el uso de los datos de los consumidores por parte de las empresas proveedoras de productos y servicios puede injerir en la autonomía privada de los usuarios (Monsalve, 2017).

En este sentido, se ha hecho necesario recordar que, a pesar de encontrarse en un escenario distinto al físico, en el comercio electrónico el tratamiento de datos se sigue sometiendo a los principios de legalidad, finalidad, libertad, veracidad y claridad, transparencia, acceso y seguridad consagrados en el artículo 4 de la Ley 1581 de 2012 (Monsalve, 2017).

De acuerdo con el CONPES (2016) el desarrollo de actividades económicas en el entorno digital representa incertidumbres y riesgos para los consumidores, los cuales deben ser constantemente gestionados para evitar amenazas y ataques cibernéticos. Esto ha hecho necesaria la creación de normativas como la ley 1273 (2009), la cual establece que el acceso abusivo, la interceptación y la violación de datos personales constituyen delitos que pueden generar multas y penas de prisión.

El panorama en el que los usuarios pierden el control de sus datos en el comercio electrónico genera desconfianza en los consumidores para brindar su información personal y bancaria en las distintas plataformas (CRC, 2017). Por ello, en la Ley 1480 (2011) se adoptan mecanismos de seguridad apropiados y confiables para garantizar la protección de datos del consumidor (Art. 50), así, por ejemplo, de acuerdo con el artículo 52 de esa misma ley, cuando la venta se hace a través de comercio electrónico el proveedor debe tomar medidas eficaces para verificar la edad del consumidor y asegurarse de que si es menor de edad haya autorización de los padres para llevar a cabo la transacción.

Según la Superintendencia de Industria y Comercio (2019) las empresas inmersas en el comercio electrónico deben implementar estrategias de responsabilidad en el tratamiento de datos personales, incorporar la privacidad y ética en sus políticas de tratamiento de datos, garantizar la seguridad de los datos de los consumidores, verificar que los datos fueron obtenidos de forma lícita y que puede usarlos para las actividades implicadas en el comercio electrónico.

Además, deben recolectar solo los datos necesarios para los fines del comercio electrónico, no contactar a los usuarios que no quieren recibir más publicidad y suprimir sus datos cuando ellos lo soliciten, usar los datos en días y horas que no afecten la tranquilidad de los usuarios. Todo ello, con el fin de incrementar la confianza y la transparencia con los clientes titulares de los datos personales (Superintendencia de Industria y Comercio, 2019).

La Superintendencia de Industria y Comercio (2019) recalca que el tratamiento de datos en el comercio electrónico debe obedecer a la Ley 1581 de 2012 y el Decreto 1377 de 2013. En ese marco normativo, las organizaciones deben conservar evidencia de haber informado clara y expresamente a los titulares sobre lo dispuesto en el artículo 12 de la Ley 1581 de 2012, así como proporcionar copias de dicha información cuando sea requerido por el titular.

Asimismo, deben solicitar y mantener registros de las autorizaciones otorgadas por los titulares en las condiciones estipuladas por la ley (Art. 17, Ley 1581, 2012). Adicionalmente, es crucial que se proporcione una descripción detallada de los procedimientos utilizados para la recolección, almacenamiento, uso, circulación y eliminación de datos personales, junto con una explicación sobre la necesidad de recopilar dichos datos en cada caso (Art. 4, Decreto 1377, 2013).

Además, se debe documentar adecuadamente los procedimientos relativos al tratamiento, conservación y eliminación de los datos personales de acuerdo con las disposiciones pertinentes, y se deben establecer políticas de tratamiento de datos y asegurar que los encargados del tratamiento cumplan con ellas (Art. 13, Decreto 1377, 2013).

Finalmente, se debe mantener el modelo del Aviso de Privacidad utilizado para informar a los titulares sobre las políticas de tratamiento de datos mientras se traten datos personales según dicho modelo y subsistan las obligaciones correspondientes, y se deben tomar medidas razonables para garantizar la precisión y suficiencia de los datos personales en las bases de datos, incluyendo su actualización, rectificación o supresión cuando así lo solicite el titular o sea necesario según lo detectado por el responsable del tratamiento (Arts. 16 y 20, Decreto 1377, 2013).

