Protección de datos en el comercio electrónico: Análisis comparado y perspectivas para la regulación en Venezuela

Víctor Corredor*
Valeria Ramos**
RVDM, nro. XV, 2025, pp. 413-430

Resumen: El presente artículo analiza el crecimiento exponencial del comercio electrónico en Venezuela y la marcada ausencia de un marco legislativo específico que regule la protección de datos personales en este entorno. A través de una metodología de derecho comparado, se examinan los estándares normativos de Colombia, Argentina y Chile para evidenciar el rezago del ordenamiento jurídico venezolano, el cual se sustenta precariamente en principios constitucionales y en la acción de Habeas Data, resultando insuficiente ante los desafíos del comercio electrónico. El estudio concluye que, ante el vacío legal y la inseguridad jurídica resultante que desincentiva la inversión y vulnera al consumidor, la autorregulación corporativa (*compliance*) se presenta como el mecanismo idóneo y necesario.

Palabras clave: protección de datos, comercio electrónico, consumidor, autorregulación, compliance, derecho comparado.

Data protection in electronic commerce: Comparative analysis and regulatory perspectives for Venezuela

Abstract: *This article analyzes the exponential growth of e-commerce in Venezuela and the marked absence of a specific legislative framework regulating personal data protection within this environment. Through a comparative law methodology, the regulatory standards of Colombia, Argentina, and Chile are examined to highlight the lag in the Venezuelan legal system, which relies precariously on constitutional principles and the Habeas Data action, proving insufficient for the challenges of electronic commerce. The study concludes that, faced with the legal void and resulting legal uncertainty that discourages investment and leaves consumers vulnerable, corporate self-regulation (compliance) emerges as the ideal and necessary mechanism.*

Keywords: *data protection, e-commerce, consumer, self-regulation, compliance, comparative law.*

Recibido: 23/11/2025
Aprobado: 25/11/2025

* Abogado, Universidad Católica Andres Bello, 2023. Especialización de Derecho Mercantil de la Universidad Central de Venezuela. Email: abgvictorcorredor@gmail.com

** Abogado, Universidad Católica Andres Bello, 2023. Especialización de Derecho Mercantil de la Universidad Central de Venezuela. Email: Valramoss17@gmail.com

Protección de datos en el comercio electrónico: Análisis comparado y perspectivas para la regulación en Venezuela

Víctor Corredor*
Valeria Ramos**
RVDM, nro. XV, 2025, pp. 413-430

SUMARIO:

INTRODUCCIÓN

El comercio internacional ha evolucionado. Para los consumidores no es un fenómeno desconocido y para las empresas, la internacionalización no representa su mayor reto. El comercio se ha expandido a nivel mundial, reflejando su crecimiento dentro de las plataformas tecnológicas, contenidos digitales, medios de pagos, entre otras. En palabras de Luis Cova Arria, podríamos expresarlo de la siguiente manera: "El Comercio Electrónico constituye una nueva forma de efectuar una de las actividades más antiguas de la Humanidad: el comercio; el intercambio de bienes o servicios. La electrónica y sus instrumentos, vienen cada día sustituyendo de una manera más generalizada a la voz y al papel, clásicos medios de apoyo para la emisión y recepción de voluntades negociales y sus secuelas jurídicas y empresariales."[1]

Cada año, los servicios de informática y/o tecnología, obtienen más demanda. En países como Estados Unidos, se ha visualizado un crecimiento del 12% en este mercado, con una capitalización de mercado de más de un billón de dólares. En otros países como Perú, Brasil, Indonesia o Egipto; el crecimiento ha sido significativo y se ha permitido la exportación de estos servicios[2]. En Venezuela, según fuentes guberna-

---

* Abogado, Universidad Católica Andres Bello, 2023. Especialización de Derecho Mercantil de la Universidad Central de Venezuela. Email: abgvictorcorredor@gmail.com

** Abogado, Universidad Católica Andres Bello, 2023. Especialización de Derecho Mercantil de la Universidad Central de Venezuela. Email: Valramoss17@gmail.com

1 Luis Cova Arria, «Problemas legales del comercio electrónico y los obstáculos para la implementación de la Ley Modelo de la CNUDMI sobre el comercio electrónico», *Revista Venezolana de Derecho Mercantil*, n.º 11, acceso el 22 de noviembre de 2025, http://www.ulpiano.org.ve/revistas/bases/artic/texto/RVDM/11/RVDM_2023_11_23-54.pdf.

2 Organización Mundial del Comercio, *Perspectivas del Comercio Mundial y estadísticas* (Ginebra: OMC, abril de 2025), acceso el 22 de noviembre de 2025, https://www.wto.org/spanish/ress/booksp_s/trade_outlook25_s.pdf.

mentales, el comercio electrónico tuvo un crecimiento del noventa y siete por ciento (97%) en el año 2024[3], además de esto, organizaciones como VenaCham expresan que las plataforma tecnológicas enfocadas en los pagos en línea, servicios de entrega y transporte protagonizan el mercado venezolano y pudiera incrementar hasta un ciento por ciento (100%) su crecimiento[4].

Sin embargo, este crecimiento exponencial no solo representa aspectos positivos para la economía, también representa riesgos, vulneraciones, posibles violaciones de derechos de los consumidores y actividades, las cuales podrían ser reguladas. A día de hoy, la mayoría de los países han legislado en materia de comercio electrónico, intermediarios de internet, plataformas de pago, delitos informáticos, entre otras; con especial énfasis en un aspecto fundamental para la sociedad, el mercado y el consumidor, como lo son los datos personales.

A pesar de la actual legislación en la región, nuestro país se ha quedado estancado en principios constitucionales, la ley de delitos informáticos, algunas resoluciones de entes reguladores y una visión limitada de la protección de datos a través del hábeas data. Hoy día existe la necesidad de sancionar una ley en materia de comercio electrónico y protección de datos que extienda la esfera de derechos de los ciudadanos y el uso de forma adecuada de los datos personales por cualquier persona natural o jurídica que ejerza actos de comercio de forma electrónica.

La base fundamental para esta regulación es el artículo 60 de la Constitución Nacional, el cual expresa: "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos."[5]

En realidad, esto no resulta suficiente, el comercio electrónico en Venezuela se ha visto invadido de problemas de ciberseguridad, bases de datos expuestas, y violaciones al derecho a la propia imagen, confidencialidad, entre otros. Como ejemplo de esto podemos visualizar el caso de secuestro de datos que sufrió la compañía Digitel, en el cual se vulneraron datos de usuarios de la empresa, aliados comerciales y proveedores[6]. Asimismo, destaca el caso más conocido por los consumidores de plataformas

---

[3] Ministerio de Economía y Finanzas, «Comercio electrónico en el país se incrementó un 97% en el 2024», acceso el 22 de noviembre de 2025, https://www.mppef.gob.ve/comercio-electronico-en-el-pais-se-incremento-un-97-en-el-2024/.

[4] MDS Telecom, «Estiman crecimiento superior a 100% del e-commerce en Venezuela», *MDS Telecom News*, acceso el 22 de noviembre de 2025.

[5] *Constitución de la República Bolivariana de Venezuela*, Gaceta Oficial Extraordinaria n.º 36.860, 30 de diciembre de 1999, art. 60, https://www.oas.org/dil/esp/constitucion_venezuela.pdf.

[6] Asilo Digital, «Hackeo a Digitel en 2024: Todo lo que necesitas saber», *Asilo Digital*, acceso el 22 de noviembre de 2025, https://www.asilodigital.com/que-esta-pasando-con-digitel/.

tecnológicas de pago o de telefonías móviles de "María", una modalidad de phishing que se ha implementado en el país desde un tiempo hasta el día de hoy, que ha afectado en gran parte a la sociedad[7].

Los datos personales, se encuentran reflejados en el día a día a través de aplicaciones móviles, centros comerciales, navegadores de internet, telefonía, medios de pago, o cualquier otro servicio prestado a través de la informática o tecnología, las cuales pueden registran nuestra geolocalización, imagen, audio, video o cualquier otro tipo de dato que pueda vulnerar nuestra intimidad.

Todas estas situaciones hacen preguntarse a los consumidores sí ¿El comercio electrónico en Venezuela, es suficientemente seguro? ¿Qué medidas se implementan para proteger mis datos personales? ¿Cuál es la responsabilidad de las empresas prestadores de servicios en caso de una violación a mis derechos? ¿Las empresas prestadoras de servicio están obligadas a proteger los datos de los usuarios y/o consumidores? ¿La autorregulación es la clave para las empresas prestadores de servicio?

1. ¿Qué son los datos?

En la actualidad, son escasas las empresas que no participan en el ecosistema digital, esta realidad ha generado nuevas necesidades, esto quiere decir, que realizan sus ventas a través de plataformas de internet, guardan información en la nube, requieren proveedores de software, etcétera, esto a su vez ha creado nuevas necesidades, dos de ellas, que consideramos primordiales son: 1) la necesidad de proteger al consumidor, en el sentido de la protección de sus datos y 2) la necesidad de que las empresas tengan seguridad jurídica al momento de operar en un territorio, de cuáles son los parámetros que deben seguir para la protección de los datos del consumidor.

Atendiendo lo planteado anteriormente, es necesario precisar qué se entiende por "datos" y por "datos personales", en virtud de que ellos juegan un papel fundamental al momento de la protección del consumidor, ahora bien, en general los datos pueden ser representaciones numéricas, textuales, audiovisuales, o de cualquier otra naturaleza, capaz de describir hechos, circunstancias, características, que pueden ser almacenados, procesados y capaz de transmitirse por medios electrónicos o físicos, la Ley contra delitos informáticos en el artículo 3, apartado C sobre Data (datos) nos indica que podemos entender por datos a la luz del ordenamiento jurídico Venezolano y lo define como hechos, conceptos, instrucciones o caracteres representados de una manera apropiada

[7] Blog Jurídicos Venezuela, «"Hola, soy María y cambié de número": Modus operandi para extorsionar», acceso el 22 de noviembre de 2025, https://blog.juridicosvenezuela.com/hola-soy-maria-y-cambie-de-numero-modus-operandi-para-extorsionar/.

para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado[8].

