LA FRAGMENTACIÓN NORMATIVA EN LA PROTECCIÓN DE DATOS EN EL COMERCIO ELECTRÓNICO COLOMBIANO

REGULATORY GAPS IN DATA PROTECTION FOR E-COMMERCE IN COLOMBIA

DOI: https://doi.org/10.17981/juridcuc.21.1.2025.11

Fecha de Recepción: 2025/03/25 Fecha de Aceptación: 2025/08/05

Manuel Antonio Pérez Vásquez
Universidad del Sinú-Elías Bechara Zainúm, Colombia
manuelperezv@unisinu.edu.co

Para citar este articulo:
Pérez, M. (2025). La fragmentación normativa en la protección de datos en el comercio electrónico colombiano. *Jurídicas CUC, 21*(1), pp. 213 - 231. DOI: http://doi.org/10.17981/juridcuc.21.1.2025.11

Resumen

En este artículo se centra en la fragmentación en las normativas sobre la protección de datos personales en el comercio electrónico. Mediante un enfoque cualitativo basado en la revisión de documentos, se reconocen graves deficiencias legales, así como grandes problemas en su implementación y regulación. Se determinó que la ausencia de una regulación particular para el comercio electrónico en el país perjudica la protección de datos, e impacta sobre la confianza del consumidor, restringiendo así el avance del ecosistema digital. Este articulo coloca en clara evidencia que en Colombia persiste una fragmentación normativa en la protección de datos personales, especialmente en el comercio electrónico, lo cual genera inseguridad jurídica ya que las leyes actuales están desarticuladas, lo cual limita su capacidad de control de la SIC, socavando aún más la confianza del consumidor y la competitividad digital. Se confirma que la falta de regulación específica obstaculiza la adaptación empresarial y la inserción internacional. Como conclusión central, se propone un sistema integral que modernice la legislación, refuerce la supervisión y promueva un entorno digital seguro e innovador.

Palabras clave: Comercio electrónico, legislación, protección de datos, seguridad informática.

Abstract

This article focuses on the fragmentation of regulations on personal data protection in e-commerce. Using a qualitative approach based on document review, serious legal deficiencies are identified, as well as major problems in their implementation and regulation. It was determined that the absence of specific rules for e-commerce in the country undermines data protection and impacts consumer confidence, thereby restricting the advancement of the digital ecosystem. This article clearly shows that Colombia continues to suffer from regulatory fragmentation in the protection of personal data, especially in e-commerce, which creates legal uncertainty as current laws are disjointed, limiting the SIC's ability to enforce them and further undermining consumer confidence and digital competitiveness. It is confirmed that the lack of specific regulation hinders business adaptation and international integration. As a central conclusion, a comprehensive system is proposed to modernize legislation, strengthen supervision, and promote a secure and innovative digital environment.

Keywords: E-commerce, legislation, data protection, IT security.

INTRODUCCIÓN

El comercio internacional ha estado históricamente vinculado al intercambio de información, hechos como la difusión de la cultura, el conocimiento hasta la gestión de documentos como facturas, certificados de aduana y contratos. Ha representado un salto ampliado para las operaciones comerciales fueras de las fronteras nacionales, estos intercambios han hecho que las operaciones globales hayan evolucionado considerablemente, y como consecuencia, el flujo constante de información a través de esas fronteras ha causado un crecimiento exponencial positivo, ya que ha acercado al hombre más a las nuevas tecnologías de la información, generando consigo un estallido crucial para el aumento de las operaciones comerciales, no obstante, este crecimiento ha generado desafíos regulatorios más desafiantes, ya que los países a nivel global pasan por un proceso de transición hacia nuevos modelos de gobierno, lo que dificulta y deja poca claridad acerca de las restricciones sobre cantidades y el almacenamiento de datos.

A pesar de los avances en la legislación de protección de datos en muchos países, la falta de uniformidad en las regulaciones sigue siendo un obstáculo que complica la interoperabilidad a nivel global. En el caso particular de Colombia, el comercio electrónico ha tenido un notable crecimiento en los últimos años, todo ello impulsado por la digitalización de la economía y el aumento del acceso a Internet (Lund y Tyson, 2017). No obstante, el desarrollo de este campo se ha visto frenado por los constantes retos de carácter regulatorios, y aún más en lo concerniente con la protección de datos personales, este articulo defiende la hipótesis de que la falta de regulación específica sobre el comercio electrónico en Colombia genera mucha inseguridad jurídica, lo que causa efectos negativos en el comercio digital y sobre la confianza del consumidor.

DESARROLLO

METODOLOGÍA

En este artículo se propone un análisis jurídico exhaustivo sobre la protección de los datos personales en el comercio electrónico colombiano. la investigación, de enfoque cualitativo, utilizo una metodología documental y analítica, para así llevar a cabo una evaluación crítica y muy detallada de la permanente desarticulación normativa que existe en este campo. Este análisis permitió identificar vacíos legales, lo que demuestra que los desafíos frente a la protección de datos en Colombia son bastante amplios. Por otro lado, se analizó los efectos adversos sobre la fragmentación regulatoria, lo cual evidencio una base normativa indeleble, sobre la cual crear unos cimientos sólidos sobre la protección de los datos personales en el país. Para llevar a cabo esta investigación, se recopilo una gran cantidad de información relevante, se comparó y analizo la normativa nacional, los acuerdos internacionales acerca de la protección de datos, y los textos con un carácter especializado tanto en el derecho digital como en el comercio electrónico, y una serie de informes por parte de los organismos gubernamentales y (ONG).

El propósito de la investigación se centra principalmente en explorar las inconsistencia jurídicas encontradas en la normativa colombiana, relacionadas con la protección de datos en el ámbito del comercio electrónico, inicialmente se realizó un abordaje de

estas inconsistencias en aras de determinar el impacto sobre la competitividad de las empresas colombianas, que se dedican a realizar operaciones comerciales en el ámbito global y digital, todo ello con el fin de determinar cómo los derechos y la protección del consumidor puede proteger las transacciones que se realizan en línea, esta investigación se justifica en la ausencia de un marco normativo legal integral y coherente en Colombia que aborde de manera más precisa la protección de los datos personales en el escenario del comercio internacional. Por otra parte, se realizó una comparación de la situación actual colombiana con diferentes normativas internacionales como referencia, tuvimos presente el Reglamento General de Protección de Datos (GDPR) del Mercado Común Europeo, con el objetivo de hacer un análisis detallado para identificar posibles áreas de mejora y en la no prevalencia de inconsistencias futuras, ayudando con esto a que el flujo real de la información, sea más constante y segura, todo esto se ha logrado a través, de un análisis jurisprudencial profundo, con el fin, de acercar más el escenario normativo global a una normativa más ajustada a lo local. Este hecho permitirá mejorar los niveles de confianza de los consumidores e incrementará la buena imagen de las empresas colombianas fuera de las fronteras nacionales.