En ese sentido, el tratamiento y protección de datos en el comercio electrónico no cuenta con normativa específica, sino que se remite a las disposiciones generales de habeas data como una forma de mitigar los riesgos y la desconfianza que se puede generar en los consumidores. No obstante, esa falta de regulación específica conlleva que las personas que brindan sus datos personales en el comercio electrónico, por la forma en que se pierde el control sobre ellos, se encuentren en una situación de asimetría respecto a las entidades públicas y privadas que recolectan, agregan y explotan su información (CONPES, 2018).

En este contexto, a pesar de la remisión a normas generales de tratamiento de datos, aún subsisten retos jurídicos para asegurar la protección de la información personal que suministran los consumidores del comercio electrónico a entidades públicas y privadas de Colombia. Por ello, en el siguiente apartado se exponen algunos de los retos que se han identificado desde la doctrina y académicos para dar luz a nuevas acciones y normas que amplíen la protección de los datos en el comercio electrónico colombiano.

Desafíos jurídicos del comercio electrónico y la protección de datos en Colombia en 2023

Como ya se mencionó en el capítulo anterior, a pesar de que el marco jurídico colombiano se adapta de forma general a la protección de datos en el comercio electrónico, según autores como Monsalve (2017) se hace necesario crear e implementar una regulación específica para asegurar la correcta aplicación y amplias garantías para los consumidores del comercio electrónico tratándose de la protección de sus datos.

Para Ayala et al. (2020) es importante que el legislador colombiano reflexione sobre la seguridad y confidencialidad de los datos, y la privacidad y la integridad personal en el tratamiento de los datos en el contexto de la cuarta revolución industrial y las nuevas tecnologías, teniendo en cuenta que se pueden dar diversas afectaciones a las garantías fundamentales en el uso de la tecnología, por ejemplo, en el comercio electrónico.

Además de esto, Monsalve (2017) defiende la idea de que los consumidores se informe y conozcan sobre sus derechos y deberes en cuanto a sus datos personales. Para ello, es necesario que se fomente una cultura de protección como política de Estado, en la que se promueva que los ciudadanos sean cautelosos al momento de exponer sus datos

personales en la red. También, el Estado debe vigilar que las organizaciones cumplan con los fines del comercio electrónico para el uso de datos de acuerdo con la normativa vigente.

En ese mismo sentido, Flórez y Camelo (2023) señalan que la regulación colombiana actual de tratamiento y protección de datos no es suficiente para enfrentar los retos de la tecnología, ya que no es claro si la normativa existente, al momento de ser aplicada, cuenta con las herramientas suficientes para hacerse cumplir o sancionar a las empresas que las incumplan. Pese a los esfuerzos del legislador colombiano por adoptar directrices españolas y de la Unión Europea en materia de tratamiento de datos, no se han cubierto todos los aspectos necesarios considerando la era digital, por eso, el reto está en construir una normativa que brinde mayores garantías (Ayala, 2020).

De acuerdo con Gómez et al. (2020), en Colombia, es necesario fortalecer el régimen de protección de datos, lo cual se puede lograr creando una autoridad autónoma e independiente para esta materia, se deben diseñar herramientas tecnológicas y nuevos modelos para el control del tratamiento de datos teniendo en cuenta, no solo los intereses del mercado, sino también los derechos humanos.

Es importante que las empresas consideren que el mal manejo de los datos personales de los consumidores del comercio electrónico no solo puede derivar en reclamos y sanciones por parte de la Superintendencia de Industria y Comercio, sino que puede implicar daño económico, social y reputacional para la compañía y toda la industria. En esa línea, las organizaciones que llevan a cabo el comercio electrónico están llamadas a tener mecanismos jurídicos para prevenir fraudes, delitos informáticos y, en general, mal uso de los datos personales de sus clientes, para generar mayor confianza y asegurar el crecimiento de las transacciones y negocios en línea (Niño, 2022).

Si bien existe una regulación general de habeas data que pretende ser aplicable a las diversas situaciones que se presentan en el comercio electrónico, existe el desafío para el Estado y las autoridades de hacer aplicables estas normas por medio de mecanismos más robustos, que le recuerden a las compañías su obligación de proteger los derechos de los consumidores del comercio electrónico sobre sus datos personales.

