# LA PROTECCIÓN DE DATOS COMO FRENO AL ABUSO DE POSICIÓN DE DOMINIO EN VENEZUELA

**Autores:**
Ramón I. Andrade Monagas
Ignacio J. Andrade Cifuentes
Luis González Morales

# LA PROTECCIÓN DE DATOS COMO FRENO AL ABUSO DE POSICIÓN DE DOMINIO EN VENEZUELA

## Data Protection as a Restraint on Abuse of Dominant Position in Venezuela

**Ramón I. Andrade Monagas**[1]
**Ignacio J. Andrade Cifuentes**[2]
**Luis González Morales**[3]

**SUMARIO:**



***Resumen***

Este trabajo tiene como propósito desarrollar y argumentar por qué y cómo la ausencia de normas robustas, actualizadas y específicas en materia de protección de datos e intercambio de información podría afectar la libre competencia y resultar en el abuso de posición de dominio de las empresas tecnológicas con acceso a la información personal de sus usuarios. A estos efectos, se revisarán las normas en materia de protección de datos que existen en Venezuela y analizaremos su capacidad de satisfacer las demandas actuales de esta materia. También revisaremos las normas vigentes en materia de derecho de la competencia, particularmente, en lo que respecta a la posición de dominio y su abuso. Con ello, presentaremos algunas situaciones en las que la ausencia de normas robustas, actualizadas y específicas en materia de protección de datos e intercambio de información podría resultar en el abuso de posición de dominio. Finalmente, presentaremos nuestras conclusiones y recomendaciones al respecto.

---

[1] Socio en Ponte Andrade & Casanova, Madrid, España. Abogado de la Universidad Católica Andrés Bello (1995), Especialista en Derecho Financiero de la misma universidad (2003, mención *cum laude*), y Masters of Business Administration (TRIUM Global Executive MBA Program) del Stern School of Business de la Universidad de Nueva York, London School of Economics and Political Science (LSE) y HEC School of Management (París) (2009). Fue socio de la firma global de abogados Norton Rose Fulbright de 2000 a 2017 y Director de Activos Especiales de la Corporación Andina de Fomento (CAF)de 2017 a 2022. Correo electrónico: randrade@epaclaw.com.

[2] Abogado en Ponte Andrade & Casanova, Caracas, Venezuela. Abogado de la Universidad Católica Andrés Bello (2019, mención *cum laude*) y Especialista en Derecho Financiero de la misma universidad (2022, mención *summa cum laude*). Profesor de Pregrado y Posgrado en la Universidad Católica Andrés Bello y Miembro del Consejo de Posgrado de la Facultad de Derecho de esa universidad. Correo electrónico: ijandradec@epaclaw.com.

[3] Abogado en Ponte Andrade & Casanova, Caracas, Venezuela. Abogado de la Universidad Católica Andrés Bello (2020). Correo electrónico: lgonzalez@epac.com.ve.

***Palabras clave***

Protección de datos/ libre competencia/ abuso de posición de dominio.

***ABSTRACT***

The primary objective of this paper is to establish and argue the potential detrimental impact of the absence of robust, updated, and specific rules on data protection and information exchange on free competition. This absence could result in the abuse of dominant position by technology companies with access to personal user information. To achieve this, the paper will examine the current data protection regulations in Venezuela and evaluate their adequacy in meeting current demands. Furthermore, this paper will review the existing competition law regulations, particularly in relation to dominance and its potential abuse. The paper will also present scenarios demonstrating how the lack of robust rules in data protection and information exchange could lead to the abuse of dominance. Ultimately, we will present our findings and offer recommendations in this regard.

***Keywords***

Data protection/ free competition/ abuse of dominant position.

## I. INTRODUCCIÓN

En 1999, una investigación[4] de mercado reveló que más de 100 millones de estadounidenses usaban el internet, un crecimiento exponencial que refleja la expansión global de esta tecnología. Hoy, los datos personales recopilados a través de estas plataformas se han convertido en uno de los recursos más valiosos, explotados comercialmente por empresas con acceso masivo a la información de sus usuarios. Ese mismo año, International Data Corporation predijo que esa tendencia continuaría y que, para finales de 2003, habría unos 502 millones de usuarios del internet en el mundo entero[5]. Se quedaron cortos; para 2004, el Computer Industry Almanac calculaba unos 935 millones de usuarios globalmente[6]. Para abril 2024, DataReportal estimó unos 5,44 mil millones de usuarios en línea, equivalentes al 67,1% de la población mundial[7]. Se estima que, en 2024, se transarán alrededor de 6,3 trillones de dólares en comercio electrónico[8] y que se envían unos 347,3 mil millones de correos electrónicos por día a lo largo de las 7 horas, en promedio, que pasan en internet[9].

Este crecimiento no sorprende. Es evidente el enorme potencial comercial y social del internet, el cual es explotable económicamente por la facilidad de alcanzar directa e individualmente a los usuarios y rastrear cada operación realizada. Cada vez que alguien visita una página web,

---

[4] Reuters. 1999. «Internet users now exceed 100 million» sitio web de The New York Times. Último acceso: 1 de julio de 2024. https://www.nytimes.com/1999/11/12/business/internet-users-now-exceed-100-million.html

[5] *Ibid.*

[6] Peterson, Michael P. 2005. «A decade of maps and the internet.» Editado por Global Congresos. *XXII International Cartographic Conference*. Coruña: The International Cartographic Association (ICA-ACI). Último acceso: 14 de julio de 2024. https://shorturl.at/9aLZM.

[7] Kemp, Simon. 2024. *Digital 2024 April Global Statshot Report*. 24 de abril. Último acceso: 14 de julio de 2024. https://datareportal.com/reports/digital-2024-april-global-statshot.

[8] Snyder, Kristy. 2024. *35 e-Commerce statistics of 2024*. 28 de marzo. Último acceso: 14 de julio de 2024. https://shorturl.at/Y8bhC.