RESULTADOS - DISCUSIÓN

Marco normativo sobre la protección de datos personales a nivel global

En el año 2022, las transacciones realizadas por medios digitales sobrepasaron los cinco billones de dólares, consolidándose como un componente fundamental dentro de la economía mundial. Como es de esperarse en un cambio paradigmático, el crecimiento constante ha representado un desafío enorme en los aspectos regulatorios, en especial porque el tema de la protección de datos sigue siendo un tema susceptible a ojos de muchos, y en especial por sus implicancias alrededor de la protección y la privacidad de estos, ámbitos donde las leyes actuales no han logrado mantenerse al ritmo acelerado de la innovación tecnológica (Syafta et al., 2022).

Esta situación ha traído consigo un mayor desafió para los entes reguladores en las operaciones internacionales, logrando con ello un aumento desmesurado en los costos de la cadena logística y, sobre la mano de obra, hechos que han repercutido de manera negativa en la competitividad de las empresas locales. Por otro lado, las restricciones impuestas en el comercio internacional de datos han ido aumentando, gracias a la falta de claridad sobre una legislación clara y eficiente en dirimir conflictos—al existir vacíos y vicios normativos motivadas por inquietudes relativas a la seguridad y la privacidad—cada una de estas exenciones han perpetuado un desarrollo mayor del comercio electrónico, este escenario ha propiciado nuevas dinámicas frente a la obligación de almacenar y salvaguardar la información dentro de las fronteras nacionales, con lo cual se ha creado un obstáculo frente a la interoperabilidad digital. Este panorama ha afectado tanto los procesos de innovación como el crecimiento económico a escala más global, esto deja en evidencia la necesidad urgente de modernizar los marcos legales tradicionales y adaptarlos a los retos de la era digital.

En relación con lo anterior, expertos alrededor del mundo han dejado de manifiesto que las normativas en las que convergen la localización de datos, aunque buscan atender preocupaciones legítimas, se han convertido en barreras no arancelarias para la expansión del comercio digital, este hecho ha limitado la colaboración transfronteriza y el crecimiento económico y va en contraposición con la (OMC) respecto a la apertura de las fronteras comerciales. En suma, la información se ha transformado en uno de los recursos intangibles y comerciales más valiosos del planeta, por lo que se hace manifiesto una actualización de nuestros instrumentos normativos em aras de garantizar un equilibrio entre seguridad, desarrollo tecnológico y libre circulación de datos. Sumado a esto, Azmeh et al. (2020) nos habla acerca de la importancia significativa de salvaguardar la soberanía de los datos y de propiciar una integración internacional en este campo.

No obstante, como lo indican Ferencz y Gonzales (2019), existen unas barreras regulatorias que limitan el libre flujo de datos lo que podría amenazar esta integración. Según Ayunda (2022), la poca ausencia frente a un marco legal fuerte ha generado muchos vacíos en la regulación y una significante inseguridad jurídica, lo cual afecta considerablemente a los usuarios. En esa dirección, Hassan (2012) expone que muchos países en la región de Latinoamérica enfrentan problemas de salvaguarda de datos, lo cual contrasta con el modelo europeo establecido a través del Reglamento General de Protección de Datos (GDPR), que se ha convertido en un referente a nivel internacional en este ámbito.

El RGPD no solo establece un conjunto de principios fundamentales —como la limitación de datos, la disminución de multas, la responsabilidad y la seguridad desde su diseño—, sino que además determina una responsabilidad activa a quienes manejan datos para asegurar el cumplimiento de estas directrices (Goddard, 2017; Hoofnagle, Van der Sloot y Borgesius, 2019). Este marco normativo posiciona a la Unión Europea como líder en la defensa de datos personales, a diferencia de otras naciones que aún están desarrollando proyectos de ley orientados hacia esa dirección, y en donde son notables las falencias estructurales que demuestran la discrepancia normativa entre el hemisferio norte y el sur.

Teniendo en cuenta el planteamiento anterior, Ayunda (2022) incorpora un modelo teórico sustentado en la teoría del derecho responsivo, el cual aboga por una evolución de las leyes a la par de los cambios sociales y tecnológicos. Lo cual va en contraposición del legalismo liberal, que se caracteriza por una rigidez estricta frente a la separación institucional, el enfoque responsivo es claro ya que defiende la construcción de marcos normativos más flexibles, con mayor poder de adaptación y capaces de acoplarse a contextos específicos, en pro de impulsar fines sociales relevantes. Desde hace algunos años esta perspectiva ha cobrado especial trascendencia en campos complejos como el Big Data, donde la vasta y automatizada recolección de información personal puede intensificar desigualdades y riesgos de exclusión social (Wachter et al., 2017).

Por su parte, Ayunda (2022) nuevamente hace alusión sobre el valor económico del Big Data ya que exige una atención rigurosa frente a sus implicaciones éticas, sociales y legales, es por esto por lo que advierte sobre las graves consecuencias que puede acarrear su uso desmedido y sin controles adecuados. Para Bieker et al. (2016) las evidencias sobre la aplicación de inteligencia artificial en la gestión de datos pueden

perpetuar sesgos o excluir a determinados colectivos si no se establecen reglas claras que promuevan la equidad y la supervisión democrática. Es por esto por lo que resulta fundamental que las políticas de protección de datos vayan más allá y trasciendan de la simple salvaguarda de la privacidad individual, la integración de principios de justicia algorítmica, transparencia tecnológica y responsabilidad social en su formulación.

Desde una óptica integral de los derechos humanos, la salvaguarda de la información personal recientemente ha venido experimentando una atención desmedida, ya que esta empezó a verse y entenderse como una extensión legítima del derecho a la privacidad, a la dignidad y al control sobre los datos propios. En este sentido, Hisbulloh (2021) manifiesta que la ausencia de una regulación clara y eficaz en materia de protección de datos no solo revela falencias en la gestión administrativa, sino que también evidencia un incumplimiento del Estado en su obligación de garantizar derechos fundamentales. Es por ello por lo que se hizo necesario, el Proyecto de Ley de Protección de Datos Personales, el cual debe ser concebido no solo como una cuestión de tecnicismos, sino más bien, como una cuestión de responsabilidades constitucionales orientadas a un fortalecimiento de la función estatal en la defensa efectiva de los ciudadanos en el ámbito de la protección digital.

Precisando un poco la percepción anterior, la heterogeneidad en los enfoques regulatorios adoptados por distintos países es cada vez mayor, lo que nos deja ver un panorama un poco incierto, ya —que oscilan entre la no intervención y la concesión de permisos específicos— generando un entorno normativo fragmentado que dificulta la armonización global, lo cual dificulta y aumenta la inseguridad jurídica en el comercio digital (López et al., 2022; Ferracane y van der Marel, 2021). En respuesta a esta problemática, se han desarrollado iniciativas internacionales, pero estas aún son escasas frente a la demanda constante y a la dinámica misma del crecimiento exponencial de los países, recientemente se empezó la implementación de las Reglas de Privacidad Transfronteriza de APEC y las recomendaciones de la OCDE, que buscan promover la alineación normativa entre naciones (OECD, 2022; UNCTAD, 2021). No obstante, en países emergentes como Colombia existen muchas limitaciones técnicas y normativas, al igual que en otros sectores como el de infraestructura que obstaculizan la implementación efectiva de estas regulaciones (CIGI, IPSOS, ISOC y UNCTAD, 2019).