Uno de los principales desafíos radica, entonces, en la adaptación de las regulaciones existentes a la dinámica y complejidad del comercio electrónico moderno. Las

normas actuales pueden no abordar adecuadamente las nuevas formas de recopilación y uso de datos, como el seguimiento en línea y la segmentación de audiencia, que son prácticas comunes en la era digital (Gómez et al., 2020). Esto crea lagunas en la protección de la privacidad y la seguridad de los usuarios en línea.

Además, la necesidad de que las autoridades sean más estrictas en la aplicación de estas normas es fundamental para garantizar la confianza de los consumidores en el comercio electrónico. Los usuarios deben tener la certeza de que sus datos personales están siendo manejados de manera segura y que se respetan sus derechos de privacidad (Flórez y Camelo, 2023). La falta de aplicación rigurosa de las regulaciones puede llevar a prácticas abusivas por parte de algunas empresas que buscan aprovecharse de la información personal de los usuarios sin su consentimiento

La protección de datos es esencial no solo desde una perspectiva de privacidad, sino también desde un punto de vista de seguridad. Los datos personales pueden ser vulnerables a ataques cibernéticos y violaciones de seguridad si no se aplican medidas adecuadas (Arteaga, 2023). Por lo tanto, las autoridades deben asegurarse de que las empresas cumplan con estándares de seguridad cibernética sólidos para proteger la información sensible de los usuarios.

Finalmente, está el desafío de que los usuarios tomen conciencia y se eduquen sobre la importancia de sus datos personales y el riesgo que corren en la red. Muchos consumidores pueden no estar plenamente informados sobre sus derechos en cuanto al manejo de sus datos personales en línea. En ese sentido, las autoridades deben trabajar en la promoción de la educación digital y la concienciación sobre la importancia de la privacidad en línea, así como en la forma en que pueden ejercer sus derechos.

Conclusiones

Este artículo se propuso analizar los desafíos jurídicos del comercio electrónico y la protección de datos para Colombia en 2023. Para ello se abordó los avances jurídicos en la regulación de la protección de datos, del comercio electrónico y de la relación entre los dos.

A partir de los hallazgos se concluye que en el contexto colombiano, la regulación del tratamiento de datos personales ha evolucionado a lo largo del tiempo, desde la Ley

1266 (2008) hasta la Ley Estatutaria 1581 (2012), estableciendo principios fundamentales de transparencia, seguridad y confidencialidad. La Corte Constitucional ha desempeñado un papel crucial al desarrollar reglas jurisprudenciales para proteger los datos personales y promover el habeas data como un derecho fundamental autónomo. A medida que la tecnología avanza y las implicaciones tecnológicas y jurídicas se vuelven más complejas, los retos futuros en la protección del habeas data se centran en la administración de datos por parte de empresas privadas, lo que requiere una revisión y actualización continua de la normativa y la jurisprudencia para garantizar la protección adecuada de los datos personales y la privacidad de los individuos en un entorno digital en constante cambio.

Sobre el comercio electrónico se concluye que ha experimentado un crecimiento significativo en Colombia, sobre todo por la pandemia de COVID-19. A medida que se ha convertido en una parte esencial de la sociedad colombiana, se han implementado regulaciones y leyes, como la Ley 527 de 1999 y la Ley 1480 de 2011, para abordar aspectos legales y la protección del consumidor en este ámbito. La Cámara Colombiana de Comercio Electrónico (CCCE) juega un papel fundamental en la promoción y supervisión del comercio electrónico, proporcionando datos que respaldan el desarrollo de políticas públicas. En este contexto, la relación entre la protección de datos y el comercio electrónico se vuelve esencial en el sistema jurídico colombiano debido al manejo de grandes cantidades de información personal de los consumidores en transacciones en línea.

En cuanto a la protección de datos en el marco del comercio electrónico es posible concluir que a pesar de que se aplican principios legales generales de protección de datos, como los establecidos en la Ley 1581 de 2012, la falta de una regulación específica y la ineficaz aplicación del régimen general de habeas data en el comercio electrónico crea desafíos y asimetrías en la relación entre los consumidores y las entidades que recopilan y explotan sus datos. Estos desafíos destacan la necesidad de nuevas acciones y normativas que fortalezcan la protección de los datos personales en el contexto del comercio electrónico en Colombia.