[9] Singh, Shubham. 2024. *How Many Emails Are Sent Per Day in 2024?* 21 de mayo. Último acceso: 14 de julio de 2024. https://www.demandsage.com/how-many-emails-are-sent-per-day/.

envía un correo, usa un reloj inteligente para medir su actividad física, cuelga una imagen o video a una red social, pide con su voz a los asistentes de inteligencia artificial como Alexa, Cortana o Siri que anote un listado de compras, o accede una publicidad, el usuario está dejando un rastro –una huella– digital, muchas veces con información que lo identifica. Esto puede incluir direcciones de IP, direcciones de correos electrónicos, ubicaciones GPS en vivo, nombres, fechas de nacimiento, datos de cuentas bancarias, tarjetas de crédito, hábitos, imágenes, voz, alergias y enfermedades, entre otros. Y estos datos personales pueden ser aprovechados comercialmente por las empresas que los reciben y recopilan, permitiéndole, no solo personalizar su mensaje con base en la información personal de cada usuario, sino acceder a un mercado en el que se transa la información en sí misma.

En Venezuela, el auge de plataformas digitales[10] ha seguido la tendencia global, pero con una gran diferencia: la falta de regulación robusta en protección de datos ha permitido que las empresas tecnológicas con acceso masivo a información personal adquieran una posición de dominio en el mercado. Este vacío legal no solo afecta la privacidad de los usuarios, sino que también crea desigualdades competitivas entre empresas, vulnerando la libre competencia.

Considerando lo anterior, no es difícil sostener que la información y los datos han obtenido una significación y entidad económica monumental, pudiendo ser explotados y aprovechados comercialmente de múltiples formas. Ello conlleva a la posibilidad de que aquellas empresas que recolecten y usen de forma indiscriminada una mayor cantidad de datos, obtengan una ventaja competitiva injustificada y una posición de dominio en su respectivo rubro, la cual, posiblemente, sea abusada en detrimento de la libre competencia.

En ese contexto, este trabajo tiene como propósito desarrollar y argumentar por qué y cómo, en nuestro criterio, la ausencia de normas robustas, actualizadas y específicas en materia de protección de datos e intercambio de información podría afectar la libre competencia y resultar en el abuso de posición de dominio de las empresas tecnológicas con acceso a la información personal de sus usuarios.

A estos efectos, revisaremos las normas en materia de protección de datos que existen en Venezuela y analizaremos su capacidad de satisfacer las demandas actuales de esta materia. También revisaremos las normas vigentes en materia de derecho de la competencia, particularmente, en lo que respecta a la posición de dominio y su abuso. Con ello, presentaremos algunas situaciones en las que la ausencia de normas robustas, actualizadas y específicas en materia de protección de datos e intercambio de información podría resultar en el abuso de posición de dominio, y nuestras conclusiones y recomendaciones al respecto.

## II. LOS MECANISMOS DE PROTECCIÓN DE LA INFOMACIÓN PERSONAL EN EL ORDENAMIENTO JURÍDICO VENEZOLANO SON POCOS, DISPERSOS E INSUFICIENTES EN EL CONTEXTO ACTUAL DEL INTERNET Y LA PROVISIÓN DE BIENES Y SERVICIOS EN LÍNEA

En este acápite, esbozaremos los principales instrumentos normativos que tratan la protección de datos personales. Como podrá apreciarse, los mecanismos de protección de la información personal en el ordenamiento jurídico venezolano son pocos, generales, dispersos e insuficientes en el contexto actual del internet y la provisión de bienes y servicios en línea.

[10] El Interés. 2024. *Más trabajo y mayores sueldos: así es el próspero negocio de delivery en Venezuela.* 23 de abril. Último acceso: 16 de julio de 2024. https://elestimulo.com/elinteres/empresas/2024-04-23/el-negocio-del-delivery-prospera-en-venezuela-estudio/.

## 2.1 Protección constitucional y habeas data

En este subtítulo, no pretendemos agotar este tema ni desarrollar con demasiada profundidad la figura del *habeas data,* sobre todo, considerando lo extenso que ha sido su desarrollo por la doctrina y la jurisprudencia. Dicho eso, sí esbozaremos sus características esenciales, especialmente las condiciones para su procedencia, para sostener que, tal como está actualmente diseñado y en el contexto de la acelerada y profunda digitalización que vivimos actualmente, el *habeas data* no es capaz de proteger suficientemente a las personas.

La Constitución venezolana[11] establece el derecho a la privacidad e intimidad personal y familiar, remitiendo a la ley la limitación del uso de la informática para proteger y garantizar el derecho[12]. También estipula el derecho de toda persona a acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados y a conocer el uso que se haga de los mismos y su finalidad, pudiendo solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos[13].

Esta disposición es ratificada por artículo 167 de la Ley Orgánica del Tribunal Supremo de Justicia[14]. Según este artículo, las personas tienen derecho a :

> Conocer los datos que a ella se refieran, así como su finalidad, que consten en registros o bancos de datos públicos o privados y, en su caso, exigir la supresión, rectificación, confidencialidad, inclusión, actualización o el uso correcto de los datos cuando resulten inexactos o agraviantes.

A esta acción judicial se le conoce como *habeas data*. El *habeas data* ha sido considerado por un sector de la doctrina y de la jurisprudencia como una especie de amparo[15], que busca proteger los derechos de los registrados en los archivos o bancos de datos, que puedan contener información equivocada, antigua, falsa o con potenciales fines discriminatorios, o lesivas del

[11] Gaceta Oficial N° 5.908 Extraordinario del 19 de febrero de 2009.

[12] Artículo 60 – Constitución. 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.

[13] Artículo 28 – Constitución. Toda persona tiene 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 aquéllos, 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.

Exposición de Motivos – Constitución. … Se reconoce por vez primera en el constitucionalismo venezolano, el hábeas data o el derecho de las personas de acceso a la información que sobre sí mismas o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley. El hábeas data incluye el derecho de las personas de conocer el uso que se haga de tales registros y su finalidad, y de solicitar ante el tribunal competente su actualización, rectificación o destrucción, si fuesen erróneos o afectasen ilegítimamente sus derechos…

[14] Gaceta Oficial N° 6.684 Extraordinario del 19 de enero de 2022.