Es importante considerar, que el comercio electrónico aún se encuentra en unas etapas bastante tempranas ya que este debe contar con garantías más ajustadas a la realidad del país y que sean equivalentes a las normas tradicionales del comercio internacional, velando que la privacidad de los consumidores frente a las transacciones digitales sean cada vez más seguras, en aras de salvaguardar la protección del consumidor, estas condiciones esenciales para fomentar la confianza y el desarrollo sostenible del mercado en línea (OECD, 2016; UNCTAD, 2023). Son fundamentales ya que no existe un marco regulatorio apropiado, que permita disminuir la desconfianza por parte de los usuarios y, a la vez, su participación en las plataformas digitales (UNCTAD, 2022).

A nivel de bloques comerciales, la unión europea ha logrado avances significativos, implementando Leyes como la ley de Servicios Digitales (DSA) y la Ley de Mercados Digitales (DMA), lo cual significa un avance sin precedentes, para otros países como Estados Unidos, existe una ausencia de una legislación federal armonizada, este hecho,

deja espacios vacíos y vicios de ley confederadas en la regulación (Pashynskyi, 2023; Tovino, 2020). Por otro lado, la prevalencia de grandes plataformas digitales ha causado muchas preocupaciones, sobre la manera en que estas gestionan los datos y el efecto negativo que este puede representar para los consumidores, ya que los competidores, específicamente pueden discrepar en la determinación de precios, lo cual alteraría los resultados en los motores de búsqueda, debido a que tales aspectos afectan directamente la privacidad y la competencia justa (Karim et al., 2022; Ayunda, 2022; Tikkinen-Piri et al., 2018).

En este contexto, tecnologías como la IA y los algoritmos de fijación de precios han complicado la aplicación de las leyes tradicionales que regulan la competencia y protegen a los consumidores (Syafta et al., 2022). Es por ello por lo que, en el manejo de las plataformas digitales, se pudo ver la necesidad de establecer de manera urgente regulaciones más eficientes que se ajustaran a las necesidades de los consumidores (Karim et al., 2022; Ayunda, 2022). Recientemente el bloque económico de la U.E ha asumido un papel bastante proactivo frente a la lucha contra un sinnúmero de abusos que no contaban con una regulación clara, logrando enfatizar en la urgencia de mejorar y adaptar la normatividad vigente, en aras de responder efectivamente a los retos que plantea el entorno digital contemporáneo (Syafta et al., 2022).

Siguiendo el hilo conductor anterior se hace prescindible destacar que la ausencia de la interrelación con las personas en las transacciones en línea aumenta el riesgo de fraudes electrónicos, esto ha creado un escenario importante ya que, se logró la inclusión de la responsabilidad del producto y métodos alternativos de resolución de disputas (ADR/ODR), lo cual había sido una necesidad imperante desde hacía mucho tiempo, con estos instrumentos creados como fundamentos para mejorar la protección de los consumidores en el ámbito digital (Abdulrauf y Fombad, 2016; Syafta et al., 2022). Existiendo estos parámetros la claridad de la información paso a ser un eje central, logrando así que los consumidores reciban datos verídicos y completos sobre los productos, precios y condiciones de servicio, aunque las variaciones entre distintas jurisdicciones complican su aplicación uniforme (Abdulrauf y Fombad, 2016).

Desafíos regulatorios en la protección de datos personales a nivel internacional

Las últimas estadísticas evidencian un aumento en la preocupación mundial acerca de la protección de información personal en el comercio en línea. Según Husain (2024), el 73 % de los consumidores se muestra más preocupado por su privacidad en línea que en el pasado, y el 67 % considera que los gobiernos deberían asumir un papel más activo en la protección de datos personales. A pesar de ello, un 66 % cree que la responsabilidad recae sobre el propio usuario. Se proyecta que, para finales del año 2024, el 75 % de la población mundial estará cubierta por normativas de privacidad (Husain, 2024).

En cuanto al uso de redes sociales, un 38 % de los usuarios ha reducido su uso y un 36 % ha eliminado cuentas debido a preocupaciones sobre privacidad; además, el 89 % muestra inquietud por la recolección de datos de menores. La confianza en línea también se ve afectada: el 87 % no haría negocios con empresas que no protejan sus datos y el 71 % dejaría de hacerlo si estos se comparten sin consentimiento. Frente

al avance de la inteligencia artificial, el 70 % desconfía de su uso por parte de las empresas y el 81 % teme usos inesperados de su información, mientras que el 91 % de las organizaciones reconoce la necesidad de ser más transparentes. A pesar de este panorama, más del 70 % de los profesionales señala que gestionar adecuadamente la privacidad aporta beneficios empresariales, como la eficiencia operativa, la confianza del cliente y la reducción de pérdidas, lo que demuestra que la protección de datos no solo es una obligación ética, sino también una ventaja competitiva para las organizaciones (Husain, 2024). La siguiente figura indica el porcentaje de poblacional a nivel mundial protegido por normas de privacidad (2020 y 2024).

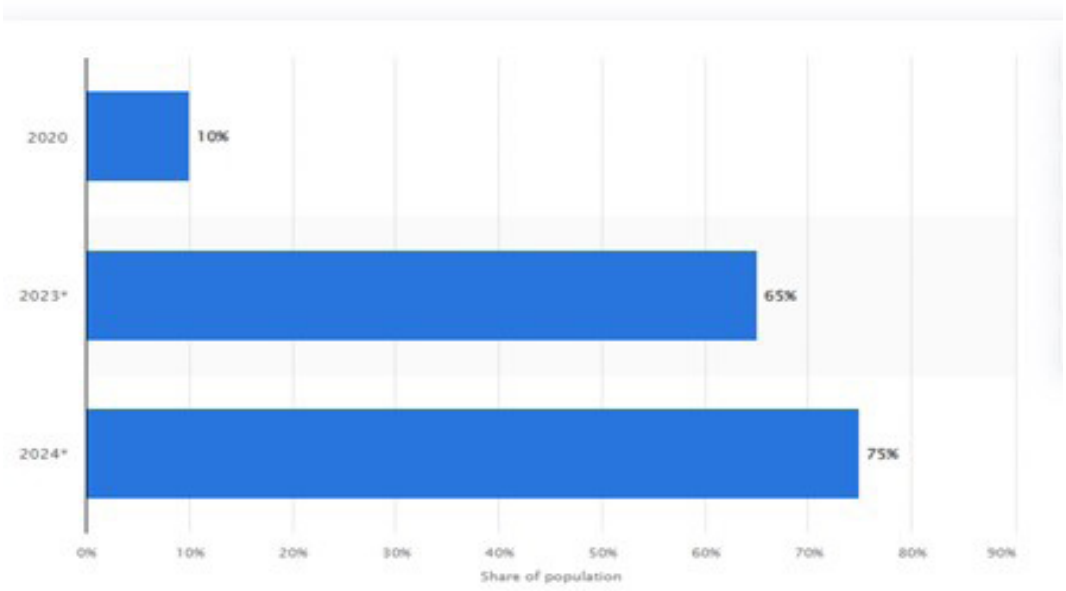

Figura 1. Población mundial con datos personales cubiertos por la normativa de privacidad 2020-2024
Nota: Statista 2025, adaptado de Petrosyan (2024).