El comercio electrónico en Colombia enfrenta importantes desafíos legales en materia de protección de datos en el contexto de la era digital y la cuarta revolución industrial. A pesar de contar con un marco jurídico general que aborda la protección de

datos, existe la necesidad apremiante de establecer una regulación específica que garantice una aplicación efectiva y sólidas salvaguardias para los consumidores que confían sus datos personales en el entorno del comercio electrónico. Además, es crucial fomentar una cultura de protección de datos y conciencia entre los ciudadanos, promoviendo el conocimiento de sus derechos y deberes en este ámbito.

El fortalecimiento del régimen de protección de datos, posiblemente a través de la creación de una autoridad independiente especializada en habeas data dentro del comercio electrónico o el fortalecimiento de la Superintendencia de Industria y Comercio, y la adopción de herramientas tecnológicas avanzadas son pasos esenciales para abordar los retos actuales y futuros en la protección de datos en el comercio electrónico colombiano. En última instancia, las empresas que operan en este sector deben reconocer que la gestión adecuada de los datos personales no solo es esencial para el cumplimiento normativo, sino también para mantener la confianza de los consumidores y asegurar el crecimiento sostenible de las transacciones en línea.

Referencias

Arteaga, C. D. (2023). Ciberdelincuencia: a propósito del derecho penal informático en Colombia. *Episteme. Revista De divulgación En Estudios Socioterritoriales, 13*(1), 38–47. https://doi.org/10.15332/27113833.8322

Ayala, J., Ariza, J. y González, L. (2020). La protección de datos en la era digital Colombia - España. Revista Politécnico Grancolombiano. Bogotá, Colombia.

BlackSip. (2019). Blackindex: *El Reporte Del E-Commerce En Colombia 2019*. En BlackSip. https://content.blacksip.com/hubfs/EBOOK BLACKINDEX REPORTE 2019 ECOMMERCE COLOMBIA by BLACKSIP 2.pdf?utm_medium=email&_hsenc=p2ANqtz93sktfI7jZAOtevVhtY5vOQT2h2UuSlgbT5miXVxkxmflLk4-LPBCa7tcqBMWXXmHaNIZdoxGAIYFb78hh1Sfh2aNJid2z5Kv8aPxEPZoTUv5X5o&_hsmi=8

Cámara Colombiana de Comercio Electrónico-CCCE-. (2022). *Informe del comercio electrónico en 2022 y perspectivas 2023.* Cámara Colombiana de Comercio

Electrónico: https://www.ccce.org.co/gestion_gremial/informe-del-comercio-electronico-en-2022-y-perspectivas-2023/

Cámara Colombiana de Comercio Electrónico-CCCE-. (s.f). *¿Qué es la CCCE?* Cámara Colombiana de Comercio Electrónico: https://www.ccce.org.co/ccce/

Castiblanco, M. P. (17 de agosto de 2022). *En el segundo trimestre del 2022, la Cámara Colombiana de Comercio Electrónico reveló el aumento de transacciones de ventas en línea en Colombia a través del Informe de Comportamiento*. Revista P&M: https://www.revistapym.com.co/articulos/digital/53095/camara-colombiana-de-comercio-electronico-26-6-de-aumento-en-ventas-en-linea

Comisión de Regulación de Comunicaciones-CRC-. (2017). *El comercio electrónico en Colombia. Análisis integral y perspectiva regulatoria.* (Documento soporte), CRC: https://www.crcom.gov.co/system/files/Biblioteca%20Virtual/Documento%20soporte/comelecptd_0.pdf

Consejo Nacional de Política Económica y Social (CONPES). (2020). *Documento CONPES 4012 de 30 de noviembre de 2020*. Departamento Nacional de Planeación: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4012.pdf

Consejo Nacional de Política Económica y Social-CONPES-. (2011). *Documento CONPES 3701 de 14 de julio de 2011*. Departamento Nacional de Planeación: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

Consejo Nacional de Política Económica y Social-CONPES-. (2016). *Documento CONPES 3854 de 11 de abril de 2016*. Departamento Nacional de Planeación: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Consejo Nacional de Política Económica y Social-CONPES-. (2018). *Documento CONPES 3920 de 17 de abril de 2018*. Departamento Nacional de Planeación: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf

Consejo Nacional de Política Económica y Social-CONPES-. (2019). *Documento CONPES 3995 de 1 de julio de 2019*. Departamento Nacional de Planeación: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Corte Constitucional. (1992). *Sentencia T-414 de 16 de junio de 1992.* (M. P. Ciro Angarita Baron). https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Corte Constitucional. (1994). *Sentencia T-157 de 24 de marzo de 1994.* (M. P. Hernando Herrera Vergara). https://www.corteconstitucional.gov.co/relatoria/1994/T-157-94.htm

Corte Constitucional. (1995). *Sentencia SU-082 de 1995*. (M. P. Jorge Arango Mejía). https://www.corteconstitucional.gov.co/relatoria/1995/su082-95.htm

Corte Constitucional. (1999). *Sentencia T-307 de 5 de mayo de 1999.* (M. P. Eduardo Cifuentes Muñoz). https://www.corteconstitucional.gov.co/relatoria/1999/T-307-99.htm

Corte Constitucional. (2002). *Sentencia T-729 de 5 de septiembre de 2002.* (M. P. Eduardo Montealegre Lynett). https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

Corte Constitucional. (2008). *Sentencia C-1011 de 16 de octubre de 2008. (M. P. Jaime Córdoba Triviño).* https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm

Corte Constitucional. (2011). *Sentencia C-748 de 6 de octubre de 2011.* (M. P. Jorge Ignacio Pretelt Chaljub). https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Corte Constitucional. (2012). *Sentencia C-540 de 12 de julio de 2012.* (M. P. Jorge Iván Palacio Palacio). https://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm

Corte Constitucional. (2015*). Sentencia T-058 de 12 de febrero de 2015*. (M. P. Luis Guillermo Guerrero Pérez). https://www.corteconstitucional.gov.co/relatoria/2015/T-058-15.htm

Corte Constitucional. (2018). *Sentencia T-238 de 26 de junio de 2018*. (M. P. Gloria Stella Ortiz Delgado). https://www.corteconstitucional.gov.co/relatoria/2018/T-238-18.htm

Corte Constitucional. (2020*). Sentencia T-509 de 9 de diciembre de 2020*. (M. P. José Fernando Reyes Cuartas). https://www.corteconstitucional.gov.co/relatoria/2020/T-509-20.htm

Corte Constitucional. (2021). Sentencia SU-139 de 14 de mayo de 2021. (M. P. Jorge Enrique Ibañez Najar). https://www.corteconstitucional.gov.co/relatoria/2021/SU139-21.htm

Corte Constitucional. (2022a*). Sentencia C-406 de 17 de noviembre de 2022*. (M. P. Cristina Pardo Schlesinger). https://www.corteconstitucional.gov.co/relatoria/2022/C-406-22.htm

Corte Constitucional. (2022b). Sentencia SU-086 de 9 de marzo de 2022. (M. P. Cristina Pardo Schlesinger). https://www.corteconstitucional.gov.co/relatoria/2022/SU086-22.htm

Decreto 1377 de 2013. (2013). *Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015*. Diario Oficial 48834 de junio 27 de 2013.

Devis, J.; Gómez, M. P. y López, E. (2019). Obligación de información y asimetrías de información en el mercado bancario colombiano. *Revista de Economía Institucional, 21* (41), 162-182. https://doi.org/10.18601/01245996.v21n41.07

Escudero, A. (2018). Redefinición del "aprendizaje en red" en la cuarta revolución industrial. *Apertura, 10* (1). https://doi.org/10.32870/ap.v10n1.1140

Flórez, M. L. y Camelo, A. M. (2023). Tecnologías de reconocimiento facial en Colombia: Análisis comparativo en relación con la protección de datos. *Ius et Praxis, 29* (1). http://dx.doi.org/10.4067/S0718-00122023000100003

García, R., Caldas, J. Dávila, D. y Thoene, U. (2020). Políticas públicas de inclusión digital en Colombia. Una evaluación del Plan Vive Digital I (2010-2014). *Revista Espacios, 41* (7). https://www.revistaespacios.com/a20v41n07/20410713.html

Gil, J. C. (2017). El debido proceso en la Ley de Habeas Data. *Revista CES Derecho, 8* (1). 191-204. http://www.scielo.org.co/scielo.php?pid=S2145-77192017000100011&script=sci_arttext

Gómez, A.; Arévalo, S.; Bernal, D. y Rosero, D. (2020) El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho*, (20), 272-294. https://scielo.isciii.es/scielo.php?pid=S1886-58872020000300017&script=sci_arttext

Hernández, R. (2018). *Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.