[15] Ver: Rondón de Sansó, Hildegaard. 2001. *Análisis de la Constitución Venezolana de 1999 (parte orgánica y sistemas)*. Caracas: Ex Libris. // Sagües, Nestor. 1995. *Derecho Procesal Constitucional. Acción de Amparo.* Buenos Aires: Astrea.

derecho a la intimidad de las personas[16]. Incluso, en ocasiones, se le ha tratado, aunque con diferencias, como un amparo constitucional[17], aunque en otras ocasiones se ha concluido que los derechos que contiene el *habeas data* daban origen a acciones autónomas, distintas y no siempre vinculadas al amparo constitucional[18].

Según la jurisprudencia de la Sala Constitucional del Tribunal Supremo de Justicia[19], el *habeas data* trata del derecho de las personas a conocer la información que sobre ellas haya sido compiladas por otras, sean estas el Estado o los particulares, pues todos son capaces de recopilar, almacenar y compilar datos de personas o de sus bienes. Como esta compilación, almacenamiento y uso de la información pueden afectar la vida privada, el honor, la intimidad, la reputación y otros valores constitucionales, la Constitución otorga a las personas los derechos contemplados en su artículo 28. De acuerdo con la Sala, estos derechos son:

- El derecho de conocer sobre la existencia de tales registros.
- El derecho de acceso individual a la información, la cual puede ser nominativa, o donde la persona queda vinculada a comunidades o a grupos de personas.
- El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él.
- El derecho de conocer el uso y finalidad que hace de la información quien la registra.

---

[16] Chavero Gazdik, Rafael. 2001. *El Nuevo Régimen de Amparo Constitucional.* Caracas: Editorial Sherwood. P. 40.

[17] El amparo constitucional está contemplado en el artículo 27 de la Constitución, el cual establece que toda persona tiene derecho a ser amparada por los tribunales en el ejercicio de sus derechos constitucionales, lo cual se extiende a aquellos derechos inherentes a la persona que no se encuentren expresamente establecidos en la Constitución. Así, conforme a la Exposición de Motivos de la Constitución, el amparo constitucional tiene por finalidad la tutela judicial reforzada de los derechos humanos. La doctrina concibe al amparo como «una garantía constitucional, entendiendo tal concepto en el sentido de que con el mismo se alude al medio a través del cual se hacen efectivos los derechos, las restantes garantías, las facultades y las potestades que la Constitución consagra.» Rondón de Sansó, Hildegaard. 1994. *Amparo Constitucional.* Caracas: Arte. P. 30.

La Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales ("Ley Orgánica de Amparo"), en su artículo 6, «precisa que la [violación o amenaza del derecho o garantía constitucional] sea actual, es decir, que no haya cesado; que sea reparable, y que no haya sido consentida» Brewer-Carías, Allan. 2011. «El Amparo Constitucional en Venezuela.» *Revista IUS* (Centro Internacional de Estudios sobre Ley y Derecho) 5 (27). https://www.revistaius.com/index.php/ius/article/view/88. P. 14.

Además, entre otros supuestos, no debe haber alternativas al amparo para restituir el derecho vulnerado, y el agraviado tampoco puede haber optado por recurrir a las vías judiciales ordinarias o hecho uso de los medios judiciales preexistentes. De esta forma, el amparo constitucional no busca *prevenir* violaciones a los derechos constitucionales, sino *corregirlas y resarcir* la lesión de algún derecho o garantía constitucional. En otras palabras, el amparo busca hacer «desaparecer el hecho o acto invocado y privado como lesivo o perturbador a un derecho o garantía constitucional; o restablecerse a un estado que se asemeje a ella» (*Ibid.*), restableciendo las cosas al estado en anterior al momento de la lesión.

Dicho lo anterior, la Sala Constitucional del Tribunal Supremo de Justicia fijó unas diferencias entre el amparo y el *Habeas Data*. En sentencia N° 182 del 8 de marzo de 2005, estableció: «La distinción entre amparo y Habeas Data se basa en que, a través de la primera no se pueden constituir derechos, sino restablecer los mismos. Por tanto, cuando se denuncie una violación a algunos de los derechos que enumera el artículo 28 de la Constitución, la vía idónea y procedente es el amparo, en cambio, cuando la circunstancia no constituya ninguna denuncia de violación concreta, sino solicitud de actualización, rectificación, destrucción de datos falsos o erróneos, procede una demanda de Habeas Data.»

[18] Ver: Brewer Carías, Allan. s.f. «El proceso constitucional de las acciones de habeas data en Venezuela: las sentencias de la Sala Constitucional como fuente del derecho procesal constitucional.» Último acceso: 14 de julio de 2024. https://allanbrewercarias.net/Content/449725d9-f1cb-474b-8ab2-41efb849fea8/Content/II,%204,%20638.%20PROCEDIMIENTO%20EN%20LAS%20ACCIONES%20DE%20HABEAS%20DATA.%201-10.doc.pdf.

[19] *Ruth Capriles y otros.* 2000. Sentencia N° 1050 (Sala Constitucional del Tribunal Supremo de Justicia, 23 de agosto). También, *Insaca vs. Ministerio de Sanidad y Asistencia Social.* 2001. Sentencia N° 332 (Sala Constitucional del Tribunal Supremo de Justicia, 14 de mayo).

- El derecho de actualización, a fin de que se corrija lo que resulta inexacto o se transformó por el transcurso del tiempo.
- El derecho a la rectificación del dato falso o incompleto.
- El derecho de destrucción de los datos erróneos o que afectan ilegítimamente los derechos de las personas.

Como puede apreciarse, el *habeas data* tiene una doble vertiente. Por un lado, permite a las personas a solicitar el acceso a su información personal. Por el otro, permite a las personas solicitar la actualización, rectificación o la destrucción de datos erróneos o lesivos a sus derechos. De esta forma, «[p]osibilita la adecuación de una verdad formal (aquello insertado –errónea o lesivamente– en el registro respectivo) a una verdad material (lo que realmente es). Puede decirse que posibilita una "adecuación de verdades"»[20]. Esta doble vertiente ha sido reconocida pacíficamente por la Sala Constitucional del Tribunal Supremo de Justicia[21].

Lo anterior también ha conducido a que el *habeas data* se conciba, por su naturaleza y efectos, como el *derecho al olvido*[22]. Este se traduce en «la acción de exigirle al Estado el derecho al olvido» por medio de la eliminación de registros que se hayan mantenido sobre el individuo, especialmente cuando estos se encuentren errados o irrelevantes.[23]

Por otro lado, de acuerdo con la redacción del artículo 167 de la Ley Orgánica del Tribunal Supremo de Justicia[24], se entiende que la persona interesada solo podrá interponer el *habeas data* (i) después de haber solicitado al administrador de la base de datos conocimiento de la información, su corrección, rectificación, actualización, supresión, confidencialidad o uso correcto, y (ii) después de que este no haya respondido dentro de los veinte (20) días hábiles siguientes a la solicitud o haya negado dicha solicitud. Sobre este punto, la Sala Constitucional ha establecido que la persona ha debido ejercer sus derechos previamente ante el recopilador de la información, y es ante la negación al acceso a la información o ante la omisión de la solicitud de acceso a la información o la falta de explicación legal de para qué se recoge la información, que se puede entender que se infringe su situación jurídica y sus derechos constitucionales.[25]

Considerando lo anterior, se puede concluir que el *habeas data* es una acción posterior a la recopilación o uso de la información personal. Además, para su admisibilidad se requiere que el interesado haya solicitado acceso o modificación de la información al recopilador o

[20] Herníquez Maionica, Giancarlo. 2003. «El habeas data y el derecho de la persona con trastornos de identidad de género a obtener documentos relativos a su identidad biológica.» *Revista de Derecho Constitucional N° 8* 67-80. http://www.ulpiano.org.ve/revistas/bases/artic/texto/RDCONS/8/rdcons_2003_8_67-80.pdf.

[21] *Veedores de la UCAB.* 2000. (Sala Constitucional del Tribunal Supremo de Justicia, 23 de agosto).

[22] García, Carilym. 2018. «Habeas Data como mecanismo de protección del derecho al acceso a la información personal en el derecho constitucional venezolano.» *Data Ciencia - Revista Multidisciplinaria Electrónica del Núcleo LUZ - Costa Oriental del Lago* 1 (1). Último acceso: 14 de julio de 2024. P. 69.

[23] ídem, 69.

[24] Artículo 167 – Ley Orgánica del Tribunal Supremo de Justicia. Toda persona tiene derecho a conocer los datos que a ella se refieran así como su finalidad, que consten en registros o bancos de datos públicos o privados; y, en su caso, exigir la supresión, rectificación, confidencialidad, inclusión, actualización o el uso correcto de los datos cuando resulten inexactos o agraviantes. // El Habeas Data sólo podrá interponerse en caso de que el administrador de la base de datos se abstenga de responder el previo requerimiento formulado por el agraviado dentro de los veinte días hábiles siguientes al mismo o lo haga en sentido negativo, salvo que medien circunstancias de comprobada urgencia.

[25] *Insaca vs. Ministerio de Sanidad y Asistencia Social.* 2001. Sentencia N° 332 (Sala Constitucional del Tribunal Supremo de Justicia, 14 de mayo).

almacenador y que este haya (i) no respondido la solicitud o (ii) que la haya negado o (iii) que no haya explicado la finalidad del uso de la información.

En este contexto, considerando la rapidez con la que se intercambia la información en el marco de los negocios digitales actuales, el *habeas data,* en nuestro criterio, resulta insuficiente para proteger a las personas de la recopilación, transmisión, uso y comercialización de su información. En gran parte, esta insuficiencia se debe a que, tal como está diseñado, el *habeas data* opera *ex post*; esto es: no buscan *prevenir* el almacenamiento, uso o transferencia injustificada e ilegítima de la información, sino *corregir* las infracciones que puedan llegar a ocurrir una vez almacenada, usada o transferida la información. La profunda digitalización que vivimos, donde las personas están expuestas a brindar información consciente o inconscientemente a negocios en Venezuela y en el extranjero, esta circunstancia propende a dejar la información de las personas desprotegidas, pues el *habeas data* solo opera después de que el daño está hecho.[26]

## 2.2 Legislación en protección al consumidor

Como mencionamos arriba, nuestra Constitución remite a la Ley el establecimiento de límites al uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Parte de la normativa que regula el uso, almacenamiento y transferencia de la información personal en el ámbito comercial era aquella en materia de protección al consumidor, la cual ha sido objeto de múltiples reformas y derogatorias.

Actualmente nuestra legislación de protección al consumidor está conformada por leyes de control de precios que no regulan la protección de datos, y que derogaron expresa y totalmente las leyes de protección integral al consumidor, que sí regulaban la protección de datos personales.

Sin pretender agotar este tema, iniciaremos con la Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios, que es la última ley de protección integral al consumidor antes de su derogatoria por el régimen actual de control de precios.

En febrero de 2010, fue promulgada la Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios[27], la cual estipulaba que sus disposiciones, que son de orden público, tenían por objeto la defensa, protección y salvaguarda de los derechos e intereses individuales y colectivos en el acceso de las personas a los bienes y servicios para la satisfacción de las necesidades, estableciendo los ilícitos administrativos, sus procedimientos y sanciones; los delitos y su penalización, el resarcimiento de los daños sufridos, su aplicación por parte del Poder Público con la participación activa y protagónica de las comunidades, en resguardo de la paz social, la justicia, el derecho a la vida y la salud del pueblo (artículo 1).

Esta Ley fue principalmente utilizada para regular el desarrollo de las operaciones de los proveedores de bienes y servicios del país, estableciendo disposiciones específicas en materia de la calidad de los bienes ofertados, el acondicionamiento de los establecimientos comerciales, obligaciones sobre la información proporcionada a los consumidores sobre servicios que contratan e incluso exigencias específicas sobre el comportamiento de los comerciantes.