Según la figura, existe una clara tendencia al alza en la protección de la población mundial bajo normas de privacidad. En el año 2020, solo el 10 % de la población estaba cubierta por regulaciones de privacidad, lo que indica que en ese momento la mayoría de los países aún no contaban con marcos normativos sólidos. Para el año 2023, la cifra aumentó drásticamente hasta el 65 %, lo que refleja un avance amplio sobre la adopción de normativas de privacidad en diversas regiones del mundo.

Para el año Dos mil Veinticuatro, las cifras seguían en aumento, ya que alcanzaron un 73%. Este aumento es bastante considerable ya que sugiere la tendencia es a seguir implementando y fortaleciendo las normativas en respuesta a la presión socioeconómica para garantizar la privacidad de los ciudadanos. No obstante, es preocupante que aproximadamente un 27% de la población mundial aún no se encuentre amparada por normativas específicas de protección de la privacidad, lo que pone de manifiesto la urgente necesidad de intensificar esfuerzos regulatorios, especialmente en regiones como América Latina, África y ciertas zonas de Asia. En muchos casos, las estadísticas hacen ver que las leyes concernientes frente a la privacidad de datos, es un tema en constante crecimiento, por las implicancias a las que conlleva, ya que alcanzar una homogenización global es un reto arduo aún. Sin embargo, el mayor desafío radica no solo en la mera creación de normativas, sino más bien en garantizar una aplicación

efectiva y un cumplimiento riguroso para proteger realmente la información personal de los ciudadanos (Petrosyan, 2024).

El Reglamento General de Protección de Datos (RGPD) de la U.E es considerado un referente en este ámbito, ya que ha logrado de manera significativa tener un impacto sobre la imposición de sanciones de tipo económica, mejorando con esto la percepción del manejo de los datos, con lo cual se ha conseguido una transformación de las estrategias empresariales y una mejora en la percepción de los consumidores. Hasta 2023, las sanciones impuestas hasta el momento por diferentes delitos en este contexto superaban los 2.800 millones de euros, un hecho sin precedentes, lo cual deja de manifiesta la importancia creciente por la gestión responsable de los datos y, la privacidad, este hecho ha permitido el fortalecimiento de aspectos como la responsabilidad social corporativa. A nivel de los usuarios, las regulaciones han fomentado un nivel aun mayor de confianza y transparencia, con un 31% de la población europea han reportado mejoras significativas en sus experiencias relacionadas con la privacidad e integridad de sus datos.

Para las entidades, como el RGPD estas cifras viene cobrando un significado importante ya que se demuestra una gestión de datos más rigurosa y una salvaguarda mayor, lo que significa que hay un mejor escenario para la inversión en ciberseguridad. No obstante, aún se observa que cerca del 30% de las empresas en Europa aun no cumplen con la normatividad vigente. Más allá de las fronteras europeas, también ha influido en países como Estados Unidos, donde diversas compañías han ajustado sus políticas para alinearse con estos estándares internacionales de privacidad (Petrosyan, 2024). A nivel demográfico, las personas mayores de 45 años son las más afectadas por violaciones de datos, mientras que los jóvenes entre 25 y 34 años parecen estar mejor protegidos, posiblemente debido a una mayor familiaridad con las tecnologías de seguridad (Petrosyan, 2024).

Teniendo en consideración otros escenarios fuera de Europa, en America del norte la preocupación por la privacidad es bastante preocupante, es por ello, que E.E.U.U ha venido mostrando un mayor compromiso (58%), en comparación con los países de su misma región, ya que mientras que América Latina y Oceanía presentan niveles muy bajos, solo el (4%). En líneas generales, el RGPD viene revolucionado la consecución de datos personales, logrando con ello impulsar a las empresas a mejorar sus medidas de seguridad digital y a los consumidores por exigir mayor claridad en un entorno regulatorio en constante evolución. Igualmente, las crecientes sanciones impuestas a empresas tecnológicas por incumplimientos en la protección de datos personales evidencian la importancia de garantizar la seguridad y privacidad de la información en la era digital. Empresas como Meta (Facebook), Didi Global y Amazon han enfrentado multas millonarias debido a la falta de cumplimiento con normativas como el Reglamento General de Protección de Datos (RGPD), reflejando la creciente preocupación de los reguladores por la vulnerabilidad de los usuarios frente a filtraciones, uso indebido y falta de transparencia en el manejo de sus datos (González-Pizarro et al., 2022).

En línea con el anterior escenario, Colombia enfrenta un desafío dual: por un lado, asegurar que su normativa esté en concordancia con marcos como el RGPD europeo, el cual ha generado sanciones de miles millones de euros, además de impulsar mejoras en la transparencia, la ciberseguridad y la confianza; y por el otro, mejorar la efectividad de

su aplicación para prevenir que la falta de claridad y coherencia en las normas amenace los derechos de los usuarios y la competitividad digital del país. la falta de coherencia normativa, aduciendo los datos ya expuestos, no solo se impacta la protección legal del consumidor digital, sino adicionalmente dificulta la capacidad de actuación frente a infracciones, y con ello, haciendo más onerosa la colaboración entre países, lo que mina la confianza del usuario final, esto resulta preocupante dado que la mayoría de las organizaciones admiten que necesitan ser más responsables y transparentes en el manejo de los datos personales.

Situación Normativa en la Protección de Datos en el Comercio Electrónico Colombiano

En la actualidad Colombia ha dado sus primeras impresiones acerca de la implementación de un marco regulatorio destinado a salvaguardar la información personal, si tenemos en cuenta el artículo 15 de su Constitución Nacional, el cual, garantiza el derecho al hábeas data. Y considerando las leyes 1266 de 2008 y 1581 de 2012 las cuales abordan los temas de información financiera y la consecución de datos en términos generales. Y las normativas que establecen los principios fundamentales de legalidad, privacidad y de la protección de datos, asigna a la Superintendencia de Industria y Comercio (SIC) la función de supervisar y sancionar el cumplimiento de estas reglas. En la Actualidad, la aplicación efectiva de la normativa en el ámbito digital aun es escaza, y enfrenta importantes retos que todavía exigen un desarrollo más claro y sólido en la jurisprudencia. En por esto que, la Ley 527 de 1999 se centra en el comercio electrónico, ya que busca regular los aspectos técnicos como firmas digitales y un mejor uso de correos electrónicos; Sin embargo, su alcance es bastante limitado, ya que no ofrece una protección integral de los datos personales en el espacio digital. Regulaciones como la Ley 1480 de 2011, enfatiza sobre la protección del consumidor, sin embargo, esta encuentra dificultades para ser aplicadas en transacciones que trascienden las fronteras nacionales.

Tomando como referencia el Acuerdo Colombiano de Comercio Electrónico (ACIEC), derivado de la Ley 527 de 1999, la búsqueda en la armonización de las normativas internacionales y regionales ha resultado ser una labor titánica, ya que la estandarización debe apuntar a un objetivo claro, ya que lo que se persigue es con el firme propósito de fortalecer la seguridad jurídica en las operaciones en línea. No obstante, persisten importantes vacíos legales, solapamientos normativos y una débil coordinación entre los diferentes niveles jurídicos, tanto a nivel nacional como internacional, lo que limita la coherencia y eficacia del sistema regulatorio en el comercio digital. Estos factores evidencian la necesidad de revisar y actualizar el marco normativo para garantizar mayores certezas y protección en el entorno digital.

El ACIEC fue creado para proteger y aumentar la confianza sobre el entorno digital, buscando con esto, incrementar y facilitar aún más el desarrollo del comercio electrónico, en aras de garantizar una fluida interoperabilidad entre Colombia y sus diferentes socios comerciales, todo ello, en el contexto de unos principios de neutralidad tecnológica y no discriminación. Sin embargo, su implementación y aplicabilidad enfrentan diversas vicisitudes internas. aunque el Acuerdo de Comercio Electrónico Colombiano, adquiere una importante relevancia en la política de comercio electrónico y sobre la digitalización,

sus alcances aún son muy incipientes, ya que, esta se ve limitada por una persistente fragmentación normativa.

El marco regulatorio como está concebido en la actualidad, a pesar de impulsar la armonización y simplificación del comercio digital, no ha logrado ser incorporado de manera efectiva dentro del sistema jurídico nacional. Ya que persisten desajustes entre los principios que impulsa el ACIEC y la legislación colombiana, hay casos particulares como en el consentimiento informado, la transferencia internacional de datos y la resolución adecuada de conflictos. Por no mencionar más, todo esto sumado a una falta de coherencia normativa se resta la falta de una capacidad institucional limitada, que, junto a órganos como la Superintendencia de Industria y Comercio, desconocen abiertamente de los mecanismos adecuados para supervisar plataformas extranjeras que operan en Colombia sin presencia física.

Para corregir estas dificultades, se hace indispensable buscar una conexión que permita consolidar las regulaciones nacionales, con los tratados internacionales y, en un estadio mayor con la jurisprudencia constitucional, buscando así garantizar la protección efectiva del consumidor en el ámbito digital, logrando con esto el fortalecimiento de la seguridad jurídica del comercio electrónico. La Corte Constitucional y la Corte Suprema de justicia, han venido dejando importantes referentes, pero corresponde al legislador abordar la discrepancia entre las normas tradicionales y las nuevas dinámicas del comercio en línea. Para algunos juristas la solución radica en realizar una reforma integral con una visión global, con el concurso de una colaboración internacional efectiva que permita asegurar una auténtica soberanía digital para los países y, así resguardar los datos personales de los colombianos, de manera segura y efectiva.

Para el caso colombiano las normativas que guardan relación con el Habeas Data y los derechos del consumidor operan de manera independiente, como si fuesen dos reglamentos en contraposición, poco eficientes y sin una coordinación efectiva, esto genera incertidumbre sobre qué entidad tiene la autoridad en ciertas circunstancias digitales. En este marco, el fallo de la Corte Constitucional ha sido fundamental al considerar el derecho al hábeas data como un derecho separado (Sentencia T-414 de 1992, reafirmada en la T-729 de 2002), aceptando que debe ser aplicado también en el contexto digital. Además, en la Sentencia T-062 de 2021, la Corte determina que el flujo de datos en plataformas digitales no exime a estas de la obligación de adherirse a los principios de finalidad, legalidad y consentimiento informado, incluso si los servidores están situados en el extranjero. Sin embargo, la implementación de estos principios está comprometida por la ausencia de un sistema integral de cumplimiento digital que permita a la Superintendencia de Industria y Comercio (SIC) llevar a cabo una supervisión efectiva sobre entidades internacionales con presencia digital en Colombia.

Es importante señalar que la falta de alineación entre las normativas generales relacionadas con el habeas data, la Ley 1266 de 2008 que regula la información financiera y crediticia, y el Estatuto del Consumidor (Ley 1480 de 2011) evidencia una fragmentación legal que obstaculiza una protección completa y efectiva contra las prácticas de recolección, manejo y transferencia de datos realizadas por plataformas digitales. En el ámbito jurídico, el Tribunal Constitucional ha señalado que el hábeas data es un derecho autónomo y fundamental para los ciudadanos colombianos, por lo

que, cuya protección no solo debe aplicar para la presencialidad, sino que más bien debe extenderse también al entorno digital. Teniendo como referente la sentencia T-414 de 1992, y su revisión posterior en la T-729 de 2002, se logró dilucidar que toda persona tiene el derecho a conocer, actualizar y corregir sus datos personales, aun incluso cuando estos datos hayan sido recopilados por entidades privadas.

En recientes revisiones, en la Sentencia T-275 de 2021, de la Corte, se afirmó que las plataformas digitales están obligadas a respetar los principios de legalidad, finalidad y consentimiento, sin importar que sus servidores se ubiquen fuera del territorio nacional. Esto causo un revuelo sin precedentes ya que el pronunciamiento resalta la trascendencia de proteger los datos personales, aún más allá de las fronteras, especialmente en el contexto del comercio electrónico.

Esto significo para Colombia entrar a mediar sobre grandes retos al intentar aplicar resoluciones o sentencias extranjeras que buscan proteger los derechos de los consumidores digitales dentro de su jurisdicción. Lo cual hasta el momento resultaba imposible, teniendo en cuenta un referente claro fue el análisis crítico sobre las cláusulas contractuales que se imponían de manera unilateral por las plataformas, las cuales desconocían en gran medida la jurisdicción a aplicar, para así crear un escenario favorable para las empresas extranjeras en lo que respecta a dirimir conflictos. Desconociendo en este sentido, la legislación colombiana la cual ha establecido parámetros para que, aunque las partes puedan pactar ciertos acuerdos, se garantice la protección efectiva de los derechos dentro del territorio nacional. Con un árbitro imparcial y designado por la cámara de comercio internacional, aplicando de manera efectiva la jurisdicción para este tipo de operaciones internacionales, no se debe ignorar el derecho constitucional de acceder a la justicia de manera efectiva, especialmente cuando el consumidor se encuentra en una posición desfavorable.