Hernández, E. M. y Hernández, L. C. (2021). *Manual de comercio electrónico*. ECOE Ediciones.

Hootsuite, & We Are Social. (2020). Digital 2020: Colombia — DataReportal. Datareportal.com: https://datareportal.com/reports/digital-2020-colombia?rq=colombia

Knight, G. y Liesch, P. (2016). Internationalization: from incremental to born global. *Journal of World Business, 51* (1). 93-102.

Ley 1231 de 2008. (2008). *Por la cual se unifica la factura como título valor como mecanismo de financiación para el micro, pequeño y mediano empresario, y se dictan otras disposiciones*. Diario Oficial No. 47.053 de 17 de julio de 2008.

Ley 1273 de 2009. (2009). *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.* Diario Oficial No. 47.223 de 5 de enero de 2009.

Ley 1480 de 2011. (2011). *Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones.* Diario Oficial No. 48.220 de 12 de octubre de 2011

Ley 527 de 1999. (1999). *Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.* Diario Oficial No. 43.673, de 21 de agosto de 1999.

Ley Estatutaria 1581 de 2012. (2012). *Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587 de 18 de octubre de 2012.

Limas, S. J. (2020). El comercio electrónico (e-commerce) un aliado estratégico para las empresas en Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (34). 235-251. https://media.proquest.com/media/hms/PFT/1/DPfNH?_s=dUUCiOsO60vMwKUELDnlCmqY1x0%3D

López, D. (2011). Los códigos de conducta como solución idónea frente a la elevada desprotección de la privacidad en Internet. *Revista de Derecho Comunicaciones y Nuevas Tecnologías,* (6), 4-21. https://dialnet.unirioja.es/servlet/articulo?codigo=3809310

Martínez, R., Palma, A., & Velásquez, A. (2020). *Revolución tecnológica e inclusión social: reflexiones sobre desafíos y oportunidades para la política social en América Latina.* [Serie Políticas Sociales, N° 233]. Comisión Económica para América Latina y el Caribe (CEPAL). (LC/TS.2020/88). https://www.cepal.org/sites/default/files/publication/files/45901/S2000401_es.pdf

Mejía, M., Hurtado, S. V., y Grisales, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista De Ciencias Sociales, XXIX* (2), 356-372.

Ministerio de Tecnologías de la Información y las Comunicaciones-MinTIC- (2022). Índice de brecha digital regional. Resultados 2021. MinTIC: https://colombiatic.mintic.gov.co/679/articles-238353_recurso_1.pdf

Monsalve, V. (2017). La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. *Revista Prolegómenos Derechos y Valores, 20 (*39), 163-195. DOI: http://dx.doi.org/10.18359/prole.2729

Moreno, M. P. (2014). Comercio electrónico y su impacto en la globalización. *Observatorio de la economía latinoamericana, 201,* 1-12.

Newman, V. (2015). *Datos personales e información pública: oscuridad en lo privado luz en lo público*. Centro de Estudios de Derecho, Justicia y Sociedad.

Niño, D. Y. (2022). Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico. *Revista CES Derecho, 13* (1). https://doi.org/10.21615/cesder.6386

Observatorio eCommerce. (2019). *Prospectiva para el comercio electrónico en Colombia.* MinTic: https://www.ccce.org.co/wp-content/uploads/2017/06/Prospectiva-eCommerce-Observatorio-CCCE.pdf

Observatorio eCommerce. (2021). Análisis Normativo del Comercio Electrónico en Colombia, investigación. MinTic: https://observatorioecommerce.mintic.gov.co/797/articles-198739_recurso_1.pdf

Ragnedda, M. (2017). *The Third Digital Divide: A Weberian Approach to Digital Inequalities*. New York: Routledge

Ramírez, E. M. (2021). *¿Qué pasó con el comercio electrónico en 2021?* Cámara Colombiana de Comercio Electrónico: https://www.ccce.org.co/noticias/que-paso-con-el-comercio-electronico-en-2021/

Rose, G. (2016). *The Fourth Industrial Revolution: A Davos reader*. Council on Foreign Relations.

Superintendencia de Industria y Comercio. (2019). *Guía sobre el tratamiento de datos personales para fines de comercio electrónico.* Superintendencia de Industria y Comercio-SIC-: https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf