



**DESAFÍOS DE COLOMBIA Y SUS ENTIDADES EN LA PROTECCIÓN
TRANSFRONTERIZA DE DATOS Y DEL COMERCIO ELECTRÓNICO.**

Autor:

JUAN RICARDO GAMA ESCOVAR

Director:

JUAN FELIPE JARAMILLO CASTILLO

**Trabajo presentado como requisito parcial para acceder al título de Máster en
Derecho Corporativo**

**Facultad de Jurisprudencia
Programa de Maestría en Derecho Corporativo
Bogotá, Colombia 2025**

RESUMEN

El trabajo analiza los desafíos de Colombia para proteger a los consumidores y los datos personales en el comercio electrónico transfronterizo. Examina los límites territoriales de la Ley 1480 y de la Ley 1581, el papel de la SIC y los mecanismos de cooperación (ICPEN y econsumer.gov), y compara el marco colombiano con el GDPR y la LGPD a fin de proponer reformas aplicables (ODR, representante local, SCC/BCR).

ABSTRACT

The paper analyzes Colombia's challenges in protecting consumers and personal data in cross-border e-commerce. It examines the territorial limits of Law 1480 and Law 1581, the role of the SIC, and cooperation mechanisms (ICPEN and econsumer.gov), and compares the Colombian framework with the GDPR and the LGPD in order to propose applicable reforms (ODR, local representative, SCC/BCR).

I. PROTECCIÓN AL CONSUMIDOR

1. Estado actual del comercio electrónico y la protección al consumidor en Colombia.

1.1. Definición y clasificación del comercio electrónico

En la era digital, y con el surgimiento en el último siglo del término “Tecnología de la información y las comunicaciones” el comercio y la relación entre productor, vendedor y consumidores, ha visto un cambio radical, en como se compra y como se vende. Pero para entenderse se debe partir de la definición de “Comercio electrónico” y sus implicaciones prácticas en el entorno normal de la economía mundial, y cómo estas han transmutado como se interpreta el derecho en el espacio. En términos muy generales el Comercio electrónico puede llegar a definirse como “la compra o venta de bienes o servicios que se realiza a través del Internet. “

Sin embargo termina siendo bastante corta esta definición, ya que se deja de lado en esta a los actores más importantes de la operación del comercio electrónico, siendo estos, los clientes (customers) los comercios (Business) e incluso el Gobierno (Government). Es así que el comercio electrónico se clasifica de varias maneras de acuerdo con los actores que intervienen en su desarrollo y la naturaleza de la transacción por ejemplo: el comercio electrónico entre empresas (B2B) Business to Business (B2B) implica transacciones comerciales entre dos empresas; que se cimienta en relaciones entre iguales, que tienen intereses comunes y propios, por lo que normalmente estas relaciones se regulan a través de contratos de libre discusión con cláusulas regidas por la voluntad de ambas partes. Mientras que el comercio electrónico entre empresas y consumidores (B2C) Business to customer se refiere a las transacciones realizadas entre una empresa y los consumidores finales, que implica una relación de desigualdad, donde hay una clara asimetría de la información, por lo que en la práctica estas relaciones se regulan por un contrato de adhesión redactado y exigido por parte del empresario. Por otro lado, el comercio electrónico entre consumidores (C2C) Customer to Customer involucra transacciones directas entre los propios consumidores a través de plataformas en línea, por lo cual en teoría es una relación de igualdad entre partes,

pero que se desarrolla en el marco de una plataforma virtual provista por un proveedor que provee un contrato de adhesión al que ambas partes vendedoras y compradoras deberán atenerse para el correcto desarrollo de la actividad comercial. Es más, también se cuenta con el comercio electrónico entre empresas y administraciones públicas (B2G) Business to Government, donde las empresas realizan transacciones con las entidades del gobierno de país en el que operan, estas relaciones normalmente se regulan por la normatividad específica en materia de contratación pública, por lo que normalmente existe una negociación que termina fijando un contrato negociado por ambas partes con igualdad y asimetría de la información, pero con una parte que normalmente tiene atribuciones exorbitantes, siendo esta normalmente el gobierno comprador. (MinTIC. ABC del eCommerce)

1.2. Diferencias con el comercio tradicional

Cabe aclarar que es importante el identificar las mayores diferencias que existen entre el comercio tradicional y el comercio electrónico, según Erick Rincón, éstas recaen en que:

- A. Las operaciones se realizan por vía electrónica a través de un mensaje de datos.
- B. El lugar en donde se encuentren las partes en principio no es relevante.
- C. No queda prueba en papel sobre el acuerdo o pago, siempre y cuando así lo acuerden las partes.
- D. El bien que se importa de manera electrónica no pasa por ningún tipo de inspección ni aduana (en caso del denominado comercio electrónico directo)
- E. En la mayoría de los casos no hay intermediarios.
- F. Cada empresa, por pequeña que sea, puede llegar a tener presencia mundial, pues su acceso y presencia en los diferentes mercados es ilimitada.

Estas características, más que todo la irrelevancia del lugar de la transacción, así como la facilidad de éstas sin que muchas veces se pueda tener una trazabilidad de estas, y aunado al hecho de que los vendedores pueden vender a cualquier lugar del mundo, indiferente de su país de origen. Hace que estas transacciones sean de especial cuidado por lo fácil que puede ser el que existan estafas, o violaciones directas a los derechos de los consumidores.

Es ahora cuando se hace importante el entrar a analizar la legislación colombiana, y que herramientas ofrece para proteger a los consumidores electrónicos, pero más especialmente a los consumidores electrónicos de vendedores transfronterizos. La ley 1480 de 2011, surgió como un elemento normativo que buscaba dinamizar y hacer más asequible la justicia para uno de los actores más vulnerables dentro de las relaciones comerciales en Colombia. El Consumidor, quien, para la ley, es “Toda persona natural o jurídica que, como destinatario final, adquiera, utilice o disfrute de un bien o servicio, en desarrollo de una relación de consumo.” Es decir la ley busca proteger a quienes buscan obtener bienes y servicios sin un fin comercial, más allá del de su propio disfrute. Sin embargo, más de allá de la simple compra u obtención, la calidad de consumidor se aclara al comprender la visión de Mauricio Velandia que “Consumidor” es quien usa, desgasta, agota o extingue el producto, es decir quien se relaciona de manera directa con el producto, entendiéndose así que la calidad de comprador puede ser distinta a la del consumidor, o muchas otras veces el consumidor y el comprador, se confundirán con la misma persona (RODRIGUEZ CARRION) .

En este contexto, surge entonces la duda, de por que la legislación Colombiana brinda una protección especial a aquellas personas que tienen la calidad de “Consumidor” En términos

Desafíos de Colombia y sus entidades en la protección transfronteriza de datos y del comercio electrónico.

generales la necesidad de una protección especial para los consumidores se fundamenta en la asimetría existente entre proveedores y consumidores, especialmente en términos de información y poder de negociación. Esta desigualdad puede conducir a prácticas abusivas por parte de los proveedores, afectando los derechos de los consumidores. Por ello, la legislación colombiana ha adoptado medidas para equilibrar esta relación y garantizar una protección efectiva, dichos esfuerzos se han centrado en regularizar y vigilar de manera directa las relaciones de consumo, es por eso que existe la ley 1480 de 2011, así como la ley 1328 de 2009. Sin embargo a pesar de la existencia de la normatividad especial en la materia, estos parecen ser suficientes y efectivos para las relaciones de consumo que se presentan en entornos físicos dentro del territorio Colombiano.

1.3. Alcance del Estatuto del Consumidor y el principio de territorialidad

Ahora bien, ¿qué ocurre en los casos en los que se presenta esta asimetría en un contexto tan complejo, como lo es el comercio electrónico transfronterizo? Al indagar la ley 1480 se encuentra que, esta establece un ámbito de aplicación territorial conforme al principio de territorialidad consagrado en el artículo 18 del Código Civil colombiano, el cual dispone que "la ley es obligatoria tanto a los nacionales como a los extranjeros residentes en Colombia" Este principio implica que las disposiciones de la ley son aplicables a todas las relaciones de consumo que ocurren dentro del territorio nacional, abarcando tanto a los productos nacionales como a los importados. De esta manera, la ley regula los derechos y obligaciones surgidas entre productores, proveedores y consumidores en Colombia, sin importar la procedencia de los bienes o servicios. Sin embargo, la aplicación extraterritorial de la ley es limitada, ya que, según el principio de territorialidad, las leyes colombianas obligan dentro del territorio del Estado, salvo excepciones específicas previstas en tratados o normas internacionales.

De lo anterior se desprende entonces un vacío preocupante, ya que estaríamos ante un escenario en donde la ley, y las entidades de control solo tendrán validez y más que todo poder de ejecución ante entidades que se encuentren directamente constituidas en el territorio Colombiano, dejando vulnerables a 88% de adultos colombianos que a día de hoy ya compran por internet (Payments and Commerce Market Intelligence PCMI), más específicamente a 15% de esa base de compradores quienes realizan compras a tiendas en línea de origen transfronterizo, cómo lo puede ser Aliexpress, Temu, Amazon entre muchos otros comercios que a pesar de vender a consumidores Colombianos, no se encuentran contemplados en la lista de productores y vendedores a los cuales se verían regulados de manera directa por el estatuto de consumidor, en razón a que no se encuentran legalmente constituidos en Colombia.

Pero ¿qué implica realmente que la ley este limitada en el espacio? La primera intuición que se esperaría, es que a pesar de que el principio de territorialidad no permite que las entidades de control puedan hacer exigible la ley Colombiana a entidades que no estén debidamente constituidas en el territorio nacional. Si debiese existir un alcance más amplio, ya que estas entidades si están operando en Colombia, al tener proveedores, pasarelas de pago y medios de pago, así como incluso acuerdos comerciales con Bancos Colombianos, procesos de logística establecidos, y cumplimiento de normas aduaneras. Por lo que las entidades de control en principio tendrían todas las herramientas suficientes para afectar el negocio de

estos comercios electrónicos y hacer exigibles sus decisiones relacionadas con la protección de los derechos de los consumidores.

1.4. Limitaciones jurisdiccionales de la SIC

En este sentido, las entidades de control tendrían herramientas suficientes para incidir en el negocio de estos comercios electrónicos y hacer exigibles sus decisiones relacionadas con la protección de los derechos de los consumidores. Adicionalmente, las Directrices de la OCDE (OCDE, 2003) para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas se enfocan en crear la necesidad de establecer mecanismos de cooperación internacional para perseguir prácticas fraudulentas y engañosas, incluso cuando los proveedores se encuentran fuera de la jurisdicción nacional.

Uno de los aspectos más relevantes de estas directrices es el enfoque de la aplicación de medidas de resarcimiento transfronterizo, como lo podría ser el congelamiento de activos, para garantizar la efectividad de las decisiones de las autoridades de protección al consumidor, en el caso de Colombia la SIC. Si un proveedor extranjero incurre en prácticas comerciales fraudulentas que afectan a consumidores colombianos, las entidades de control podrían coordinarse con sus contrapartes en otros países para inmovilizar fondos, ejecutar sanciones o bloquear servicios financieros utilizados para el fraude.

En este contexto, si bien la territorialidad es un límite formal, la globalización del comercio y las herramientas legales disponibles pueden fortalecer la protección de los consumidores, permitiendo que las entidades regulatorias ejerzan su autoridad más allá de las fronteras nacionales cuando existan vínculos comerciales claros con el país.

Teniendo en cuenta esta falencia en razón a la territorialidad, se debe pasar a comprender la manera en la que se protegen realmente los derechos de los consumidores en Colombia. La Ley 1480 de 2011 (Congreso de la República de Colombia, 2011) (Estatuto del Consumidor) establece las normas que rigen las relaciones de consumo en el país. No obstante, la Superintendencia de Industria y Comercio (SIC) ha señalado que, en ausencia de una representación formal en Colombia, no es posible imponer sanciones o hacer exigibles decisiones contra estos proveedores.

En efecto, la SIC en concepto 24-458242 emitido a petición del fin académico de este trabajo precisó, con base en el principio de territorialidad consagrado en la Constitución Política y en normas como el artículo 18 del Código Civil, que las disposiciones legales, incluyendo las de protección al consumidor, solo son exigibles a quienes se encuentren dentro del territorio colombiano. Así, si una empresa extranjera de comercio electrónico no cuenta con presencia física o representación legal en Colombia y no ha pactado expresamente la aplicación de la ley colombiana en sus contratos, esta queda fuera del alcance del Estatuto del Consumidor. De manera específica, el artículo 50 de la Ley 1480 señala que las obligaciones allí contenidas aplican exclusivamente a proveedores ubicados en el territorio nacional.

2. Cooperación internacional y herramientas existentes

2.1. Participación en redes globales y plataformas multilaterales

Ante estas limitaciones, la regulación colombiana ha buscado alternativas a través de mecanismos de cooperación internacional. Las Directrices de Protección al Consumidor sobre Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas destacan la necesidad de colaboración entre diferentes naciones para abordar el fraude en el comercio electrónico. Algunas de las estrategias recomendadas por la OCDE incluyen:

1. Trabajar de manera conjunta con autoridades de diferentes países para investigar y sancionar casos fraudulentos.
2. Compartir información relacionada con infractores y esquemas de fraude.
3. Congelar activos y hacer cumplir sanciones para garantizar el reembolso de los clientes afectados.

2.1.1. Red ICPEN

En este contexto, Colombia ha reconocido que actuar en solitario no es suficiente para proteger a sus consumidores. Por ello, a través de la Superintendencia de Industria y Comercio (SIC), el país ha fortalecido su participación en redes y acuerdos internacionales, destacándose como un actor comprometido en la defensa de los derechos de los consumidores a nivel global. Uno de los principales escenarios de esta labor es la Red Internacional de Protección al Consumidor (ICPEN, 2020) y Aplicación de la Ley (ICPEN), un foro global que reúne a agencias gubernamentales de diversos países para coordinar esfuerzos contra prácticas comerciales engañosas y fraudulentas en el ámbito transfronterizo.

Colombia se incorporó formalmente a ICPEN alrededor de 2012, alcanzando el estatus de miembro en una red que entonces agrupaba a unas 40 naciones. Este hito fue un motivo de orgullo para la SIC, que destacó las ventajas de esta integración: “permitirá compartir información sobre productos defectuosos y riesgos globales, combatir infracciones transfronterizas a las leyes de protección al consumidor y garantizar que los derechos de los consumidores colombianos sean respetados en otros países”. En la práctica, la membresía en ICPEN le otorga a la SIC la capacidad de contactar directamente a sus contrapartes extranjeras para alertar sobre estafas que afecten a ciudadanos colombianos o para colaborar en investigaciones internacionales. Además, permite participar en iniciativas conjuntas, como el “Mes de la Prevención del Fraude”, una campaña anual de ICPEN que promueve actividades coordinadas en todos los países miembros para educar y proteger a los consumidores.

El compromiso de Colombia con esta red ha sido notable. Durante el periodo 2019-2020, la SIC asumió la presidencia de ICPEN, liderando las iniciativas globales de la red durante ese año. Bajo su dirección, se priorizaron temas clave como la seguridad en el comercio electrónico y el fortalecimiento de la cooperación internacional. Un ejemplo significativo fue la organización de conferencias internacionales en Colombia en 2018, enfocadas en el comercio electrónico, que consolidaron la posición del país como un referente en la agenda global de protección al consumidor. Esta participación refleja el esfuerzo de Colombia por estar a la vanguardia en la defensa de los derechos de los consumidores, no solo a nivel nacional, sino también en el escenario internacional. Siguiendo con esta línea la SIC se

adhiirió desde el 2020 al sistema econsumer.gov gestionada por la FTC como un medio para disminuir las barreras territoriales propias de las transacciones transfronterizas.

2.2. Econsumer.gov

econsumer.gov (FTC, 2023): Origen, Crecimiento y Funcionamiento

En un contexto donde la digitalización ha transformado los hábitos de consumo, las compras en línea se han convertido en una práctica cotidiana que abre un abanico de oportunidades, pero también de riesgos. Los consumidores se enfrentan a un entorno donde los fraudes transfronterizos son cada vez más sofisticados, lo que plantea desafíos significativos para la protección de sus derechos. En respuesta a esta problemática, en abril de 2001, un grupo de agencias de protección al consumidor de diversos países unió esfuerzos para crear econsumer.gov (FTC, 2023), una plataforma internacional diseñada para combatir el fraude en el comercio electrónico transnacional. Este proyecto, impulsado por la Red Internacional de Protección al Consumidor (ICPEN, 2020) y Aplicación de la Ley (ICPEN), con el respaldo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), marcó un hito en la cooperación global para garantizar transacciones seguras.

El propósito de econsumer.gov (FTC, 2023) es doble: ofrecer a los consumidores un canal confiable para reportar irregularidades en transacciones con empresas extranjeras y facilitar la colaboración entre autoridades de distintos países para investigar y sancionar prácticas comerciales desleales. Si bien la adhesión a econsumer.gov (FTC, 2023) no extiende la jurisdicción de la SIC ni modifica la legislación “sí permite a los consumidores en Colombia ser oídos por las autoridades competentes en casos transfronterizos”, según explicó la Superintendencia. Desde su creación, la plataforma ha experimentado un crecimiento notable, integrando a más de 65 países que comparten información y coordinan acciones para enfrentar el fraude a escala global.

La plataforma cumple tres funciones esenciales:

1. Recepción y registro de denuncias: econsumer.gov (FTC, 2023) permite a los consumidores presentar quejas relacionadas con problemas en compras en línea, desde productos no entregados hasta cargos no autorizados en tarjetas de crédito. Este mecanismo asegura que las experiencias individuales sean documentadas y accesibles para su análisis.
2. Intercambio de información entre países: Las denuncias recopiladas son analizadas por agencias gubernamentales de los países miembros, lo que facilita la identificación de patrones de fraude transfronterizo. Esta colaboración agiliza las investigaciones y permite una respuesta coordinada contra los responsables.
3. Educación y prevención del consumidor: Más allá de gestionar quejas, la plataforma ofrece recursos educativos para empoderar a los consumidores, ayudándoles a reconocer señales de alerta y a adoptar prácticas seguras en sus transacciones en línea.

Flujo práctico de denuncia en *econsumer.gov*

1. Ingresar a la plataforma: acceder a econsumer.gov y seleccionar el idioma (la opción en español está disponible).
2. Registrar la queja: describir la compra, el proveedor extranjero, las fechas y los montos; adjuntar soportes como correos electrónicos, capturas de pantalla o comprobantes de pago.
3. Enviar el reporte: el sistema comparte automáticamente el caso con la autoridad de consumo del país miembro pertinente.
4. Seguimiento: el consumidor debe revisar su correo electrónico para atender posibles comunicaciones o solicitudes de información adicional de la autoridad competente.
5. Resultados posibles: el proceso puede concluir en orientación al consumidor, derivación a la autoridad local, acciones coordinadas con otras jurisdicciones o cierre informativo.

2.2.1 Países Miembros y Expansión

En sus inicios, *econsumer.gov* (FTC, 2023) contaba con la participación de 13 países. A medida que el comercio electrónico creció, más naciones se sumaron al esfuerzo de combatir fraudes en línea. Actualmente, entre los países miembros se encuentran:

- América: Estados Unidos, Canadá, México, Brasil, Colombia, Chile, Argentina.
- Europa: Alemania, Francia, España, Reino Unido, Italia, Países Bajos, Suecia, Irlanda.
- Asia-Pacífico: Australia, Japón, Corea del Sur, Singapur, Nueva Zelanda.
- África y Medio Oriente: Sudáfrica, Egipto, Israel.

Cada país cuenta con una agencia gubernamental responsable de proteger a los consumidores y gestionar las quejas recibidas. En el caso de Colombia, la Superintendencia de Industria y Comercio (SIC) se unió a la red en 2020, permitiendo a los colombianos reportar problemas con empresas extranjeras y fortaleciendo la cooperación internacional en esta materia.

2.2.2 Econsumer.gov en Colombia

Econsumer.gov se ha convertido en una pieza clave en la protección de los consumidores a nivel global. Gracias a esta plataforma, es posible reportar fraudes transfronterizos y acceder a la ayuda de agencias gubernamentales de distintos países. Sin embargo, para seguir avanzando en la lucha contra el fraude digital, es fundamental fortalecer la cooperación internacional y mejorar los mecanismos de sanción para que las empresas infractoras no queden impunes.

Sorprende que a pesar de que es una herramienta supremamente útil para los consumidores en Colombia, la SIC poco o nada ha fomentado su uso.

Como ejercicio académico e investigativo, en 5 ocasiones distintas se realizó la consulta a diferentes agentes del Chat de la SIC de la posibilidad que existía de demandar por derechos

al consumidor a una empresa extranjera (Amazon, AliExpress, Temu...) , de los cuales solamente 2 de los agentes tenían conocimiento de la posibilidad de acudir a Econsumer.gov de resto, la mayoría solo se limitaba a decir que no era posible demandar a esas entidades por el principio de territorialidad que gobierna la ley 1480 de 2011. Más allá de esto no existía más información al respecto. Así mismo es supremamente llamativo el hecho de que la plataforma virtual de la SIC, la cual es utilizada para realizar denuncias y demandas en contra de entidades y personas naturales por el incumplimiento de la ley de protección al consumidor, no permite ni está vinculada para realizar la denuncia en econsumer.gov , hecho del cual se desprende entonces que la SIC no ha sabido implementar ni sabe educar a los consumidores en Colombia sobre esta herramienta. Lo que preocupa bastante, en tanto a que se está dejando de lado a múltiples consumidores que día a día realizan compras a entidades transfronterizas. Esto con motivo de la clara falta de conocimiento de los mismos agentes de la SIC que no entienden la importancia de acoger y velar por la protección de los consumidores en Colombia.

2.3. Acuerdos bilaterales y multilaterales

Colombia ha fortalecido su posición en la protección del consumidor mediante la suscripción de Memorandos de Entendimiento (MoU) con diversas agencias homólogas. Un ejemplo reciente es el MoU multilateral firmado en 2023 con la Comisión Federal de Comercio (FTC) de Estados Unidos, el Servicio Nacional del Consumidor (Sernac) de Chile, la Procuraduría Federal del Consumidor (Profeco) de México y el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) de Perú. Este acuerdo, disponible en ftc.gov, marca un hito en la cooperación regional. Anteriormente, Colombia ya había establecido convenios bilaterales, como el firmado con la Agencia Española de Consumo, y otros acuerdos para promover la colaboración técnica con diversos países. En el contexto de la Alianza del Pacífico, que reúne a Colombia, Chile, Perú y México, se han compartido experiencias en protección al consumidor, aunque aún no se ha desarrollado un sistema unificado para gestionar quejas transfronterizas. A nivel global, Colombia participa activamente en la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), contribuyendo a los grupos de expertos en derecho del consumidor, y, desde su ingreso a la OCDE en 2020, colabora en la implementación de las Recomendaciones sobre Comercio Electrónico y Cooperación Transfronteriza.

2.3.1 Participación en redes iberoamericanas y regionales

Además de su presencia en organismos globales como la Red Internacional de Protección al Consumidor (ICPEN, 2020) y Aplicación de la Ley (ICPEN) y la OCDE, Colombia ha consolidado su rol en espacios regionales. En el ámbito de la seguridad de productos de consumo, el país integra la Red de Consumo Seguro de la Organización de los Estados Americanos (OEA), que facilita el intercambio de alertas sobre productos peligrosos. Asimismo, participa en la Red Iberoamericana de Agencias de Protección al Consumidor, un foro que, aunque no cuenta con una estructura legal rígida, permite coordinar políticas públicas y abre la puerta a posibles acuerdos entre países hispanohablantes, promovidos por programas de la Asociación Iberoamericana de Ministerios Públicos (AIAMP) y otras organizaciones.

2.3.2 Limitaciones actuales en la cooperación internacional

A pesar de estos avances, persisten limitaciones significativas. Actualmente, no existe un tratado internacional vinculante que garantice el reconocimiento y ejecución de sanciones o decisiones de agencias de consumo en otros países. Por ejemplo, si la Superintendencia de Industria y Comercio (SIC) impone una multa a un proveedor extranjero, su ejecución fuera de Colombia es compleja, ya que requiere convertir la sanción en una sentencia civil ejecutable internacionalmente, un proceso lento y engorroso. Además, no existe un “tribunal internacional de consumo” para resolver disputas transfronterizas. Frente a esto, expertos proponen avanzar hacia acuerdos de reconocimiento mutuo de decisiones o la creación de sistemas globales de resolución de controversias en línea. La Unión Europea, con su plataforma de Resolución de Disputas en Línea (ODR), ofrece un modelo inspirador. En América Latina, se podría explorar una plataforma ODR regional o fortalecer iniciativas como econsumer, que actualmente funciona como un portal de denuncias, pero no como un mecanismo de mediación efectiva.

3. Retos y Desafíos en la Protección al Consumidor

Aunque econsumer.gov (FTC, 2023) y otras herramientas de colaboración multilateral han sido una herramienta valiosa para enfrentar fraudes en el comercio digital, aún existen desafíos importantes, como:

- imposibilidad o dificultad de sancionar a empresas que operan en el mercado digital sin presencia física en el país afectado: Muchas compañías, especialmente aquellas que participan en actividades fraudulentas o prácticas comerciales poco éticas, estructuran deliberadamente su presencia en línea para evadir la jurisdicción de ciertos países. Al no contar con una sede, activos o representantes legales en el territorio donde ocurre el perjuicio, se complica la aplicación de medidas administrativas o judiciales.

Este vacío legal genera un sentimiento de impunidad que socava la confianza de los consumidores en los sistemas de protección. Incluso cuando se emiten sanciones por parte de las autoridades, la falta de mecanismos eficaces para hacerlas cumplir a nivel internacional reduce su efecto disuasorio. En muchos casos, los países afectados dependen de la voluntad de cooperación del país donde la empresa tiene su base de operaciones, lo cual no siempre se da, especialmente cuando no existen tratados bilaterales de asistencia legal.

- Disparidad entre los marcos normativos de protección al consumidor en las distintas jurisdicciones: Mientras que algunos países han desarrollado legislaciones robustas y actualizadas en materia de comercio electrónico, otros aún carecen de normas específicas para regular este tipo de actividades. Esta asimetría crea brechas que pueden ser aprovechadas por actores malintencionados para establecerse en territorios con regulaciones más laxas o con menor capacidad de fiscalización.

Además, las diferencias en definiciones legales, procedimientos de investigación y niveles de protección reconocidos a los consumidores dificultan la armonización de esfuerzos entre autoridades. Incluso cuando los países están dispuestos a cooperar, las discrepancias jurídicas pueden impedir la realización de investigaciones conjuntas o la ejecución recíproca de sanciones. Esta falta de estandarización pone de

manifiesto la necesidad de impulsar acuerdos multilaterales que permitan un enfoque más coordinado y eficiente.

- Naturaleza dinámica y en constante evolución de los fraudes digitales representa un desafío permanente para los sistemas de protección al consumidor: Los delincuentes se adaptan rápidamente a las nuevas tecnologías, creando métodos cada vez más sofisticados para engañar a los usuarios, desde sitios web falsos que imitan plataformas reconocidas, hasta esquemas complejos de suplantación de identidad y uso indebido de datos personales.

Las autoridades, por su parte, enfrentan la presión de actualizar constantemente sus herramientas de monitoreo, sus estrategias de prevención y sus capacidades técnicas para identificar patrones fraudulentos antes de que causen un daño masivo. Esto requiere no solo inversión en infraestructura tecnológica y capacitación, sino también una colaboración activa entre gobiernos, sector privado y organizaciones de la sociedad civil.

Entendidos los retos, se puede llegar a adoptar mejoras basadas en la experiencia de otras legislaciones más avanzadas en estos asuntos específicos.

3.1 Modelos de protección transfronteriza del consumidor: experiencias internacionales y lecciones para Colombia

La protección de los consumidores en contextos transfronterizos demanda no solo marcos legales nacionales robustos, sino también mecanismos de cooperación internacional, sistemas alternativos de resolución de conflictos y enfoques multilaterales adaptados al comercio digital. A continuación, se analizan tres modelos internacionales —Unión Europea, Estados Unidos y Brasil— cuyas experiencias ofrecen lecciones clave para fortalecer el sistema colombiano de protección al consumidor.

3.1.1 Unión Europea: un modelo integrado de cooperación y prevención

La Unión Europea (UE) ha consolidado uno de los sistemas más avanzados para la protección transfronteriza de los consumidores, garantizando derechos uniformes en todo el bloque, independientemente del país donde se realice una compra.

Instrumentos clave:

- Reglamento ODR (524/2013): Proporciona una plataforma digital gratuita que permite a los consumidores resolver disputas por compras en línea con comerciantes de distintos países de la UE, sin recurrir a tribunales.
- Red ECC-Net (Centros Europeos del Consumidor): Una red de oficinas nacionales que asesora y apoya a los consumidores en reclamaciones transfronterizas, fomentando la mediación.
- Reglamento CPC (2017/2394): Obliga a las autoridades de consumo de los Estados miembros a colaborar en la investigación y sanción de infracciones con impacto transnacional, permitiendo que una autoridad actúe a solicitud de otra. (Gonzales Vaqué)

Desafíos de Colombia y sus entidades en la protección transfronteriza de datos y del comercio electrónico.

3.1.2 Lecciones para Colombia:

- Desarrollar una plataforma nacional de resolución de disputas en línea (ODR) para agilizar la gestión de reclamos por compras electrónicas, tanto nacionales como internacionales.
- Explorar, junto a países aliados como México, Chile y Perú, la creación de una red regional de mediación y protección transfronteriza, inspirada en la ECC-Net.
- Promover reformas normativas que adopten el principio de destino, exigiendo que las empresas extranjeras que comercialicen activamente en Colombia cumplan con las leyes locales de protección al consumidor.

3.1.3. Estados Unidos: cooperación internacional con énfasis en la ejecución

Aunque Estados Unidos no cuenta con una ley federal unificada de protección al consumidor, la Comisión Federal de Comercio (FTC) lidera un sistema basado en una sólida capacidad investigativa y sancionatoria, con un enfoque en la cooperación internacional.

Instrumentos clave:

- SAFE WEB Act: Faculta a la FTC para colaborar con autoridades extranjeras en la investigación de fraudes transfronterizos que afectan a consumidores de otros países.
- econsumer.gov (FTC, 2023): Plataforma multilateral gestionada por la FTC, integrada a la red ICPEN, que recopila quejas sobre comercio electrónico y facilita el intercambio de información entre agencias de consumo.
- Memorandos de Entendimiento (MoU): La FTC ha firmado acuerdos con países latinoamericanos, incluido Colombia, para compartir datos y coordinar investigaciones sobre fraudes transfronterizos.

Lecciones para Colombia:

- Ampliar los acuerdos de cooperación de la Superintendencia de Industria y Comercio (SIC) con autoridades de otros países, incorporando cláusulas operativas para el intercambio de datos y la coordinación de sanciones.
- Fortalecer las capacidades de análisis digital y monitoreo internacional de la SIC para identificar patrones de fraude en el comercio electrónico transfronterizo.
- Publicar informes periódicos sobre fraudes internacionales que afecten a consumidores colombianos, siguiendo el modelo del “Consumer Sentinel Network” de la FTC.

3.2 Brasil: normativa sólida y cooperación regional

Brasil destaca por su robusto marco legal de protección al consumidor, respaldado por el Código de Defensa do Consumidor y reformas recientes que abordan el comercio electrónico y la cooperación regional en el Mercosur.

Instrumentos clave:

- Decreto 10.271/2020 (Mercosur): Exige que los proveedores extranjeros que operen en Brasil cumplan con estándares estrictos de información previa, como identidad, condiciones, precios y políticas de devolución.
- Plataforma consumidor.gov.br: Permite a los consumidores presentar quejas directamente a las empresas, incluidas algunas extranjeras, con la obligación de responder públicamente.
- Acuerdos regionales del Mercosur: La Resolución 37/2019 establece principios comunes para la protección del consumidor en el comercio electrónico entre los Estados miembros.

Lecciones para Colombia:

- Establecer por ley la obligatoriedad de que los proveedores extranjeros que dirijan ofertas al mercado colombiano cuenten con un representante legal en el país, garantizando la exigibilidad de derechos, similar al modelo del GDPR y el decreto brasileño.
- Reformar la Ley 1480 para incluir requisitos mínimos de información precontractual en plataformas extranjeras, como idioma, condiciones de retracto y garantías.
- Promover un marco común de protección al consumidor en el comercio electrónico en el ámbito de la Alianza del Pacífico o la Comunidad Andina, tomando como referencia la experiencia de Brasil en el Mercosur.

4. Conclusiones sobre Protección al Consumidor

El análisis de los retos que Colombia enfrenta en la protección transfronteriza de consumidores y datos personales pone en evidencia desafíos críticos que demandan soluciones urgentes y coordinadas desde los ámbitos normativo, institucional y de cooperación internacional. Estas problemáticas no solo afectan la seguridad de los ciudadanos, sino que también inciden en la confianza hacia un entorno digital en constante expansión.

Uno de los principales obstáculos identificados es la limitada aplicación territorial del Estatuto del Consumidor (Ley 1480 de 2011 (Congreso de la República de Colombia, 2011)). Esta norma, aunque sólida en su diseño, no logra extender su alcance a proveedores extranjeros que carecen de presencia formal en Colombia. Según la Superintendencia de Industria y Comercio (SIC), la ausencia de una sede física o representante legal en el país dificulta la ejecución de sanciones o decisiones contra estas empresas, dejando a los consumidores colombianos en una posición vulnerable. Esta situación es especialmente alarmante si consideramos que el 88% de los adultos en Colombia realiza compras en línea, y un 15% de ellos interactúa con plataformas internacionales como Amazon, AliExpress o Temu. La falta de mecanismos efectivos para garantizar la protección en estas transacciones fomenta una percepción de desamparo que puede erosionar la confianza en el comercio electrónico global.

Para superar estas barreras, Colombia ha buscado integrarse a iniciativas internacionales como la Red Internacional de Protección al Consumidor (ICPEN, 2020) (ICPEN) y la plataforma econsumer.gov (FTC, 2023), que facilitan la denuncia de fraudes transfronterizos y promueven la colaboración entre países. Sin embargo, el impacto de estas herramientas se

Desafíos de Colombia y sus entidades en la protección transfronteriza de datos y del comercio electrónico.

ve limitado por su escasa difusión y el desconocimiento de su uso, incluso entre los propios funcionarios de la SIC, lo que reduce su utilidad para los consumidores.

La experiencia de otros países ofrece valiosas lecciones para Colombia. Modelos como los de la Unión Europea, Estados Unidos y Brasil destacan por el uso de plataformas digitales para la resolución de disputas en línea (ODR), acuerdos bilaterales y regionales que fortalecen la cooperación internacional, y normativas que exigen representación local a empresas extranjeras. Implementar una plataforma nacional de ODR, obligar a las empresas extranjeras a contar con un representante en Colombia y consolidar acuerdos internacionales más operativos podrían ser pasos clave para fortalecer la protección de los consumidores colombianos.

II. Protección de Datos Personales

5. Marco general del régimen colombiano de protección de datos

En un entorno digital caracterizado por una creciente interconexión global, la transferencia de datos personales entre países se ha consolidado como un pilar fundamental para el funcionamiento del comercio electrónico, los servicios en línea y la economía global. Sin embargo, esta dinámica plantea desafíos importantes para los sistemas jurídicos nacionales, especialmente en lo que respecta a la garantía de los derechos de los titulares de la información. En el contexto colombiano, la normativa vigente establece estándares rigurosos para las transferencias internacionales de datos, con el propósito de evitar que la información personal quede expuesta en jurisdicciones que no ofrezcan niveles adecuados de protección.

Consciente de esta necesidad, la Superintendencia de Industria y Comercio (SIC) ha desarrollado mecanismos regulatorios que facilitan estas transferencias, siempre que se realicen hacia países que garanticen un nivel de protección equiparable al exigido por la legislación colombiana. La Circular Externa 005 de 2017, emitida por la Superintendencia de Industria y Comercio (SIC) y recogida en el Capítulo 5 del Título V de la Circular Única, establece una lista de países que cumplen con los estándares de protección de datos personales exigidos por la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012). Esta norma facilita las transferencias internacionales de datos hacia dichas jurisdicciones sin necesidad de autorizaciones previas, ya que sus marcos legales garantizan derechos fundamentales como el acceso, la rectificación, la supresión y la oposición al tratamiento de datos.

Sin embargo, esta lista, aunque es un paso adelante, deja fuera países clave como China, India y Rusia, que no alcanzan los niveles de protección requeridos por Colombia. En particular, China, sede de gigantes del comercio electrónico como AliExpress, Temu y Shein, no es considerado un destino seguro para los datos personales desde la perspectiva colombiana. Estas plataformas recopilan información sensible de usuarios colombianos, como datos de contacto, ubicación, historial de compras y métodos de pago. Según el artículo 26 de la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012), transferir estos datos a China requeriría el consentimiento expreso e informado del titular, una autorización previa de la SIC o una excepción legal, como la ejecución de un contrato en beneficio del usuario.

En la práctica, sin embargo, estas transferencias se realizan sin un control efectivo. Las plataformas mencionadas no suelen solicitar autorizaciones formales, ni hacen uso de las plataformas como el Registro Nacional de Bases de Datos (RNBD) con el fin de cargar las

bases de datos que recopilan de sus clientes en Colombia y la SIC no ha evidenciado una supervisión activa ni ha iniciado procesos relevantes contra ellas relativo al cumplimiento, de las normas de transferencia internacional. Esto revela una brecha significativa entre la regulación y su aplicación real, dejando a los consumidores colombianos en una posición vulnerable. Los datos que entregan a estas empresas, radicadas en jurisdicciones no reguladas, carecen de garantías claras, y el consentimiento que se obtiene en estas plataformas suele ser vago, incumpliendo los requisitos de ser libre, previo, informado y específico que exige la legislación colombiana.

Esta problemática pone de manifiesto una asimetría estructural en la protección de datos. Los consumidores colombianos interactúan con empresas globales sin que existan mecanismos robustos para reclamar o proteger sus derechos ante posibles vulneraciones. Durante el V Congreso Internacional de Protección de Datos Personales de la SIC en 2023, se destacó la necesidad de avanzar en cooperación internacional, supervisión transfronteriza y fortalecimiento institucional, dado el auge del comercio electrónico. Sin embargo, estas intenciones aún no se han concretado en medidas prácticas que aborden los riesgos del tratamiento masivo de datos por parte de empresas extranjeras.

Aunque la Circular 005 y sus posteriores modificaciones, son instrumentos técnicos valiosos, su es limitado sin una implementación efectiva. La SIC debería desarrollar capacidades de fiscalización, incorporar herramientas tecnológicas para rastrear transferencias de datos y articularse con agencias internacionales para garantizar el cumplimiento normativo. Además, sería fundamental establecer protocolos claros para identificar y sancionar transferencias ilegales, así como definir responsabilidades compartidas para empresas que operan en Colombia sin presencia física en el país.

Una vía prometedora sería adoptar mecanismos alternativos, como cláusulas contractuales tipo o normas corporativas vinculantes (BCR), inspirados en el Reglamento General de Protección de Datos (GDPR) europeo, para autorizar ciertas transferencias bajo condiciones estrictas. Asimismo, resulta crucial exigir a las plataformas globales que acceden al mercado colombiano mayor transparencia y adaptación voluntaria a las normas locales. Estas medidas, combinadas con una supervisión más efectiva, podrían fortalecer la protección de los derechos de los consumidores en un contexto digital sin fronteras.

6. Comparación internacional: GDPR y LGPD

Por otro lado es Pertinente el entender como funciona en el resto del mundo. La comparación entre el sistema colombiano de protección de datos personales, basado en la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012) y la Circular Externa 005 de 2017, con marcos regulatorios más avanzados como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y la Lei Geral de Proteção de Dados (LGPD) de Brasil revela diferencias estructurales significativas, especialmente en el ámbito del comercio electrónico y las transferencias internacionales de datos.

El GDPR, vigente desde 2018 tras su aprobación como Reglamento (UE) 2016/679, es ampliamente reconocido como el estándar global más robusto en protección de datos. Por su parte, la LGPD, promulgada en Brasil en 2018 y plenamente vigente desde 2020, se inspira en el modelo europeo. Ambos marcos comparten características clave que los distinguen del sistema colombiano:

Desafíos de Colombia y sus entidades en la protección transfronteriza de datos y del comercio electrónico.

1. Responsabilidad proactiva: Tanto el GDPR (artículos 37-39) como la LGPD (artículo 41) exigen la designación de un Delegado de Protección de Datos (DPO) en organizaciones que manejan datos sensibles o a gran escala. Esta figura supervisa el cumplimiento normativo y actúa como enlace con las autoridades reguladoras, garantizando una gestión interna efectiva de la protección de datos.
2. Derechos digitales avanzados: Ambos regímenes consagran derechos como la portabilidad de datos, el derecho al olvido (supresión) y la protección contra decisiones automatizadas sin intervención humana (artículos 15-22 del GDPR; artículos 17-20 de la LGPD). Estos derechos empoderan a los ciudadanos y refuerzan su control sobre su información personal.
3. Transferencias internacionales: Tanto el GDPR (artículo 45) como la LGPD (artículo 33) prohíben transferencias de datos a países que no ofrezcan un nivel adecuado de protección, salvo que se implementen salvaguardas como las Cláusulas Contractuales Tipo (SCCs) o las Normas Corporativas Vinculantes (BCRs).

Las SCCs son contratos estandarizados, aprobados por la Comisión Europea, que obligan a las empresas fuera del Espacio Económico Europeo (EEE) a cumplir con los estándares del GDPR. Son esenciales para transferencias a países como Estados Unidos, India o China, donde no existe una decisión de adecuación. Sin embargo, su validez depende de que las leyes locales del país receptor no impidan su cumplimiento efectivo. Por otro lado, las BCRs son políticas internas para grupos empresariales multinacionales, aprobadas por las autoridades de protección de datos, que garantizan un estándar uniforme de protección en todas sus filiales, incluso en jurisdicciones no adecuadas. Estas políticas incluyen compromisos jurídicos, auditorías internas y mecanismos de resolución de conflictos, pero requieren un proceso riguroso de aprobación.

En cuanto a la capacidad sancionatoria, el GDPR establece multas de hasta el 4% del volumen de negocios global anual o 20 millones de euros, lo que sea mayor (artículo 83). Casos emblemáticos, como sanciones a Meta, Amazon y Google, demuestran su aplicación efectiva. La LGPD, por su parte, impone sanciones de hasta el 2% de los ingresos en Brasil, con un límite de 50 millones de reales (aproximadamente 10 millones de dólares), además de medidas como la suspensión del tratamiento de datos.

En contraste, el sistema colombiano presenta limitaciones evidentes. La Ley 1581 de 2012 (Congreso de la República de Colombia, 2012) no contempla la figura del DPO ni ha desarrollado herramientas como las SCCs o las BCRs. Aunque el artículo 26 prohíbe transferencias a países sin niveles adecuados de protección y la Circular 005 de 2017 define criterios de adecuación, la falta de un régimen sancionador claro y de mecanismos ágiles de supervisión dificulta el control de los flujos de datos hacia plataformas en jurisdicciones como China, sede de empresas como AliExpress o Shein.

Además, Colombia no cuenta con una autoridad de protección de datos autónoma. La Delegatura para la Protección de Datos Personales, adscrita a la SIC, opera dentro de una entidad con múltiples responsabilidades, lo que contrasta con la independencia de instituciones como la Agência Nacional de Proteção de Dados (ANPD) en Brasil o la CNIL en Francia. Esta falta de autonomía limita la capacidad de fiscalización y respuesta frente a los desafíos del comercio electrónico global.

Si bien Colombia ha avanzado hacia la convergencia con estándares internacionales, aún carece de un sistema robusto de fiscalización y de una cultura organizacional consolidada en materia de cumplimiento. El Proyecto de Ley Estatutaria 152/2024C representa una oportunidad para incorporar herramientas como las SCCs o las BCRs, ya sea como requisitos obligatorios o como opciones voluntarias sujetas a evaluación periódica. Fortalecer la supervisión, promover la cooperación internacional y exigir mayor transparencia a las plataformas globales son pasos esenciales para garantizar una protección efectiva de los datos personales en un contexto digital sin fronteras.

Con el fin de ilustrar las diferencias más importantes entre legislaciones, se tiene la siguiente:

Eje	GDPR (UE)	LGPD (Brasil)	Colombia (Ley 1581 / Proy. 152/2024)
Delegado de Protección de Datos (DPO)	Exigible según riesgo/escala; arts. 37–39.	Figura análoga (encargado) art. 41.	No obligatorio hoy; proyecto fortalece gobernanza.
Base legal del tratamiento	Consentimiento, contrato, obligación legal, interés público, interés legítimo.	Bases similares; énfasis en consentimiento e interés legítimo.	Predomina consentimiento; el proyecto amplía bases y principios.
Transferencias internacionales	Adecuación, SCC, BCR; art. 45+.	Adecuación o garantías contractuales; art. 33.	Lista de países adecuados (Circular 005); faltan SCC/BCR explícitas.

Desafíos de Colombia y sus entidades en la protección transfronteriza de datos y del comercio electrónico.

Sanciones	Hasta 4% facturación global o €20M.	Hasta 2% facturación en Brasil; tope legal.	Hasta 2.000 SMLMV; el proyecto refuerza medidas.
Decisiones automatizadas / IA	Derecho a no ser objeto sin intervención humana; art. 22.	Derechos correlativos; transparencia algorítmica.	Lineamientos generales; el proyecto prevé EIPD y tratamiento de IA.

Tabla 1; Comparativa GDPR, LGPD y ley 1581. Propia análisis legislaciones.

7. Participación de Colombia en acuerdos y estándares internacionales

Colombia ha mostrado un compromiso activo en el ámbito internacional para fortalecer la protección de datos personales. Durante el XIV Encuentro Iberoamericano de Protección de Datos, celebrado en junio de 2016 en Santa Marta, los países miembros de la Red Iberoamericana de Protección de Datos acordaron elaborar los "Estándares de Protección de Datos de los Estados Iberoamericanos". Estos estándares buscan establecer principios y derechos comunes que los Estados Iberoamericanos puedan adoptar en su legislación nacional, facilitando así el flujo de datos personales entre países y promoviendo la cooperación internacional en la materia.

Así mismo en el XXII Encuentro Iberoamericano de Protección de Datos Personales celebrado en Cartagena de Indias, Colombia, el 28 de mayo de 2025), se emitió una carta abierta, en el que se recomienda a las compañías responsables del tratamiento de datos personales de manera masiva o a gran escala instando a éstas a:

“1. Designen a un representante o vocal ante la Autoridad Nacional de Protección de Datos Personales en los términos y condiciones previstos en la legislación de cada uno de los Estados miembros de la Red y, como mínimo, indiquen sus datos de contacto y lo habiliten con los poderes necesarios para realizar a cabalidad funciones de representación judicial y administrativa.

2. Dispongan de un canal de comunicación ágil y efectivo que permita recibir comunicaciones relacionadas con el tratamiento de datos personales, gestionar las solicitudes de los titulares, atender situaciones relacionados con incidentes o vulneraciones de seguridad de datos personales y recibir las notificaciones de las actuaciones administrativas que llevan a cabo las Autoridades Nacionales de Protección de Datos Personales.

3. Creen un canal prioritario (botón de emergencia) accesible para la atención de solicitudes de oposición, en especial, en los casos de publicación de fotografías, videos o audios de contenido sexual o violento cuya difusión ponga en riesgo los derechos y libertades de la persona afectada.

Ahora será importante que estas recomendaciones sean consideradas y debidamente implementadas, y será la obligación de las entidades de control como la SIC el hacer exigible y oponible ante las empresas que actúan dentro de su jurisdicción.

8. Casos emblemáticos de supervisión a multinacionales

La SIC ha ejercido su autoridad para garantizar que las empresas multinacionales que operan en Colombia cumplan con las normativas de protección de datos. A continuación, se detallan algunas de las acciones más destacadas:

8.1 Whatsapp LLC:

Fecha de la orden de la SIC	Mayo de 2021
Empresa involucrada	WhatsApp LLC
Incumplimientos detectados	- Política de Tratamiento de la Información incumplía el 57.89% de los requisitos exigidos por la regulación colombiana. - Incumplimiento del 75% de los requerimientos establecidos en el artículo 12 de la Ley 1581 de 2012.
Órdenes de la SIC	1. Crear una Política de Tratamiento de Información que cumpla con la normativa colombiana y ponerla en conocimiento de los titulares de los datos en el país. 2. Implementar mecanismos efectivos para informar a los usuarios, en idioma castellano, sobre el tratamiento de sus datos personales. 3. Registrar sus bases de datos en el Registro Nacional de Bases de Datos administrado por la SIC.
Cumplimiento posterior verificado	- Se evidencian mejoras en accesibilidad de la política en español desde la app móvil y el sitio web. - La política sigue basada en la normativa de la UE y EE.UU., no en la colombiana. - No hay registro en el RNBD ni de WhatsApp LLC ni de su matriz Meta.
Conclusión	Se evidenció un cumplimiento parcial de lo ordenado por la SIC. No se encontró una actuación o decisión posterior por parte de la autoridad. La SIC no fue lo suficientemente contundente para garantizar el cumplimiento integral de la normativa.

Tabla 2. Whatsapp; Propia extraída de la Resolución No. 29826 de 2021. 19 de mayo de 2021

8.2 TikTok

Aspecto	Descripción
Fecha de la orden de la SIC	Octubre de 2020
Empresas involucradas	ByteDance Ltd., TikTok Inc., TikTok Pte. Ltd.
Incumplimientos detectados	- Política de Tratamiento incumplía el 47.37% de los requisitos exigidos por la regulación colombiana. - No estaba en idioma castellano. - Incumplía el 58.33% de los requisitos sobre información previa a los usuarios.
Órdenes de la SIC	1. Implementar mecanismos efectivos para informar a los usuarios sobre el tratamiento de datos personales. 2. Crear una Política de Tratamiento en idioma castellano que cumpla con la normativa colombiana. 3. Registrar las bases de datos en el Registro Nacional de Bases de Datos (RNBD). 4. Presentar pruebas de la autorización previa, expresa e informada de los representantes legales de los menores de edad cuyos datos sean recolectados o tratados.
Cumplimiento posterior verificado	- Se puede cambiar el idioma de la política de privacidad al español. - La política cumple en su mayoría con la normatividad, pero persisten fallas. - En el RNBD solo aparecen registros de empleados y proveedores, no de usuarios. - No hay pruebas de autorización previa de padres de menores; aunque hay una sección de política para menores, esta está en inglés.
Conclusión	Se evidenció un cumplimiento parcial de lo ordenado por la SIC. No se encontró una actuación o decisión posterior por parte de la autoridad. La SIC no fue lo suficientemente contundente para garantizar el cumplimiento integral de la normativa.

Tabla 3. Tik Tok; Propia extraída de la Resolución No. 62132 de 2020. 5 de octubre de 2020

8.3. Facebook Colombia S.A.S.

Aspecto	Descripción
Fecha de la decisión de la SIC	Agosto de 2022
Entidad involucrada	Facebook Colombia S.A.S.
Determinación principal	Facebook Colombia S.A.S. fue considerada corresponsable del tratamiento de datos personales de los usuarios de Meta en Colombia.
Base de la decisión	Vínculos jurídicos y económicos con Facebook Global Holding II, LLC y Meta Platforms Inc., y participación en el tratamiento de datos personales mediante la plataforma.
Contexto del tratamiento de datos	El tratamiento de datos se realiza bajo la estrategia global de Meta Platforms Inc. para recolectar y aprovechar información con fines publicitarios.
Órdenes de la SIC y consecuencias del incumplimiento	La SIC emitió órdenes a todas las entidades mencionadas, indicando que el incumplimiento podría acarrear sanciones como multas de hasta 2,000 SMMLV o suspensión de actividades en Colombia.
Cumplimiento verificado	No se encontró evidencia del cumplimiento por parte de las entidades extranjeras ni de que la SIC hubiese impuesto sanciones o hecho exigibles sus órdenes.
Consulta adicional a la SIC	Se realizó una consulta directa a la SIC sobre el estado de cumplimiento de las órdenes emitidas contra WhatsApp LLC, ByteDance Ltd (TikTok), Facebook Colombia S.A.S. y Zoom Video Communications, Inc.

Tabla 4. Facebook; Propia extraída de la Resolución No. 53593 de 2020. 3 de septiembre de 2020

Ante la verificación previa de cumplimiento realizada, se decidió consultar a través de un derecho de petición a la SIC, la respuesta se dio mediante oficio con Radicado: 25-192506, aclarando que desde 2018 hasta la fecha se han emitido cuatro órdenes administrativas específicas contra estas compañías, debido a vulneraciones identificadas al régimen de protección de datos personales (Ley 1581 de 2012 (Congreso de la República de Colombia, 2012):

8.4 Respuesta de la SIC a la situación

Empresa	Resolución / Año	Órdenes principales (según texto)	Estado/seguimiento (según texto)
Zoom Video Communications, Inc.	RE-74519 (2020)	Ajustes de políticas; información clara; registro RNBD conforme Ley 1581.	Seguimiento en curso; sin evidencia pública concluyente.
WhatsApp LLC	RE-29826 (2021)	Política en español; información efectiva a usuarios; registro RNBD.	Seguimiento en curso; sin evidencia pública concluyente.
TikTok (ByteDance)	RE-62132 (2020/2023)	Información clara; política en español; autorización de menores; registro RNBD.	Cumplimiento parcial/pendiente; seguimiento en curso.
Facebook Colombia S.A.S.	RE-46342 (2023)	Corresponsabilidad; adecuación del tratamiento; medidas de cumplimiento.	Sin confirmación pública de cierre; seguimiento en curso.

Tabla 5 Respuesta SIC; Propia extraída de la respuesta en el Radicado: 25-192506

En la misma respuesta oficial, la SIC indicó expresamente que actualmente no es posible confirmar si estas órdenes han sido cumplidas plenamente, debido a que los procedimientos internos de evaluación y verificación aún están en desarrollo. En consecuencia, no se han impuesto sanciones ni se han determinado consecuencias administrativas definitivas a ninguna de las entidades mencionadas.

La SIC también aclaró cómo realiza el seguimiento a estas órdenes mediante procedimientos específicos establecidos en el documento interno denominado “Procedimiento de Investigaciones sobre Posibles Violaciones a las Normas sobre Protección de Datos Personales”. Dichos procedimientos incluyen:

1. Recepción y revisión inicial: Verificación documental tras el vencimiento del plazo para el cumplimiento.
2. Determinación del estado de cumplimiento:
 - Si está completo, se emite un "Informe de cumplimiento" y se concluye el caso.
 - Si está incompleto, se realizan solicitudes adicionales o eventualmente se procede a formulación de cargos.
 - Si requiere análisis técnico especializado (peritaje), se solicita y, de encontrarse incumplimiento, se avanza hacia formulación de cargos.
3. Uso del Registro Nacional de Bases de Datos (RNBD): Se valida directamente el cumplimiento mediante la carga y registro de información requerida en el RNBD.
4. No presentación de soportes: Implica la preparación inmediata para la formulación de cargos.
5. Apertura formal de expediente: En caso de incumplimiento reiterado o confirmado, se abre un nuevo expediente para iniciar un proceso sancionatorio formal.

La información solicitada específicamente sobre avances detallados o documentos preliminares no fue entregada, al considerarse como "documentos en construcción" bajo las excepciones establecidas en la Ley 1712 de 2014 sobre transparencia y acceso a información pública.

La respuesta recibida por parte de la SIC permite concluir preliminarmente que, si bien existen procedimientos claros de seguimiento, en la práctica aún no hay evidencia pública concluyente sobre la efectividad del cumplimiento por parte de estas multinacionales. Esta falta de conclusiones oficiales plantea interrogantes críticos sobre la eficacia real de la SIC en hacer cumplir sus decisiones en contextos transfronterizos y refuerza la necesidad de reformas normativas y mecanismos internacionales más sólidos.

9.Retos Protección de datos

A pesar de contar con un sólido marco legal a través de la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012), Colombia enfrenta varios desafíos para garantizar la

Desafíos de Colombia y sus entidades en la protección transfronteriza de datos y del comercio electrónico.

protección efectiva de los datos personales en contextos transfronterizos. Uno de los principales retos radica en la ausencia de mecanismos coercitivos extraterritoriales. Si bien la SIC ha emitido órdenes contra entidades internacionales como WhatsApp, TikTok y Facebook, aún no existe evidencia concreta de un cumplimiento sustancial de estas órdenes, lo que demuestra la limitada capacidad sancionadora de la SIC sobre actores internacionales.

Otro desafío importante es la falta de cumplimiento y coerción suficiente sobre la lista pública de países con un nivel adecuado de protección de datos ya que empresas de países que no están dentro de la lista parecen estar operando en Colombia sin la suficiente supervisión o cumplimiento de la normatividad Nacional, lo que genera inseguridad jurídica para las empresas que necesitan realizar transferencias internacionales. Esto ha impulsado la creación de un proyecto de resolución por parte de la SIC destinado a definir los criterios de idoneidad y las condiciones para la emisión de declaraciones de conformidad, aunque su implementación sigue pendiente.

La brecha tecnológica es también un albur. La SIC tiene que fortalecer su infraestructura de vigilancia digital y análisis de big data para poder detectar, investigar y sancionar eficazmente el uso indebido de datos personales. El ritmo acelerado de la innovación tecnológica, mediante herramientas como inteligencia artificial, IoT y blockchain, plantea cuestiones sobre la aplicabilidad de las normas vigentes, requiriendo una interpretación dinámica del marco normativo vigente. De la misma manera, se deben destinar más recursos a la verificación del cumplimiento de las órdenes impartidas, ya que es preocupante el hecho de que las órdenes impartidas que ya algunas tienen más de cinco años de haberse divulgado, no solo no se han cumplido, sino que la SIC no ha seguido con el proceso sancionatorio ni investigativo, como si las órdenes impartidas solo hubiesen sido una declaración de intención más que una obligación real para las entidades extranjeras.

10. Análisis del Proyecto de Ley Estatutaria 152 de 2024: Reforma al Régimen de Protección de Datos Personales en Colombia

En respuesta a los desafíos derivados de la evolución del entorno digital y las crecientes exigencias internacionales en materia de protección de datos, el Congreso de la República de Colombia tramita el Proyecto de Ley Estatutaria 152 de 2024 Cámara, orientado a reformar de manera integral el régimen general de protección de datos personales. Esta iniciativa busca actualizar la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012), cuya obsolescencia resulta evidente ante las nuevas dinámicas tecnológicas y comerciales que caracterizan el ecosistema digital.

10.1 Principales Disposiciones del Proyecto

1. Reforma integral del marco normativo: El proyecto propone la derogación expresa de la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012), consolidando un nuevo marco normativo que regula de manera integral el tratamiento de datos personales en Colombia, adaptándolo a los estándares contemporáneos.

2. Ampliación de derechos de los titulares: Se introducen nuevos derechos alineados con estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) europeo, entre los que destacan:
 - Portabilidad de datos (Art. 17), que permite a los titulares transferir sus datos entre responsables del tratamiento.
 - Derecho de oposición (Art. 18) y limitación del tratamiento (Art. 19), que otorgan mayor control sobre el uso de la información personal.
 - Prohibición de decisiones automatizadas sin intervención humana (Art. 20), garantizando una revisión humana en procesos algorítmicos significativos.
3. Evaluaciones de Impacto en Protección de Datos (EIPD): Se establece la obligación de realizar evaluaciones de impacto para tratamientos de datos que impliquen alto riesgo (Art. 31), promoviendo el principio de responsabilidad demostrada y una cultura de prevención en la gestión de datos.
4. Fortalecimiento de la autoridad de control: Sin crear una autoridad autónoma especializada, el proyecto amplía las competencias de la Superintendencia de Industria y Comercio (SIC), otorgándole facultades de inspección in situ, acceso a sistemas, medidas cautelares y la capacidad de ordenar la suspensión o cese de tratamientos de datos (Capítulo VII).
5. Adaptación a tecnologías emergentes: El proyecto aborda explícitamente el uso de tecnologías como inteligencia artificial, big data, biometría y decisiones algorítmicas, estableciendo principios específicos para garantizar su regulación adecuada (Art. 2, párrafos).
6. Régimen sancionatorio reforzado: Se introduce un esquema de sanciones más detallado, incluyendo medidas correctivas, económicas y preventivas (Art. 54 y siguientes). Las multas pueden alcanzar hasta 2.000 salarios mínimos legales mensuales vigentes, considerando criterios como proporcionalidad, reincidencia y prevención, aunque no se adopta un modelo basado en ingresos globales como el GDPR.
7. Transferencias internacionales de datos: Se regulan las transferencias de datos a terceros países, exigiendo garantías de un nivel adecuado de protección (Arts. 48 a 50). No obstante, el proyecto no desarrolla instrumentos como Cláusulas Contractuales Tipo (SCC) o Normas Corporativas Vinculantes (BCR), lo que representa una limitación para una convergencia plena con el modelo europeo.

10.2 Implicaciones y Relevancia

El Proyecto de Ley 152 de 2024 constituye un avance significativo hacia la armonización del régimen colombiano de protección de datos con estándares internacionales. Aunque no alcanza el nivel de robustez institucional del GDPR, particularmente en la ausencia de una autoridad independiente o un sistema de certificaciones, fortalece el marco normativo existente y promueve mayor seguridad jurídica en entornos digitales transfronterizos. Su implementación podría consolidar la posición de Colombia en el contexto internacional,

beneficiando tanto a los titulares de datos como a las organizaciones que operan en el ámbito digital.

11. Conclusiones sobre Protección de Datos

En el ámbito de la protección de datos personales, los desafíos son igualmente significativos. Aunque la Ley Estatutaria 1581 de 2012 y la Circular Externa 005 de 2017 establecen un marco legal sólido, su aplicación resulta insuficiente frente a plataformas internacionales que manejan datos sensibles sin cumplir con estándares adecuados de protección. Empresas como AliExpress, Temu o Shein recopilan información personal de usuarios colombianos sin una supervisión efectiva por parte de la SIC ni un consentimiento claro, como lo exige la normativa. Al comparar el marco colombiano con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea o la Lei Geral de Proteção de Dados (LGPD) de Brasil, se evidencia la ausencia de herramientas clave, como la figura del Delegado de Protección de Datos (DPO) o mecanismos como las Cláusulas Contractuales Tipo (SCCs) y las Normas Corporativas Vinculantes (BCRs), esenciales para garantizar la seguridad de los datos en contextos transfronterizos.

El Proyecto de Ley Estatutaria 152 de 2024 representa una oportunidad crucial para modernizar el régimen de protección de datos en Colombia. Esta iniciativa propone fortalecer los derechos digitales, introducir evaluaciones de impacto obligatorias para tratamientos de alto riesgo y establecer un sistema de sanciones más robusto. No obstante, persisten desafíos pendientes, como la necesidad de otorgar mayor autonomía a la autoridad de protección de datos y desarrollar instrumentos específicos para gestionar transferencias internacionales de datos, elementos fundamentales para una protección efectiva en un mundo interconectado.

Sin embargo al momento de publicación del presente artículo de opinión, el Proyecto de Ley Estatutaria 152 de 2024, fue archivado por el 19 de junio de 2025, por vencimiento de términos, sin embargo se espera que para el inicio de la nueva legislatura de 2025, se vuelva a radicar con el fin de darle el trámite pertinente.

En síntesis, Colombia enfrenta retos complejos en la protección transfronteriza de consumidores y datos personales, derivados de limitaciones normativas, una cooperación internacional aún insuficiente y una supervisión limitada. Avanzar hacia la adopción de mejores prácticas internacionales, la creación de plataformas especializadas para resolver conflictos, el fortalecimiento de acuerdos globales y una actualización normativa integral son pasos urgentes y necesarios para garantizar la seguridad y confianza de los ciudadanos colombianos en un entorno digital globalizado.

REFERENCIAS

Brasil. Decreto No. 10.271, de 6 de marzo de 2020. Diário Oficial da União, 6 de marzo de 2020.

Brasil. Lei No. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Diário Oficial da União, 15 de agosto de 2018.

Comisión Europea. Decisión de Ejecución relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el artículo 28, apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y en el artículo 29, apartado 7, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo. Diario Oficial de la Unión Europea, L 419, 10 de diciembre de 2021.

Congreso de la República de Colombia. Ley 1480 de 2011. Diario Oficial No. 48.220, 12 de octubre de 2011.

Congreso de la República de Colombia. Ley Estatutaria 1581 de 2012. Diario Oficial No. 48.587, 18 de octubre de 2012.

González Vaqué, Luis. “Modificación del régimen de la cooperación en materia de protección de los consumidores: el Reglamento (UE) 2017/2394 de 12 de diciembre de 2017.” La Ley Unión Europea, no. 57 (2018). ISSN-e 2255-551X.

Higuera-Arias, J. Las debilidades en materia de protección de datos personales en la regulación emitida por el Estado colombiano. Bogotá: Universidad Católica de Colombia, 2021.

MdE Multilateral para la Cooperación Transfronteriza en la Protección al Consumidor. Memorando de Entendimiento Multilateral sobre la Cooperación en Materia de Cumplimiento Normativo entre las Autoridades de Protección al Consumidor de Chile, Colombia, México, Perú y la Comisión Federal de Comercio de los Estados Unidos de América. 2023.

MERCOSUR. Resolución GMC No. 37/19 – Guía de Buenas Prácticas en Protección al Consumidor en el Comercio Electrónico. Montevideo: Grupo Mercado Común, 2019.

Monsalve Caballero, Vladimir. “La protección de datos de carácter personal en los contratos electrónicos con consumidores: Análisis de la legislación colombiana y de los principales referentes europeos.” Prolegómenos 20, no. 39 (2017): 163–195.

OCDE. Directrices para la protección de los consumidores de prácticas comerciales transfronterizas fraudulentas y engañosas. París: OCDE, 2003.

Desafíos de Colombia y sus entidades en la protección transfronteriza de datos y del comercio electrónico.

Red Iberoamericana de Protección de Datos (RIPD). Carta Abierta a las Compañías Responsables del Tratamiento de Datos Personales de Manera Masiva o a Gran Escala. Aprobada en el XXII Encuentro Iberoamericano de Protección de Datos Personales, Cartagena de Indias, Colombia, 28 de mayo de 2025.

Red Iberoamericana de Protección de Datos (RIPD). Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Ciudad de México: RIPD, 2017.

Rincón, Erick. Derecho del Comercio Electrónico. Valencia: Tirant lo Blanch, 2018.

Rojas-Bejarano, M. “Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.” *Novum Jus* 8, no. 1 (2014): 107–139.

Rodríguez Carrión, José Luis. La responsabilidad civil por los daños causados por productos defectuosos. Bogotá: Revista General de Derecho, Universidad Externado de Colombia, 2000.

Ruiz Nieto, Santiago. “La mediación como defensa del consumidor electrónico. Llamado al proceso ejecutivo simplificado.” *Revista de Derecho*, no. 60 (2023): 9–28.

Superintendencia de Industria y Comercio (SIC). Circular Externa No. 005 de 2017. Bogotá: SIC, 2017.

Superintendencia de Industria y Comercio. Resolución No. 29826 de 2021. 19 de mayo de 2021.

Superintendencia de Industria y Comercio. Resolución No. 74519 de 2020. 23 de noviembre de 2020.

Superintendencia de Industria y Comercio. Resolución No. 62132 de 2020. 5 de octubre de 2020.

Superintendencia de Industria y Comercio. Resolución No. 53593 de 2020. 3 de septiembre de 2020.

Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento

de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, L 119, 4 de mayo de 2016.

Unión Europea. Reglamento (UE) n.º 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n.º 2006/2004 y la Directiva 2009/22/CE (Reglamento sobre resolución de litigios en línea en materia de consumo). Diario Oficial de la Unión Europea, L 165, 18 de junio de 2013.

Velandia, Mauricio. Derecho de la Competencia y del Consumo. Bogotá: Universidad Externado de Colombia, 2020.