La falta de una regulación clara que contemple de manera global a las plataformas digitales y el comercio electrónico ha logrado generar varios vacíos legales, hechos que han ido en contravención de las buenas prácticas del comercio exterior, podemos destacar casos como el uso inapropiado de la información y, la manipulación automatizada de los precios. Aunque en la actualidad existen normas antimonopolio, estas presentan limitaciones que perjudican especialmente a las pequeñas y medianas empresas en los países menos desarrollados, afectando la equidad dentro del entorno digital. aumentando las desigualdades de una manera más alarmante, Asimismo, la disparidad en las regulaciones sobre la gestión de datos personales crea un clima de incertidumbre respecto a las responsabilidades tanto de las plataformas como de los proveedores, incrementando los riesgos para los consumidores, particularmente en lo relacionado con fraudes y el robo de identidad.

En un informe reciente de la Superintendencia de Industria y Comercio (SIC), muchas empresas vienen incumpliendo principios esenciales, tales como la obtención del consentimiento informado y la protección efectiva de la privacidad. Esto dificulta los avances y limita el crecimiento en la confianza hacia estas nuevas herramientas de la dinámica actual, es penoso mencionar que esta entidad enfrenta obstáculos para poder supervisar de manera adecuada los eventos y comportamientos en el sector tecnológico. Sumado a esto existe una falta de coordinación internacional, lo cual dificulta una

respuesta más eficaz a nivel glocal. Para el caso de nuestro país, Colombia aún no ha logrado alinearse plenamente con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, esto limita la participación del país en los mercados digitales a nivel mundial (Husain, 2024), hecho que aminora los procesos competitivos y de desarrollo empresarial.

Colombia es un país de leyes y normas y aunque existen un sinnúmero de ellas hay una que llama particularmente la atención la Ley 1581 de 2012, busca la protección de los datos personales, la Ley 1480 de 2011, también orienta sobre los derechos del consumidor, sin embargo aun es insuficiente para afrontar los desafíos propios del entorno digital, ya que elementos como la transferencia transfronteriza de datos, la automatización de decisiones y la validez y alcance de los acuerdos de consentimiento en línea aún carecen de una legislación clara y ajustada a la problemática del país. En consecuencia, se evidencia la necesidad urgente de actualizar y fortalecer el marco normativo en aras de garantizar una protección real y eficaz de las operaciones que se realizan a través del comercio electrónico y, de una mayor salvaguarda de la gestión de datos digitales.

Siguiendo la dinámica de lo anterior, se hace imprescindible llevar a cabo una modernización profunda del marco legal colombiano vigente, lo que significaría la actualización de la Ley 527 de 1999, que permita adaptarse de manera más sencilla a las nuevas realidades del comercio electrónico actual. Siendo congruentes con esto, se hace necesario que la Superintendencia de Industria y Comercio (SIC) asuma un rol más proactivo y menos pasivo, en pro del fortalecimiento de la supervisión y el control de mayores ámbitos a nivel nacional. En paralelo a esto, es importante destacar que se deben diseñar y promover unas políticas públicas más efectivas que compulsen la cooperación internacional, y una adopción más efectiva de los estándares globales, lo cual facilitara la instalación de mecanismos de supervisión más eficientes y coordinados frente a las nuevas dinámicas que exige el panorama actual.

En Colombia se ha hecho imperante la necesidad de construir una regulación más integral que permita abarcar no solo la protección de los datos personales, sino también, el comercio electrónico, y que adicionalmente también vigile a las plataformas digitales con sus avances en inteligencia artificial. La armonización normativa, es urgente y necesaria, tanto a nivel nacional como en consonancia con tratados y acuerdos internacionales, estamos en deuda con el consumidor, por ello se demanda crear bases sólidas frente al fortalecimiento de la competitividad empresarial y garantizar con ello, la estabilidad jurídica dentro del espacio digital.

El dinamismo actual ha puesto de manifiesto la imperiosa necesidad de revisar un vasto número de normas relacionadas con la protección de datos en Colombia, alineándolas con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Es por ello por lo que resulta imperativo incrementar la colaboración judicial a nivel mundial y, de explorar múltiples mecanismos para la resolución de disputas en línea. En pro de lograr una interacción más efectiva entre legisladores, jueces y autoridades reguladoras, lo cual, resulta esencial para disminuir la fragmentación regulatoria entre las partes y, así preservar los derechos digitales de la ciudadanía en un entorno digital cada vez más complejo y dinámico.

Teniendo como referencia el marco del comercio electrónico a nivel global, aun Colombia enfrenta muchos restos significativos frente a la protección de la información personal de los colombianos, y todo ello se debe en gran medida por la indebida fragmentación normativa y la baja eficacia en los sistemas de control vigentes. Donde a pesar de contar con normas como la Ley 1581 de 2012, la Ley 1266 de 2008 y la Ley 527 de 1999, estas disposiciones resultan insuficientes y discordantes frente a los riesgos digitales actuales, y aun mas con el rápido crecimiento de estas, lo cual, no deja espacio para esperas. Como respuesta estratégica a esta problemática, se ha propuesto la creación del Sistema Integral Colombiano de Protección Digital (SICPD), esta fue concebida como una alternativa nacional que busca garantizar la protección, confianza y equidad en el marco del entorno digital mediante la innovación normativa, institucional y educativa.

Para el Sistema Integral Colombiano de Protección Digital, fue concebido como un conjunto de principios, normativas y estrategias orientadas a salvar la seguridad digital de los colombianos en el ámbito digital. Sus bases se encuentran en el CONPES 3701, cuyo principio fundamental es el propósito es ampliar las capacidades del estado en materia de ciberseguridad y protección de la seguridad nacional de los datos de sus ciudadanos. En este contexto, resulta diseñar un marco legal moderno y coherente que se integre y permita una actualización de las normativas existentes para enfrentar adecuadamente los desafíos digitales presentes y futuros.

Por ello se hace imperativo crear una regulación más integral que ponga de manifiesto y especial énfasis en la protección de la información que se maneja en las plataformas digitales, redes sociales, mercados virtuales y en las tecnologías emergentes, al igual que sobre la inteligencia artificial. Siempre teniendo como referente el Reglamento General de Protección de Datos (RGPD) de la U.E, la cual habla de la incorporación de principios esenciales como la responsabilidad proactiva, la privacidad desde el diseño y la privacidad por defecto. Así, lograremos garantizar que el manejo de los datos personales esté basado en criterios de prevención y responsabilidad desde la misma concepción de los sistemas tecnológicos. Por ello, se hace necesario la implementación para la mayor parte de los países de este marco normativo ya que con ello se contribuirá con el cierre de brechas regulatorias existentes, ofreciendo una mayor certeza jurídica tanto para las empresas como para los usuarios.