Por otra parte, cuando nos referimos a datos que identifican a una persona, sea directa o indirectamente, hablamos de datos personales, y aquí entra en juego derechos fundamentales como el derecho a la privacidad el cual el Doctor Alvaro Badell lo define como un derecho fundamental, autónomo e independiente, de primera generación que es desarrollado en Venezuela en el artículo 60 de la Constitución, que ampara directamente el derecho que tiene toda persona a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación[9], por su parte la Comisión Europea en su Reglamento 2016/679 lo define como toda la información sobre una persona física identificada o identificable («el interesado»); y su vez se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona[10].

No obstante, de las definiciones citadas podemos extraer que la protección de datos personales es el derecho que tiene toda persona a que la información que lo identifica o lo puede llegar a identificar sea protegida de manera adecuada, y hay que tener en cuenta que es un derecho autónomo que comprende la facultad de los ciudadano de disponer sobre sus datos personales, de modo que en base a su consentimiento puedan controlarlos, y en consecuencia, decidir sobre ellos, sin que puedan ser objetos de divulgación o acceso por parte de terceros, sin su autorización o la previsión legal correspondiente[11].

Cabe señalar, que la Constitución de la República Bolivariana de Venezuela (en lo sucesivo la Constitución) contempla la garantía habeas data, la cual está dirigida a proteger el derecho de protección de datos ante cualquier vulneración, esta misma se encuentra en el artículo 28, y establece que:

---

8 *Ley Especial contra los Delitos Informáticos*, Gaceta Oficial n.º 37.313, 30 de octubre de 2001, art. 3, https://www.asambleanacional.gob.ve/storage/documentos/leves/ley-especi-20220309131245.pdf.

9 Rafael Badell Madrid, «El derecho constitucional a la privacidad y su conflicto con los derechos intelectuales», *Revista de Propiedad Intelectual*, n.º 19 (2016): 141-63, http://www.ulpiano.org.ve/revistas/bases/artic/texto/RPI/19/rpi_2016_19_141-163.pdf

10 Parlamento Europeo y Consejo de la Unión Europea, *Reglamento (UE) 2016/679 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*, DO L 119 de 4.5.2016, acceso el 22 de noviembre de 2025, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679.

11 Badell Madrid, «El derecho constitucional a la privacidad», 145.

> *"Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley."*[12]

Cabe resaltar, que en el artículo 60 de la Constitución, en su último párrafo se indica que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos"[13], es decir, el ordenamiento jurídico Venezolano no solo, de alguna forma, reconoce el derecho que tienen las personas a que sus datos sean protegidos y utilizados de manera adecuada, sino que además establece un mandato constitucional de que a través de la Ley se establezcan los mecanismos, parámetros, para protegerlo.

1.1. Utilización de los datos en el comercio ¿electrónico?

El comercio electrónico tiene ciertas particularidades que lo diferencian del comercio que conocemos tradicionalmente, siendo que este contempla un nuevo desafío para los mercados económicos y sus participantes bien en calidad de oferentes o demandantes[14], una de esas particulares, es que en el momento en que el consumidor realizar una compra de un producto o suscribir un servicio, necesariamente tiene que registrarse en su página web, lo que conocemos hoy en día como "tiendas en línea" y proporcionar sus datos como nombre y apellido, no obstante, hay tiendas en línea, en donde eso no basta, sino que además hay que proporcionar otro tipo de información como: número de pasaporte o cédula de identidad, dirección de casa, dirección de envío (si aplica), número de teléfono, dirección de correo, y en algunos casos pueden llegar a solicitar el nombre de usuario en redes sociales, como podemos observar, recopilan una serie de información delicada sobre la identificación de una persona, que incluso estimamos puede llegar a traspasar el derecho a su vida privada.

Asimismo, el comercio electrónico puede darse a través de aplicaciones, como *WhatsApp*, sin necesidad de tener que registrarse en una página web, cabe señalar que este, ha creado su versión *business* para mayor comodidad de las empresas o personas

---

[12] *Constitución de la República Bolivariana de Venezuela*, art. 28.

[13] *Constitución de la República Bolivariana de Venezuela*, art. 60..

[14] Mariana del Valle Buitrago Rodríguez, «El comercio electrónico y la actividad comercial digital en el Derecho Venezolano», *Revista Hacer y Saber* (2014), acceso el 22 de noviembre de 2025, http://erevistas.saber.ula.ve/index.php/hacerysaber/article/download/19835/21921931474.

que quieran vender u ofrecer sus servicios. En esta modalidad, normalmente, se exige proporcionar menos datos personales, a diferencia de tener que registrarse en una página web, sin embargo, no minimiza el riesgo de fuga y la posibilidad de transferencia o transacción de datos personales.

Ahora bien, el comercio electrónico nos ha facilitado la forma en que adquirimos productos o suscribimos servicios, en virtud de que ya no tenemos que salir de nuestra casa u oficina para, por ejemplo, realizar una compra o realizar el pago de la mensualidad de un servicio, sin embargo, es necesario plantearse las siguientes incógnitas: 1) ¿Qué uso le dan las empresas y/o personas a esos datos recopilados?; 2) ¿Hasta dónde puede llegar ese uso de los datos personales que recopilan?; y 3) ¿Por cuánto tiempo pueden mantener esa información? Recordamos que con la protección de los datos personales se busca garantizar la privacidad de las personas, el resguardo o protección de su intimidad; lo cual supone, fundamentalmente, la posibilidad real de controlar el uso y la finalidad para la cual se destina la información relativa a los datos personales de cada individuo, y la facultad de oponerse a su utilización, de manera tal de impedir que esa información sirva propósitos no aceptados por su titular[15].

En razón a lo planteado anteriormente, resulta necesario que cuando las empresas y/o personas utilicen las plataformas digitales para ofrecer sus productos y servicios, adopten mecanismos de transparencia que le permitan al consumidor conocer, de manera clara y precisa, cuáles datos se recopilan, con qué propósito, si serán compartidos con terceros previa autorización del consumidor y qué herramientas tiene el a su alcance para ejercer sus derechos de acceso, rectificación, oposición y supresión de los datos proporcionados.

Finalmente, esto constata que la ausencia de una ley de protección de datos personales en Venezuela no solo afecta a los consumidores, sino también a las propias empresas y/o personas que ofrecen sus productos y servicios, porque se encuentran en una incertidumbre jurídica al no saber si por desconocimiento han llegado a vulnerar los derechos del consumidor en ese aspecto o si su actuación en el comercio electrónico cumple estándares internacionales como por ejemplo las directrices de la OCDE en materia de protección de datos personales, lo cual puede limitarlos a expandirse internacionalmente.

---

[15] Emercio José Aponte Núñez, «La importancia de la protección de datos de carácter personal en las relaciones comerciales», *Revista de Derecho Privado*, Universidad Externado de Colombia, acceso el 22 de noviembre de 2025, https://revistas.uexternado.edu.co/index.php/derpri/article/view/561/531.

2. Derecho Comparado

La legislación venezolana, no cuenta con una ley de protección de datos al día de hoy, a fines de imponer las bases fundamentales sobre los datos personales, sensibles y la protección de los consumidores contra los responsables del archivo, en este caso las empresas que ofertan sus bienes y servicios a través de medios electrónicos. En la región, la mayoría de los países han avanzado en esta materia como podemos visualizar:

2.1. Protección de Datos en Colombia

Por lo que se refiere a la legislación colombiana, se encuentra reforzada a través de leyes, jurisprudencia e instrumentos de *"soft law"*, que han desarrollado los estándares y criterios aplicables a la protección de datos en el comercio electrónico. En el año 2012, el Congreso de Colombia sancionó la Ley Estatutaria 1581[16].

La precitada ley, expone principios como el principio de finalidad, principio de libertad, principio de veracidad, principio de transparencia, principio de acceso, principio de seguridad y principio de confidencialidad[17]. También, se presentó a la Superintendencia de Industria y Comercio (en lo sucesivo la "SIC") como la autoridad de control, teniendo competencias como velar por el cumplimiento de dicha ley, administrar el Registro Nacional Público de Bases de Datos, impartir instrucciones sobre las medidas o procedimientos a ejecutar por parte de los responsables del tratamiento de los datos personales[18].

Por otro lado, en su artículo 26, se prohíbe la transferencia de datos personales de cualquier tipo a empresas u organizaciones que residan en cualquier país sin condiciones adecuadas para la protección de datos[19]. Considerando que los avances en el comercio se presentan de manera dinámica y rápida, la precitada ley, se encuentra reglamentada en distintos enfoques a lo largo del tiempo. El primer reglamento emanado de la Presidencia de la República de Colombia, en fecha 27 de junio de 2013. Hay que mencionar que este fue el primer reglamento que extendía los criterios de aplicación de la ley de protección de datos. Se expresan las formas de manifestación de consentimiento de forma oral, escrita o por conductas inequívocas, entendiendo que en ningún caso se podrá tomar el silencio u omisión como autorización o consentimiento para el tratamiento de los datos.

---

[16] Congreso de la República de Colombia, *Ley Estatutaria 1581 de 2012*, por la cual se dictan disposiciones generales para la protección de datos personales, *Diario Oficial* n.º 48.587, 17 de octubre de 2012, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

[17] Congreso de la República de Colombia, *Ley Estatutaria 1581 de 2012*, art. 4. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[18] Congreso de la República de Colombia, *Ley Estatutaria 1581 de 2012*, art. 4, lit. g.

[19] Congreso de la República de Colombia, *Ley Estatutaria 1581 de 2012*, art. 26.

También, se desarrolló el criterio de exigibilidad a todas los responsables de las bases de datos una política de tratamiento y un aviso de privacidad al ingresar a la plataforma, asegurándose que el usuario o el consumidor pueda entender la finalidad del tratamiento de los datos y sus derechos. El criterio más importante es la diferenciación que se planteó entre transmisión internacional de datos personales a transferencia de datos personales, ya que las primeras podrán estar respaldadas por contrato de transmisión de datos[20]. La aplicación práctica de este criterio se puede visualizar al utilizar servicios como *cloud* internacionales (AWS, Azure, Google Cloud) o procesadores de pago internacionales (Stripe, PayPal) es transmisión, no transferencia, si hay contrato adecuado; esto es importante para las empresas de tecnología que residen en Colombia.

Luego, la presidencia de la República de Colombia emitió el Decreto 255 de 2022, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países[21]. El precitado decreto, complementa el anterior, desarrollando los criterios de transferencia internacional, debiendo ser aprobadas por la Superintendencia de Industria y Comercio, y la obligación de generar buenas prácticas y normas corporativas vinculantes a la transferencia de datos, inspirado en el Reglamento General de Protección de Datos de la Unión Europea.

Hasta el día de hoy, la Superintendencia de Industria y Comercio, ha podido generar experiencias sobre procesos administrativos en materia de protección de datos y comercio electrónico, como lo pueden ser los casos contra Google (Resolución 53593 del 3 de septiembre de 2020[22]) y Uber (Resolución 59876 del 28 de septiembre de 2020[23]), los cuales representan precedentes importantes para el comercio electrónico y la observancia por parte de la SIC, desarrollando el criterio de extraterritorialidad, en la cual la ley de protección de datos, es aplicable a empresas extranjeras y de igual forma recolectan datos de personas por medio de cookies u otras formas, además de esto prohibió los medios engañosos para recolectar datos y generar transparencia frente a los roles de responsable y encargados de los datos, ya que el responsable es quien decide sobre la finalidad del tratamiento y el encargado ejecuta la función por medio del responsable.

---

[20] Presidencia de la República de Colombia, *Decreto 1377 de 2013*, por el cual se reglamenta parcialmente la Ley 1581 de 2012, 27 de junio de 2013.

[21] Ministerio de Comercio, Industria y Turismo (Colombia), *Decreto 255 de 2022*, sobre normas corporativas vinculantes, 23 de febrero de 2022, https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=179087.

[22] Superintendencia de Industria y Comercio (Colombia), Resolución n.º 53593, 3 de septiembre de 2020 (Caso Google), https://sedeelectronica.sic.gov.co/sites/default/files/boletin-juridico/boletin/docs/ORDEN%20GOOGLE%281%29.1.

[23] Superintendencia de Industria y Comercio (Colombia), Resolución n.º 59876, 28 de septiembre de 2020 (Caso Uber).

La fijación de criterios que ha desarrollado la SIC, en cuanto al Comercio electrónico, sirve para otros países en la región implementar criterios a empresas internacionales que se establezcan como medios de pago, transporte, seguros, real estate, fintech, insutech o servicios de cloud.

2.2. Protección de Datos en Argentina

En Argentina, no se dispone de una ley de protección de datos enfocada en el comercio electrónico, sin embargo, en el año 2000, el Senado y Cámara de Diputados de la Nación de Argentina, sancionaron la ley 25.326[24]. Esta ley impone las bases fundamentales para la protección de los datos en Argentina. Expresando como principios generales los siguientes: La licitud de los datos recolectados; la calidad, considerando que los datos recolectados deberán ser adecuados y pertinentes según la finalidad y el ámbito para el cual se requiere; el consentimiento, considerando que el tratamiento de los datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre expreso e informado y otros principios como la seguridad de los datos, la confidencialidad y datos sensibles[25].

Igualmente, se condiciona la cesión de los datos personales con excepción a que dicha cesión se encuentre relacionada directamente con la finalidad de recolección de los datos. Con referencia a la transferencia internacional de datos personales, se encuentra permitida de forma condicionada, siempre y cuando las organización pública o privada que recibe los datos personales, cuente con los niveles de protección adecuados[26]. Por ejemplo: una empresa argentina (responsable del tratamiento) recopila datos de sus clientes y contrata servicios de almacenamiento en la nube de una empresa, en Estados Unidos (encargado del tratamiento) para gestionar esos datos. En este caso, los datos personales de los clientes que se encuentran en Argentina se transfieren a los servidores del proveedor en Estados Unidos, quien los almacena siguiendo las instrucciones de la empresa argentina.

Un avance para la legislación argentina se dio en el año 2016 con la sanción de la Ley 27.275, referente al Derecho de Acceso a la información pública, siendo esta ley la encargada de ejercer el mandato para la creación de la Agencia de Acceso a la información pública, velando por las competencias de protección de datos y llevando el registro de todas las bases de datos de la argentina[27]. Hoy en día Argentina, tiene un nivel

---

[24] Congreso de la Nación Argentina, *Ley 25.326 de Protección de los Datos Personales*, 4 de octubre de 2000, https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm.

[25] Congreso de la Nación Argentina, *Ley 25.326*, arts. 1-3.

[26] Congreso de la Nación Argentina, *Ley 25.326*, art. 12.

[27] Congreso de la Nación Argentina, *Ley 27.275 de Derecho de Acceso a la Información Pública*, 29 de septiembre de 2016, https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm

de protección de datos suficiente para sus ciudadanos, esto permite a que las empresas residenciadas en el país puedan realizar sus actividades comerciales transfronterizas con plenas facultades con otras empresas que residan en estados miembros de la Unión Europea (UE), Estados Unidos de América (USA), Nueva Zelanda, Reino Unido, Isla de Man, Uruguay, Israel, entre otros[28].

En definitiva, Argentina es uno de los países más avanzados en la materia de protección de datos, siendo el referente en modelos contractuales para la transferencia de datos personales entre dos empresas en latinoamérica.