[26] En efecto, de acuerdo con García: «Las personas que ejercen la acción de Habeas Data necesitan de normativas legales para mejorar la calidad de vida y desarrollo pleno de sus derechos humanos. Es por lo que el ciudadano afectado en dichos derechos deberá hacer cumplir la responsabilidad de los órganos de justicia en cuanto a su responsabilidad como órgano controlador del proceso, ya que existen muy pocos mecanismos en Venezuela para solventar dicha situación jurídica.» García, Carilym. 2018. «Habeas Data como mecanismo de protección…», P. 83.

[27] Gaceta Oficial Nº 39.358 del 1 de febrero de 2010.

Si bien esta norma fue derogada en el año 2014 por la Ley de Precios Justos, es importante resaltar su importancia en sus disposiciones de protección de la información de los ciudadanos. En primer lugar, en su artículo 31, la Ley incluyó el intercambio de información en la definición de «comercio electrónico» de la siguiente forma:

> A los fines de esta Ley, se entenderá como comercio electrónico, cualquier forma de negocio, transacción comercial o **intercambio de información con fines comerciales, bancarios, seguros o cualquier otra relacionada**, que sea ejecutada a través del uso de tecnologías de información y comunicación de cualquier naturaleza. Los alcances de la presente Ley, son aplicables al comercio electrónico entre la proveedora o proveedor y las personas, sin prejuicio de las leyes especiales.[28] (resaltado añadido)

A pesar de que la Ley no definía qué debía entenderse por *intercambio de información con fines comerciales,* sí reconoce que la información puede ser (i) explotada comercialmente y, dentro de ello, (ii) transada o enajenada por el titular o almacenador autorizado de brindar la información a otra persona.

Con eso en mente, y entendiendo la posibilidad de explotar comercialmente la información, resultan relevantes los artículos 37 y 38 de la Ley. Estos se referían específicamente el tratamiento y la seguridad de la información que los consumidores le suministran a los proveedores de bienes y servicios en el marco de la ejecución de sus operaciones comerciales. En particular, el artículo 37, titulado *Privacidad y Confidencialidad*, establecía lo siguiente:

> En las negociaciones electrónicas, la proveedora o el proveedor deberán garantizar a las personas la privacidad y la confidencialidad de los datos e información implicada en las transacciones realizadas, de forma tal que la información intercambiada no sea accesible para terceros no autorizados.
>
> Sin menoscabo de la privacidad y confidencialidad aquí establecida, la autoridad competente, podrá solicitar en el ejercicio de sus funciones, la información que considere necesaria y practicar las investigaciones correspondientes. La negativa al cumplimiento de lo establecido en este artículo será sancionado de conformidad con lo previsto en la presente Ley.

Esta disposición establecía la obligación del comerciante de preservar, de forma confidencial, toda la información recibida en el giro de las operaciones comerciales, permitiendo la transferencia de los datos personales recolectados por los proveedores a terceros autorizados. De esta forma, y dada la generalidad de la norma, la protección de la información personal queda regulada fundamentalmente por las políticas de seguridad y privacidad de la información de los proveedores de bienes y servicios y por los contratos celebrados con los usuarios. En la inmensa mayoría de los casos, por no decir en la totalidad, estos contratos son de adhesión, en

[28] Gaceta Oficial N° 39.358, en fecha 01 de febrero de 2010.

los cuales el poder de negociación del usuario se limita a aceptar o rechazar la suscripción del contrato en los términos establecidos por el proveedor.

Visto eso, la Ley exigía a los proveedores la inclusión en los contratos con los usuarios de ciertas disposiciones referidas a la transparencia y consentimiento en el uso y a la selección de la información personal. Por un lado, la Ley establecía en su artículo 38 que los proveedores deben otorgar al consumidor la posibilidad de escoger, dentro de la información recolectada, cuál puede ser compartida con terceros. Por otro lado, establecía la obligación de los proveedores de señalar si las personas tendrán la posibilidad de limitar el uso de su información personal y cómo la podrán limitar. También establecía la obligación de indicar si el suministro de información sobre las personas es parte integrante del modelo de negocios del proveedor.

Mientras que estas disposiciones representaban un paso en la dirección correcta, en nuestro criterio, no hubiesen sido suficientes para abarcar todas las situaciones que surgen del uso actual de tecnología por las personas, el cual está cada día más integrado a nuestra vida cotidiana. A todo evento, estas normas fueron expresamente derogadas en 2014 por la Ley Orgánica de Precios Justos[29], sin contemplar régimen de protección de los datos personales.

En efecto, la Ley Orgánica de Precios Justos, reformada varias veces pero que en general se mantiene vigente a la fecha de hoy, se enfoca en establecer un régimen de control de precios, lo cual es una política fijada por el gobierno venezolano durante los últimos 15 años. No regula otros aspectos relacionados con la protección al consumidor y, mucho menos, con la protección de datos personales.

En cambio, se limita a una mención bastante general de los derechos de las personas al acceso de bienes y servicios. A estos efectos, establece su fin como la defensa del consumidor, el cual busca alcanzar por medio de la «protección del salario y demás ingresos de las personas». Sin embargo, las disposiciones de la Ley parecen más bien enfocarse en regular y controlar las actuaciones de los comerciantes de forma injustificada, desproporcionada y atentando contra su libertad económica. Con este régimen, la Ley logra lo contrario a la defensa del consumidor: atenta contra la calidad de los bienes y servicios –fin y principio de las normas de protección al consumidor– y, además, amenaza la sostenibilidad económica de los proveedores y reduce al mínimo su capacidad de proveer bienes y servicios.[30]

En ese sentido, debido a la derogatoria expresa de la Ley para la Defensa de las Personas en el Acceso a Bienes y Servicios, no existe, en la actualidad, una ley que regule de forma general la protección de los datos de los consumidores de bienes y servicios. Dicho eso, tal como veremos más abajo, sí existen algunas normas de rango legal y sublegal de protección de usuarios y consumidores que establecen algunas obligaciones a los almacenadores, controladores y receptores de datos, pero son aplicables solamente a determinados sectores. Entre otras, encontramos la Ley de Instituciones del Sector Bancario[31] y el Reglamento para la Protección de

[29] Gaceta Oficial Nº 40.340 del 23 de enero de 2014.

[30] Al respecto, Moncho comenta que «(…) la Constitución y el ordenamiento jurídico vigente establecen que el particular debe poder acceder a ciertos bienes y servicios básicos, pero el mismo artículo 117 establece que el particular debe tener el derecho a elegir. Esa posibilidad de elección vendrá dada claramente por el mayor número de opciones posibles a las que el particular pueda tener acceso al momento de la toma de decisiones sobre la adquisición de un bien o servicio, una mayor oferta. (...) La consecuencia absoluta y directa de esa fijación de precios por debajo de los niveles de ganancia y costos necesarios es el cese en la producción, importación y comercialización, que se traduce evidentemente en un desabastecimiento paulatino pero fatal que en definitiva lo que hace es limitar cada vez más las opciones del consumidor y, por lo tanto, incumplir con la garantía contemplada en el artículo 117.» Moncho Stefani, Rodrigo. 2012. «Comentarios sobre la inconstitucionalidad de la Ley de Costo y Precios Justos.» *Anuario de Derecho Público* (Centro de Estudios de Derecho Público de la Universidad Monteávila) (5): 219-242. Último acceso: 16 de julio de 2024. http://ulpiano.org.ve/revistas/bases/artic/texto/ADPUB-MONTEAVILA/5/ADPUB_2012_5_219-242.pdf.

[31] Gaceta Oficial Nº 40.557, 8 de diciembre de 2014.

los Derechos de los Usuarios en la prestación de los Servicios de Telecomunicaciones[32]. También resultan aplicables las normas generales de responsabilidad civil contractual y extracontractual establecido en nuestro Código Civil[33].

### 2.3 Reglamento para la Protección de los Derechos de los Usuarios en la Prestación de los Servicios de Telecomunicaciones

El Reglamento para la Protección de los Derechos de los Usuarios en la Prestación de los Servicios de Telecomunicaciones tiene por objeto establecer las disposiciones que garanticen a los ciudadanos, el acceso a los servicios de telecomunicaciones en forma igualitaria y la prestación de los mismos en adecuadas condiciones de calidad, privacidad y continuidad, de conformidad con lo previsto en la Constitución, la Ley Orgánica de Telecomunicaciones y la normativa aplicable.

El Reglamento aplica a los operadores de telecomunicaciones que presten servicios en el país y a los ciudadanos en su condición de usuarios y abonados de tales servicios. Ello en las relaciones entre ellos regidas por los contratos de servicios, que el propio Reglamento define como contratos de adhesión (artículo 10.10).

- De acuerdo con el artículo 10.8 del Reglamento, los operadores son aquellas personas debidamente habilitadas por la Comisión Nacional de Telecomunicaciones, para el establecimiento y explotación de redes y para la prestación de servicios de telecomunicaciones, de conformidad con lo establecido en la Ley Orgánica de Telecomunicaciones y sus reglamentos.
- Por su parte, en su artículo 10.31, el Reglamento define *servicio de telecomunicaciones* como aquella actividad prestacional dirigida a satisfacer necesidades de telecomunicaciones, a través de la operación de una red de telecomunicaciones propia o de un tercero y de la realización de las actividades complementarias que sean necesarias para tal fin.
- De acuerdo con la Ley Orgánica de Telecomunicaciones[34], *telecomunicaciones* es toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos, u otros medios electromagnéticos afines.

En cuanto a la privacidad y protección de la información personal, el Reglamento:

- En su artículo 7, exige a los operadores la implementación de mecanismos para resguardar el secreto e inviolabilidad de las comunicaciones privadas que cursen a través de sus redes.
- En su artículo 30, exige a los operadores de servicios de telecomunicaciones la adopción de mecanismos que garanticen la confidencialidad de los datos personales suministrados por los abonados en la contratación de los servicios. En este caso particular, el Reglamento prohíbe expresamente la utilización de datos para la elaboración de bases de datos con fines comerciales o publicitarios, salvo que medie autorización expresa y escrita por parte del

[32] Gaceta Oficial Nº 41.533 del 27 de noviembre de 2018.

[33] Gaceta Oficial Nº 2.990 Extraordinario del 26 de julio de 1982.

[34] Gaceta Oficial Nº 39.610 del 7 de febrero de 2011.

usuario, sin que esta autorización pueda establecerse como condición o requisito para la contratación de servicios de telecomunicaciones.

- En su artículo 8, exige a los operadores hacer uso de las herramientas técnicas e implementar procedimientos apropiados para prevenir la comisión de delitos informáticos, especialmente, aquellos que puedan afectar los derechos de privacidad, continuidad y calidad, y hacer seguimiento periódico de los mecanismos adoptados en sus redes para tal fin.

### 2.4 Ley Especial contra los Delitos Informáticos

Promulgada en 2001, la Ley Especial Contra los Delitos Informáticos[35], la cual tiene alcance extraterritorial, tiene por objeto la protección de sistemas de información, así como sus componentes, de cualquier delito cometido contra los mismos o por medio de su uso. En su artículo 11, esta Ley sanciona con prisión de 3 a 6 años a toda persona que obtenga, revele o difunda indebidamente la información o data contenida en un sistema de tecnología de información o sus componentes. Esta sanción se aumentará en la mitad a dos tercios en caso de que la revelación o uso de la información afecte o resulte en algún daño a personas naturales o jurídicas.

La Ley también sanciona, en su artículo 13, a quienes, a través del uso de tecnologías de información, accedan, intercepten, interfieran, manipulen o usen de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro.

La inclusión de ambas normas dentro del marco de esta Ley Especial tiene dos efectos especialmente importantes en el marco de la protección de la información personal. El primero es el reconocimiento expreso de la información como un bien intangible que puede tener valor comercial en sí misma, o que puede ser de utilidad para propósitos comerciales. El segundo es la tipificación del acceso y uso no autorizado a sistemas informáticos como un delito.

### 2.5 Ley de Mensajes de Datos y Firmas Electrónicas

Aunque la Ley de Mensajes de Datos y Firmas Electrónicas[36] no establece medidas expresas para la protección de la información personal, sí somete a los Mensajes de Datos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal. Bajo esta Ley, los Mensajes de Datos son toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

### 2.6 Otras normas que tratan la protección de la información de los consumidores y la aplicación de las normas de responsabilidad civil del Código Civil

Además de las anteriores normas, existen una serie de instrumentos de distintos rangos que contienen normas relacionadas con la protección de la información de usuarios en industrias y áreas específicas. Por ejemplo, el Reglamento para la Protección de los Derechos de los Usuarios

[35] Gaceta Oficial Nº 37.313 del 30 de octubre de 2001.

[36] Gaceta Oficial Nº 37.148 del 28 de febrero de 2001. La Ley de Mensajes de Datos y Firmas Electrónicas tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

en la Prestación de los Servicios de Telecomunicaciones, la Ley de las Instituciones del Sector Bancario, la Ley de la Actividad Aseguradora, la Ley para el Control de los Casinos, Salas de Bingo y Máquinas Traganíqueles y su Reglamento, la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, entre otras.

Por ejemplo, la Ley de Instituciones del Sector Bancario, en su artículo 97, prohíbe expresamente que las bases de datos principales llevadas por los bancos se trasladen fuera del territorio nacional indicando, además, que las mismas tienen carácter confidencial y solo deberán ser utilizadas para los fines autorizados por las Leyes.

Esta Ley refuerza esta protección de la información de los usuarios al prohibir, en su artículo 90, a las instituciones bancarias a informar los antecedentes financieros personales de sus usuarios a cualquier persona natural o jurídica y organismos públicos o privados, con excepción del mismo usuario, la Superintendencia de las Instituciones del Sector Bancario, el Banco Central de Venezuela y demás entes autorizados por la Ley, salvo que el usuario autorice por escrito a la institución. Esta autorización podrá ser revocada en cualquier momento por el usuario.

También vale la pena mencionar las «Normas relativas a la recopilación o captación de datos personales de los solicitantes de los servicios de telefonía móvil y telefonía fija, a través de redes inalámbricas o números no geográficos con servicios de voz nómada»[37], las cuales abarcan temas como suministro de datos, conservación de datos, captura de firmas, registros de servicios de datos, de detalles de llamadas y de mensajes de texto, entre otros.

Visto todo lo anterior, y ante la ausencia de una legislación especial y actualizada en materia de protección al consumidor, podrían resultar aplicables las normas de responsabilidad civil contractual y extracontractual de nuestro Código Civil a (i) los contratos entre proveedores y usuarios y (ii) los almacenadores y receptores de información personal.

Sin ánimos de abundar demasiado en este punto, bajo el artículo 1.185 del Código Civil, los almacenadores y receptores de información personal podrían resultar responsables civilmente por el uso negligente, imprudente o no autorizado de la información personal, el cual genere un daño al usuario. Por su parte, bajo el artículo 1.146, el usuario podría solicitar la nulidad del contrato y reclamar daños y perjuicios en caso de que considere que existió un vicio en el consentimiento al celebrarlo o en su autorización para el uso de su información personal.

## III. EL ABUSO DE LA POSICIÓN DE DOMINIO EN LA LEY ANTIMONOPOLIO

La Ley Antimonopolio[38] fue promulgada en 2014 con el objeto de promover, proteger y regular el ejercicio de la competencia económica justa.[39] Para este fin, el legislador limita o prohíbe de

[37] Providencia Administrativa N° 171 del 20 de septiembre de 2017 de la Comisión Nacional de Telecomunicaciones (CONATEL), mediante la cual se dictan las Normas relativas a la recopilación o captación de datos personales de los solicitantes de los servicios de telefonía móvil y telefonía fija, a través de redes inalámbricas o números no geográficos con servicios de voz nómada, publicada en Gaceta Oficial N° 41.265 del 26 de octubre de 2017.

[38] Gaceta Oficial N° 40.549 del 26 de noviembre de 2014.

[39] Mientras que la Ley Antimonopolio pareciera estar destinada al beneficio de los consumidores, es importante resaltar que no todos concuerdan con dicha interpretación. Al respecto, Mónaco sostiene que «[m]ás allá que la norma que se comenta exprese que el objetivo de la Ley Antimonopolio será la proscripción de las conductas anticompetitivas que ella indica expresamente, puede apreciarse que el fin de esta pareciera más propio de una actividad administrativa de fomento de la producción nacional, que en función de la protección de los consumidores, que son en última instancia, y como hemos señalado, el bien jurídico fundamental que persigue tutelar el Derecho de la Competencia.» Monaco,

forma general las conductas, prácticas, acuerdos, convenios, contratos o decisiones que impidan, restrinjan, falseen o limiten la competencia económica (artículo 4).

Específicamente, la Ley incluye disposiciones, entre otras, contra la ejecución de *conductas manipuladoras*[40]; prohibiciones de los acuerdos que restrinjan o impidan la competencia económica entre los miembros de asociaciones, federaciones y otros grupos de sujetos regulados por la Ley[41]; prohibiciones de la celebración de contratos entre sujetos regulados por la Ley en la que se establezcan precios y contratación para la venta de bienes o prestación de servicios a terceros y que produzcan o puedan producir la restricción, falseamiento, limitación o impedimento de competencia económica justa[42]; y prohibiciones de acuerdos, decisiones o recomendaciones colectivas y concertadas para los fines contemplados en la norma[43].

De relevancia para este trabajo, la Ley prohíbe de forma general el abuso de la posición de dominio por uno o varios sujetos de la Ley (artículo 12) y específicamente las siguientes prácticas:

- La imposición discriminatoria de precios y otras condiciones de comercialización o de servicios.
- La limitación injustificada de la producción, de la distribución o del desarrollo técnico o tecnológico en perjuicio de las empresas o de los consumidores.
- La negativa injustificada a satisfacer las demandas de compra de productos o de prestación de servicios.
- La aplicación, en las relaciones comerciales o de servicios, de condiciones desiguales para prestaciones equivalentes que coloquen a unos competidores en situación de desventaja frente a otros.
- La subordinación de la celebración de contratos a la aceptación de prestaciones suplementarias que, por su naturaleza o con arreglo a los usos del comercio, no guarden relación con el objeto de tales contratos.