Simultáneamente, resulta imperante realizar una reforma de fondo que contemple la creación de la Autoridad Colombiana de Protección de Datos Digitales (ACPDD). Como un organismo autónomo que cuente con amplias facultades para imponer sanciones efectivas y proporcionales a las dinámicas que demanda el entorno actual, este organismo debe adicionalmente tener la capacidad de intervenir frente a infracciones cometidas por entidades digitales a nivel internacional. También debe estar atenta a supervisar el cumplimiento normativo, otra de las grandes cualidades con las que debe cumplir la ACPDD, es que tendría la misión de auditar algoritmos, vigilar el uso ético de la inteligencia artificial y promover convenios de cooperación con organismos internacionales, en aras del fortalecimiento de la protección de datos en un contexto cada vez más globalizado.

En Colombia también se hace necesaria la creación de una Plataforma Nacional de Certificación en Protección de Datos, denominada CERTIDATA, que funcionaría

inicialmente como un sistema voluntario de certificación para las empresas, con la posibilidad de convertirse en obligatorio en el futuro. Esta certificación facilitaría la obtención de un sello de confianza digital, que estaría a disposición de los consumidores para brindarles información clara sobre el compromiso de las organizaciones con la protección de la privacidad. Así, se contribuiría a fortalecer un mercado digital más transparente y competitivo, beneficiando especialmente a micro, pequeñas y medianas empresas al incentivar buenas prácticas.

Llegados a este punto también debemos contemplar el alcance para los startups, ya que se hace necesario la instauración de un marco regulatorio especifico, que permita impulsar los procesos de innovación, generando así nuevos desarrollos de IA, plataformas digitales experimentales, que permitirán brindar mejores servicios con sus productos y servicios en entornos controlados bajo supervisión legal. Esta medida evitaría que las regulaciones se conviertan en un obstáculo y facilitaría evaluar con anticipación el impacto que estos desarrollos puedan tener en la privacidad y la seguridad, garantizando una protección preventiva para los usuarios.

Muchas veces se ha hablado de fomentar una cultura digital sólida en la sociedad mediante programas educativos continuos liderados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Ministerio de Educación Nacional (MEN). Con la creciente necesidad de la adopción en la educación básica contenidos relacionados con programación, manejo de tic, derechos digitales, privacidad y seguridad en línea. Muestra el gran compromiso que tienen las autoridades del país por la protección de los datos personales. De igual forma, las universidades y organizaciones profesionales ven cada vez más ven la necesidad de formar auditores especializados en protección de datos o consultores en cumplimiento normativo, perfiles que actualmente son escasos en Colombia. Esta estrategia integral apunta a fortalecer tanto la protección como la confianza en el ecosistema digital del país, como la protección y buen manejo de los datos personales.

Otro tema que se hace necesario debatir es la implementación de un Mecanismo Ágil de Resolución de Disputas Digitales (MADR-D) para Colombia. Ya que este podría constituirse en una solución eficaz que enfrente las dificultades propias de las operaciones digitales, en particular aquellas que tienen un carácter internacional. Si bien este mecanismo permitiría a los consumidores como a las empresas resolver conflictos mediante plataformas digitales, logrando con esto evitar procesos judiciales costosos y prolongados. Además, la integración de este sistema con plataformas de cooperación regional como APEC, la OCDE o el Pacto Andino fortalecería la posición de Colombia como un actor activo y relevante en la gobernanza digital a nivel global.

En síntesis, esta propuesta representa una respuesta integral, innovadora y coherente a los principales desafíos que enfrenta Colombia en la protección de la información personal dentro del comercio electrónico. No solo busca solventar la discontinuidad normativa y las limitaciones institucionales actuales, sino que también proyecta un enfoque basado en la transparencia, la responsabilidad compartida y la cooperación internacional. Adoptar este mecanismo facilitaría la construcción de un entorno digital

más seguro, confiable y competitivo, posicionándose al país como un referente regional en materia de gestión digital.

CONCLUSIONES

El artículo pone en evidencia la falta significativa de coherencia normativa en Colombia en materia de protección de la información personal, especialmente dentro del comercio electrónico. Aunque existen leyes como la 1581 de 2012, la 1266 de 2008 y la 527 de 1999, estas presentan contradicciones y no han sido actualizadas para responder adecuadamente a los retos actuales del entorno digital. Esta situación crea una incertidumbre jurídica que limita la capacidad de supervisión de la Superintendencia de Industria y Comercio (SIC), afectando aspectos cruciales como la privacidad, el consentimiento informado y la protección efectiva de los datos personales. La creciente necesidad de marcos regulatorios específicos para plataformas digitales, redes sociales e inteligencia artificial agrava la desconfianza de los consumidores y dificulta la competitividad del ecosistema digital colombiano.

Los hallazgos del estudio confirman la hipótesis principal: la ausencia de una regulación clara, coordinada y específica en comercio electrónico genera un estado de inseguridad legal que perjudica tanto la competitividad nacional como la confianza de los usuarios. Las empresas, en particular las pequeñas y medianas (PYMES), enfrentan serias dificultades para adaptarse a un marco regulatorio incierto y disperso, mientras las plataformas internacionales operan sin un régimen legal claro que se ajusta a las normativas locales. Esta situación coloca a los consumidores en una posición vulnerable ante posibles fraudes o el mal uso de su información personal, y limita la integración de Colombia en mercados globales que exigen altos estándares, como el Reglamento General de Protección de Datos (RGPD) europeo. Asimismo, la falta de uniformidad regulatoria y la insuficiente capacidad sancionatoria representan obstáculos considerables para el desarrollo del comercio electrónico, disminuyendo la efectividad y el potencial de crecimiento del sector digital en Colombia.

Para enfrentar este reto, se plantea la implementación del Sistema Integral Colombiano de Protección Digital (SICPD), una estrategia estructurada que se sustenta en seis pilares esenciales. En primer lugar, la actualización y consolidación de la normativa vigente para fortalecer y articular el marco legal existente. En segundo término, la creación de una autoridad autónoma con mayores atribuciones para supervisar y sancionar efectivamente. Además, se contempla el desarrollo de una plataforma nacional de certificación que impulse la autorregulación en el sector. También se incluye un entorno regulatorio experimental que fomenta la innovación responsable en el ámbito digital. Complementariamente, el SICPD incorpora una estrategia de educación digital orientada a capacitar tanto a ciudadanos como a empresas sobre sus derechos y deberes en el entorno digital. Finalmente, se propone establecer un mecanismo ágil y eficaz para la resolución de disputas digitales, facilitando la gestión de conflictos en el comercio electrónico y otras áreas digitales.

El propósito fundamental de esta iniciativa es corregir las deficiencias regulatorias actuales, aumentar la confianza de los consumidores y fortalecer la competitividad de Colombia en el ecosistema digital global, cada vez más exigente y dinámico.

REFERENCIAS

Abdulrauf, L. A., & Fombad, C. M. (2016). Personal data protection in Nigeria: Reflections on opportunities, options, and challenges to legal reforms. *Liverpool Law Review, 38*(2), 105–134. https://doi.org/10.1007/s10991-016-9189-8

Ayunda, R. (2022). Personal data protection to e-commerce consumer: What are the legal challenges and certainties? *Law Reform, 18*(2), 144–163. https://doi.org/10.14710/lr.v18i2.43307

Azmeh, S., Foster, C., & Echavarri, R. (2020). The international trade regime and the quest for free digital trade. *International Studies Review, 22*(3), 671–692. https://doi.org/10.1093/isr/viz033

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A process for data protection impact assessment under the European General Data Protection Regulation. *Annual Privacy Forum*, 9857, 21–37. https://doi.org/10.1007/978-3-319-44760-5_2

Centre for International Governance Innovation (CIGI), Institut Public de Sondage d'Opinion Secteur (IPSOS), Internet Society (ISOC) y United Nations Conference on Trade and Development (UNCTAD). (2019). Survey: Cybercriminals, social media, lack of security increasingly fueling internet distrust. UNCTAD. https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/

Corte Constitucional de Colombia. Sentencia T-414 de 1992. https://www.informatica-juridica.com/anexos/corte-constitucional-sentencia-t-414-1992/?utm_source

Corte Constitucional de Colombia. Sentencia T-729 de 2002. https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm.

Corte Constitucional de Colombia. Sentencia T-275 de 2021. https://www.corteconstitucional.gov.co/relatoria/2021/t-275-21.htm.

Documento técnico sobre el Acuerdo Colombiano de Comercio Electrónico (ACIEC). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://observatorioecommerce.mintic.gov.co/797/articles

Departamento Nacional de Planeación. (2011). Documento CONPES 3701: Estrategia para el desarrollo del comercio electrónico en Colombia. Consejo Nacional de Política Económica y Social, República de Colombia. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf.

Ferencz, J., & Gonzales, F. (2019). Barriers to trade in digitally enabled services in the G20. *OECD Trade Policy Papers*, 232. https://doi.org/10.1787/264c4c02-en

Ferracane, M. F., & van der Marel, E. (2021). Regulating personal data: Data models and digital services trade (Policy Research Working Paper No. 9596). World Bank. https://ideas.repec.org/p/wbk/wbrwps/9596.html

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), 703–705. https://doi.org/10.2501/IJMR-2017-050

Hassan, K. H. (2012). Personal data protection in employment: New legal challenges for Malaysia. *Computer Law & Security Review, 28*(6), 696–703. https://doi.org/10.1016/j.clsr.2012.07.006

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum, 37*(2), 119–133. https://doi.org/10.26532/jh.v37i2.16272

Hoofnagle, C. J., Van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Husain, O. (2024). 79 estadísticas reveladoras sobre privacidad de datos para 2024. Enzuzo. https://www.enzuzo.com/blog/data-privacy-statistics

Karim, M. S. A., Puluhulawa, F., Puluhulawa, J., & Swarianata, V. (2022). Legal protection for consumers' personal data in online shopping. *Estudiante Law Journal, 4*(2), 623–638.

Ley 1266 de 2008. Habeas data financiero. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34488

Ley 1480 de 2011. Estatuto del Consumidor. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=44306

Ley 1581 de 2012. Protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

López González, J., Casalini, F., & Porras, J. (2022). A preliminary mapping of data localisation measures. OECD Trade Policy Papers, 262. https://www.oecd.org/en/publications/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en.html

Lund, S., & Tyson, L. (2017). La globalización no está en retirada; se ha vuelto digital. Foro Económico Mundial. https://es.weforum.org/stories/2017/02/la-globalizacion-no-esta-en-retirada-se-ha-vuelto-digital/

Organization for Economic Co-operation and Development (OECD). (2016). Consumer protection in e-commerce: OECD recommendation. OECD. https://www.oecd.org/en/publications/oecd-recommendation-of-the-council-on-consumer-protection-in-e-commerce_9789264255258-en.html

Organization for Economic Co-operation and Development (OECD). (2022a). Dark commercial patterns (OECD Digital Economy Papers No. 336). https://www.oecd.org/en/topics/dark-commercial-patterns.html

Pashynskyi, V. (2023). Administrative-legal support for the protection of citizens' personal data: Contemporary theoretical approaches. *VJHR*, (4), 55–61. https://doi.org/10.61345/1339-7915.2023.4.10

Petrosyan, A. (2024). Población mundial con datos personales cubiertos por la normativa de privacidad 2020–2024. *Statista*. https://www-statista-com.translate.goog/statistics/1175672/population-personal-data-regulations-worldwide

Reglamento General de Protección de Datos (GDPR), Unión Europea.

Syafta, G., Fahni, R., & Ningsih, A. F. (2022). Independent supervisory authority to protect social media users' personal information in Indonesia. *Ius Poenale, 3*(1), 39–48. https://doi.org/10.25041/ip.v3i1.2531

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Tovino, S. A. (2020). Mobile research applications and state data protection statutes. *The Journal of Law, Medicine & Ethics, 48*(S1), 87–93. https://doi.org/10.1177/1073110520917033

United Nations Conference on Trade and Development (UNCTAD). (2022). Digitalisation of services: What does it imply to trade and development? https://unctad.org/publication/digitalization-services-what-does-it-imply-trade-and-development

United Nations Conference on Trade and Development (UNCTAD). (2023). Building trust in digital markets through enhanced consumer protection on online platforms. https://unctad.org/system/files/information-document/ccpb_IGE_CON_2023_PROG_platforms_digital_en.pdf

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation? International. *Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

FINANCIAMIENTO

El presente artículo es producto del proyecto de investigación denominado Geopolítica y Comercio Internacional: El impacto de las tensiones geopolíticas en las cadenas de suministro. Gestionado académica y financieramente en la Universidad del Sinú: Elías Bechara Zainum. A través de la convocatoria interna de proyectos para el periodo de desarrollo (2024-2025).

CONFLICTO DE INTERES

El autor declara que no existe conflicto de interés

BIODATA

Manuel Antonio Pérez Vásquez: Postdoctor en Gerencia y Políticas Públicas, Doctor en Ciencias Sociales Mención Gerencia, Magister en Negocios Internacionales e Integración, Máster MBA internacional en Administración y Dirección de Empresas, Especialista en Gestión de Negocios Internacionales, Profesional en Negocios y Finanzas Internacionales. Universidad Del Sinú Sede Montería, en la actualidad se desempeña como docente Investigador del Programa de Negocios Internacionales, Es Investigador Senior MINCIENCIAS, Perteneciente al grupo de investigaciones CUS categoría A1.