2.3. Protección de Datos en Chile

En Chile, se encuentra sancionada la Ley 19.628, sobre la protección de la vida privada desde el 18 de agosto de 1999, dicha ley ha sido modificada hasta su última versión que entrará en vigencia el 01 de diciembre de 2026[29], la precitada reforma representa el futuro sobre la protección de datos personales en Chile y evoca principios fundamentales como licitud, finalidad, proporcionalidad, calidad, responsabilidad, transparencia y confidencialidad[30].

Al igual que en Argentina, se ordenó la creación de una Agencia que se encargue de velar por el efectivo cumplimiento de la ley de protección de datos, esto resulta interesante, ya que en dicha institución se aprobarán todas las transferencias de datos per-

---

[28] Agencia de Acceso a la Información Pública (Argentina), «Transferencias internacionales», acceso el 22 de noviembre de 2025, https://www.argentina.gob.ar/transferencias-internacionales.

[29] Congreso Nacional de Chile, *Ley 19.628 sobre Protección de la Vida Privada*, 18 de agosto de 1999 (última modificación para vigencia 2026), https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2026-12-01

[30] Congreso Nacional de Chile, *Ley 19.628*, art. 3.
b) Principio de finalidad. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines. En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; que exista una relación contractual o precontractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta, siempre que se enmarque dentro de los fines del contrato o sea coherente con las tratativas o negociaciones previas a la celebración del mismo; que el titular otorgue nuevamente su consentimiento, y cuando lo disponga la ley. c) Principio de proporcionalidad. Los datos personales que se traten deben limitarse estrictamente a aquéllos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento. Los datos personales pueden ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser suprimidos o anonimizados, sin perjuicio de las excepciones que establezca la ley. Un período de tiempo mayor requiere autorización legal o consentimiento del titular. d) Principio de calidad. Los datos personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento. e) Principio de responsabilidad. Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios contenidos en este artículo y de las obligaciones y deberes de conformidad a la ley. f) Principio de seguridad. En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos. g) Principio de transparencia e información. El responsable debe entregar al titular toda la información que sea necesaria para el ejercicio de los derechos que establece esta ley, incluyendo las políticas y las prácticas sobre el tratamiento de los datos personales, las que además deberán encontrarse

sonales internacionales, siempre y cuando el país de residencia de la empresa receptora de los datos cumpla con los estándares suficientes, tomando en cuenta la existencia de normas que reconozcan o garanticen los derechos de los titulares de datos y la existencia de una autoridad pública de control[31].

Se debe agregar que la transferencia de datos internacionales se debe formalizar a través de un contrato de transferencia de datos, que deberá ser certificado por la Agencia de control; en aquellos casos que la transferencia de datos se realice a empresas relacionadas o empresas que pertenezcan al mismo grupo empresarial, se podrán formalizar a través de normativas internas previamente aprobadas por la Agencia de Control[32].

La legislación chilena, se ha comprometido en avanzar para equipararse a otros países en la región, cuestión que nos lleva a reflexionar aún más sobre la necesidad de un marco normativo en Venezuela y su posible regulación para transferencias internacionales y/o actividades comerciales. Mientras estos avances se materializan, la Cámara de Comercio de Santiago, publicó un Código de Buenas Prácticas para el Comercio Electrónico, el cual busca reforzar los criterios sobre la legislación actual, elevando el estándar de cómo se debe informar y se obtiene el permiso de los usuarios, además de exigir la aplicación de medidas técnicas y organizativas que garanticen la confidencialidad de los datos y a su vez, la transparencia sobre los mecanismos de obtención como cookies. Para muchas empresas prestadoras de servicio, esto representa generar una infraestructura de gestión de datos activa y preventiva, no meramente reactiva, ya que la idea es minimizar los riesgos de violación de los derechos de los consumidores.

permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita. El responsable debe adoptar las medidas adecuadas y oportunas para facilitar al titular el acceso a toda la información que señala esta ley, así como cualquier otra comunicación relativa al tratamiento que realiza. h) Principio de confidencialidad. El responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2026-12-01

31 Congreso Nacional de Chile, *Ley 19.628*, art. 28.

32 Congreso Nacional de Chile, *Ley 19.628*, art. 28.

CONCLUSIONES

Las empresas y/o personas que ofrecen sus productos y/o servicios se han ido adaptando al auge tecnológico y paso a paso han ido migrando a las herramientas tecnológicas, en Venezuela se ha podido observar cómo muchas empresas y/o personas optan por ofrecer sus servicios y/o vender sus productos a través de "tiendas onlines", han creado sus propias aplicaciones o utilizan aplicaciones alternativas como whatsapp, a pesar no contar con una ley que les establezca los parámetros de cómo deberían tratarse los datos personales de sus consumidores.

No obstante, es indispensable que cualquier plataforma deba contar con medidas de protección y preguntarse al implementarlas ¿Cómo tener certeza de que una persona es quien dice ser? (Identidad real), la legitimidad de una persona para actuar frente a la solicitud de un producto o servicio es lo importante y quizás lo más fundamental al momento de expresar la voluntad y el consentimiento de establecer una relación en el comercio electrónico.

Esto nos lleva a preguntarnos ¿Cómo identificarla electrónicamente una vez establecida su identidad? (Identidad virtual). La legitimidad de una persona se puede representar de distintas formas, a través del conocimiento y visualización de su cédula de identidad o DNI, pasaporte o cualquier medio de identificación aceptado por la legislación venezolana, sin embargo, esto no resulta suficiente en algunas ocasiones, por lo tanto, hay que dirigir el esfuerzo a responder lo siguiente: ¿Cómo impedir suplantaciones físicas o electrónicas de identidad?

Hoy en día, existen sistemas de validación automática para identificaciones y muchas son muy eficientes, ya que automatizan los procesos; se observa que varios sistemas de validación presentan márgenes de error sustanciales que permiten errores sustanciales que pueden perjudicar a los usuarios o consumidores. Por lo tanto, las empresas prestadoras de servicios deben tener analistas de datos u oficial de datos para garantizar y resguardar los derechos de cada uno de los consumidores y usuarios; llevándonos a la última pregunta ¿Cómo evitar que una persona niegue haber enviado un mensaje o expresada voluntad?

En Venezuela, hay una gran masa de consumidores y/o usuarios que se han visto en la necesidad de acudir a denunciar casos de Phishing, siendo preocupante la falta de atención legislativa que hay sobre el tema. A pesar de ser un país con un sistema de Derecho Positivo, a día de hoy nuestro desarrollo en la materia se ubica en dos sentencias emanadas de la Sala Constitucional del Tribunal Supremo de Justicia, cuestión que resulta beneficioso para los vagos estándares que tenemos hoy en día, pero dichas sentencias encuadran la protección de datos en la óptica del *"Habeas data"*.

Dicho lo anterior, podemos mencionar la Sentencia emanada de la Sala Constitucional del Tribunal Supremo de Justicia Nro. 25-0195 del 21 de Mayo de 2025[33], la cual desarrolla los requisitos para ejercer un recurso de habeas data, el lapso de respuesta exigible al administrador de la base de datos y los derechos protegidos por el espectro del *"Habeas data",* establece que los Juzgados de Municipio con competencia en lo Contencioso Administrativo son competentes para conocer demandas de "*Hábeas data"* (art. 167-169 y señala que el criterio vinculante para la competencia es domicilio del solicitante.

Se establecen los requisitos para recurrir a un recurso de *"Habeas data",* el lapso de respuesta que vendría a ser de 20 días hábiles para respuesta, con excepción a casos de urgencia comprobada, siendo un procedimiento sumario y expedito. Debemos resaltar que la precitada sentencia protege y extiende la esfera de los derechos protegidos como: Actualización de datos; rectificación de información errónea; supresión de datos obsoletos y confidencialidad.

En esencia, la precitada sentencia extiende lo desarrollado en la Sentencia de la Sala Constitucional Nro. 1050 del 23 de agosto del año 2000[34], la cual define los siete derechos que se protegen con el "*Habeas Data"*, como lo pueden ser: conocer la existencia de registros, acceso individual a la información, derecho de respuesta, conocer uso y finalidad de la información, actualización de datos inexactos, rectificación de datos falsos/incompletos destrucción de datos erróneos.

En consecuencia, se desarrollan los principios de finalidad lícita del tratamiento de datos, temporalidad, veracidad y proporcionalidad. Además de esto hay que enfatizar que este recurso se presenta como una acción reactiva, protegiendo al individuo frente a algún ilícito, pero no resulta un marco legal, ni impone obligaciones preventivas a las empresas.

En el fondo, esto no resulta suficiente para el comercio electrónico en Venezuela, ni resulta comparable con los estándares internacionales necesarios como la responsabilidad por transferencias transfronterizas, transparencia en políticas de privacidad y limitación de uso secundario de datos.

La falta de regulación en materia de protección de datos, es una limitación para el crecimiento del comercio electrónico, en virtud de que evidentemente existe un vacío legal que deja una puerta abierta a que en el momento en que se presente una contro-

---

[33] Tribunal Supremo de Justicia (Sala Constitucional), Sentencia n.º 25-0195, 21 de mayo de 2025. https://historico.tsj.gob.ve/decisiones/scon/mayo/343949-0759-21525-2025-25-0195.HTML

[34] Tribunal Supremo de Justicia (Sala Constitucional), Sentencia n.º 1050, 23 de agosto de 2000. https://historico.tsj.gob.ve/decisiones/scon/agosto/1050-230800-00-2378%20.htm

versia sea difícil encontrar una solución justa que no perjudique a la empresa, pero que proteja al consumidor. Además, este panorama de inseguridad jurídica limita la posibilidad de que las empresas puedan participar plenamente en el comercio electrónico transfronterizo, lo que puede llevar a afectar su competitividad e incluso reducir la confianza de los inversionistas extranjeros en el entorno electrónico nacional.

La autorregulación en dicha materia es la clave para subsanar temporalmente la falta de regulación en dicha materia. En atención a lo planteado, se sugiere que las empresas utilicen técnicas de cifrado para proteger los datos personales y protocolos de seguridad, realizar capacitaciones de protección de datos a su personal y tener un Oficial de Datos Personales para generar políticas efectivas que garanticen la protección de los derechos de los usuarios y consumidores.

Además de esto, deben garantizar los derechos ARCO; adaptar los procesos de recopilación de datos y uso de datos personales a los estándares internacionales; en caso de realizar transacciones o transferencias de datos personales equiparar el cumplimiento de la empresa al domicilio en cual se transfieren los datos, realizar informes de riesgo e impacto del tratamiento de datos con la idea de minimizar los riesgos de la brecha digital. Con esto se espera que los servicios digitales y la comercialización electrónica en Venezuela establezcan bases firmes hasta la llegada de una regulación adecuada.

BIBLIOGRAFÍA

Agencia de Acceso a la Información Pública. «Transferencias internacionales». República Argentina. Acceso el 22 de noviembre de 2025. https://www.argentina.gob.ar/transferencias-internacionales.

Aponte Núñez, Emercio José. «La importancia de la protección de datos de carácter personal en las relaciones comerciales». *Revista de Derecho Privado* (Universidad Externado de Colombia). Acceso el 22 de noviembre de 2025. https://revistas.uexternado.edu.co/index.php/derpri/article/view/561/531.

Asamblea Nacional Constituyente. *Constitución de la República Bolivariana de Venezuela*. Gaceta Oficial Extraordinaria n.º 36.860, 30 de diciembre de 1999. https://www.oas.org/dil/esp/constitucion_venezuela.pdf.

Asamblea Nacional de la República Bolivariana de Venezuela. *Ley Especial contra los Delitos Informáticos*. Gaceta Oficial n.º 37.313, 30 de octubre de 2001. https://www.asambleanacional.gob.ve/storage/documentos/leves/ley-especi-20220309131245.pdf.

Asilo Digital. «Hackeo a Digitel en 2024: Todo lo que necesitas saber». Acceso el 22 de noviembre de 2025. https://www.asilodigital.com/que-esta-pasando-con-digitel/.

Badell Madrid, Rafael. «El derecho constitucional a la privacidad y su conflicto con los derechos intelectuales». *Revista de Propiedad Intelectual*, n.º 19 (2016): 141-163. http://www.ulpiano.org.ve/revistas/bases/artic/texto/RPI/19/rpi_2016_19_141-163.pdf.

Blog Jurídicos Venezuela. «"Hola, soy María y cambié de número": Modus operandi para extorsionar». Acceso el 22 de noviembre de 2025. https://blog.juridicosvenezuela.com/hola-soy-maria-y-cambie-de-numero-modus-operandi-para-extorsionar/.

Buitrago Rodríguez, Mariana del Valle. «El comercio electrónico y la actividad comercial digital en el Derecho Venezolano». *Revista Hacer y Saber* (2014). http://erevistas.saber.ula.ve/index.php/hacerysaber/article/download/19835/21921931474.

Congreso de la Nación Argentina. *Ley 25.326 de Protección de los Datos Personales*. 4 de octubre de 2000. https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm.

Congreso de la Nación Argentina. *Ley 27.275 de Derecho de Acceso a la Información Pública*. 29 de septiembre de 2016. https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm.

Congreso de la República de Colombia. *Ley Estatutaria 1581 de 2012*. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

Congreso Nacional de Chile. *Ley 19.628 sobre protección de la vida privada*. 18 de agosto de 1999 (última modificación para vigencia 2026). https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2026-12-01.

Cova Arria, Luis. «Problemas legales del comercio electrónico y los obstáculos para la implementación de la Ley Modelo de la CNUDMI sobre el comercio electrónico, con relación a los documentos de transporte utilizados en el comercio internacional». *Revista Venezolana de Derecho Mercantil*, n.º 11 (2023): 23-54. http://www.ulpiano.org.ve/revistas/bases/artic/texto/RVDM/11/RVDM_2023_11_23-54.pdf.

MDS Telecom. «Estiman crecimiento superior a 100% del e-commerce en Venezuela». *MDS Telecom News*. Acceso el 22 de noviembre de 2025.

Ministerio de Comercio, Industria y Turismo (Colombia). *Decreto 255 de 2022*. 23 de febrero de 2022. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=179087.

Ministerio de Economía y Finanzas. «Comercio electrónico en el país se incrementó un 97% en el 2024». Acceso el 22 de noviembre de 2025. https://www.mppef.gob.ve/comercio-electronico-en-el-pais-se-incremento-un-97-en-el-2024/.

Organización Mundial del Comercio. *Perspectivas del Comercio Mundial y estadísticas*. Ginebra: OMC, abril de 2025. https://www.wto.org/spanish/ress/booksp_s/trade_outlook25_s.pdf.

Parlamento Europeo y Consejo de la Unión Europea. *Reglamento (UE) 2016/679 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*. *Diario Oficial de la Unión Europea* L 119, 4 de mayo de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679.

Presidencia de la República de Colombia. *Decreto 1377 de 2013*. 27 de junio de 2013.

Superintendencia de Industria y Comercio (Colombia). *Resolución n.º 53593*. 3 de septiembre de 2020. https://sedeelectronica.sic.gov.co/sites/default/files/boletin-juridico/boletin/docs/ORDEN%20GOOGLE%281%29.1.

Superintendencia de Industria y Comercio (Colombia). *Resolución n.º 59876*. 28 de septiembre de 2020.

Tribunal Supremo de Justicia (Sala Constitucional). *Sentencia n.º 1050*. 23 de agosto de 2000.

Tribunal Supremo de Justicia (Sala Constitucional). *Sentencia n.º 25-0195*. 21 de mayo de 2025.