Miguel. 2016. «El Derecho de la Competencia y la Ley Antimonopolio en la segunda década del Siglo XXI o del Segundo Libro de la Poética de Aristóteles y Guillermo de Baskerville.» *Revista Electrónica de Derecho Administrativo Venezolano N° 10/2016* 233-246. https://redav.com.ve/wp-content/uploads/2017/11/El-derecho-de-la-competencia-y-la-Ley-antimonopolio- n-la-segunda-de%CC%81cada-del-siglo-XXI-MM.pdf.

[40] Artículo 7 – Ley Antimonopolio. Se prohíbe toda conducta tendiente a manipular los factores de producción, distribución, comercialización, desarrollo tecnológico o inversiones, en perjuicio de la competencia económica.

[41] Artículo 8 – Ley Antimonopolio. Se prohíben los acuerdos o convenios, que se celebren directamente o a través de uniones, asociaciones, federaciones, cooperativas y otras agrupaciones de sujetos de aplicación de este Decreto con Rango, Valor y Fuerza de Ley, que restrinjan o impidan la competencia económica entre sus miembros. Son nulos los acuerdos o decisiones tomados en asambleas de los sujetos de aplicación de este Decreto con Rango, Valor y Fuerza de Ley, que restrinjan o impidan la competencia económica.

[42] Artículo 11 – Ley Antimonopolio. Se prohíben los contratos entre los sujetos de aplicación del presente Decreto con Rango, Valor y Fuerza de Ley, en los que se establezcan precios y condiciones de contratación para la venta de bienes o prestación de servicios a terceros, y que produzcan o puedan producir el efecto de restringir, falsear, limitar o impedir la competencia económica justa, en todo o parte del mercado.

[43] Artículo 9 – Ley Antimonopolio. Se prohíben los acuerdos, decisiones o recomendaciones colectivas o prácticas concertadas para: 1. Fijar, de forma directa o indirecta, precios y otras condiciones de comercialización o de servicio. 2. Limitar la producción, la distribución, comercialización y el desarrollo técnico o tecnológico. 3. Restringir inversiones para innovación, investigación y desarrollo. 4. Repartir los mercados, áreas territoriales, sectores de suministro o fuentes de aprovisionamiento entre competidores. 5. Aplicar en las relaciones comerciales o de servicios, condiciones desiguales para prestaciones equivalentes que coloquen a unos competidores en situación de desventaja frente a otros. 6. Subordinar o condicionar la celebración de contratos a la aceptación de prestaciones suplementarias que, por su naturaleza o con arreglo a los usos del comercio, no guarden relación con el objeto de tales contratos.

De acuerdo con el artículo 13, la posición de dominio se verifica cuando:

- Una actividad económica sea realizada por una sola persona o grupo de personas vinculadas entre sí[44], en condición de comprador como de vendedor y tanto en su condición de prestador de servicios como en su calidad de usuario de los mismos.
- Exista más de una persona realizando dicha actividad, pero no exista competencia efectiva entre ellas.

La determinación de si existe o no competencia efectiva entre las personas que realizan una actividad económica es una que deben realizar las autoridades competentes considerando, entre otros elementos relevantes, lo siguiente:

- El número de competidores que participen en la respectiva actividad.
- La cuota de participación de cada competidor en el respectivo mercado, así como su capacidad instalada.
- La demanda del respectivo producto o servicio.
- La innovación tecnológica que afecte el mercado de la respectiva actividad.
- La posibilidad legal y fáctica de competencia potencial en el futuro.
- El acceso de los competidores a fuentes de financiamiento y suministro, así como a las redes de distribución.

En este punto es importante mencionar que la Ley excluye expresamente de su ámbito de aplicación a las empresas mixtas o públicas del Estado en sectores estratégicos. Esta circunstancia afecta directamente a la competencia al discriminar entre empresas privadas y aquellas con participación accionaria mayoritaria del Estado. En efecto, el Estado a través de su empresa puede en efecto abusar de su posición de dominio que viene dada, precisamente, por la magnitud de sus operaciones, capacidad económica y alcance territorial. Esta disposición, no solo es inconstitucional por violar el derecho a la igualdad, sino que es irracional porque no hay justificación para que el Estado pueda potencialmente realizar conductas en detrimento de la plena competencia[45]. Además, va en contra del derecho universal de los ciudadanos a acceder

[44] Según el artículo 14 de la Ley, Se tendrá como personas vinculadas entre sí, las siguientes: 1.- Personas que tengan una participación del cincuenta por ciento (50%) o más del capital de la otra, o ejerzan de cualquier otra forma el control sobre ella. 2. Las personas cuyo capital posea el cincuenta por ciento (50%) o más, de las personas indicadas en el ordinal anterior, o que estén sometidas al control por parte de ellas. 3. Las personas que, de alguna forma, estén sometidas al control de las personas que se señalan en los numerales anteriores. Adicionalmente, se entiende por control a la posibilidad que tiene una persona para ejercer una influencia decisiva sobre las actividades de uno de los sujetos de regulados por esta Ley, sea mediante el ejercicio de los derechos de propiedad o de uso de la totalidad o parte de los activos de éste, o mediante el ejercicio de derechos o contratos que permitan influir decisivamente sobre la composición, las deliberaciones o las decisiones de los órganos del mismo o sobre sus actividades.

[45] Al respecto, Mónaco tilda esta disposición de inconstitucional e irracional, comentando que es «inconstitucional por cuanto crea una discriminación injustificada entre empresas que pueden competir en un mismo sector y, por lo tanto, que se encuentran en una misma situación jurídica, lo cual viola el artículo 21 de la Constitución de la República Bolivariana de Venezuela que consagra el derecho a la igualdad. Irracional porque no existe una justificación válida para tolerar que un sujeto pueda realizar una conducta que se considera ilícita y violatoria de bienes jurídicos y derechos tutelados por una ley, e incluso, que puedan existir situaciones, como el caso de prácticas concertadas, donde un sujeto pueda ser sancionado por una conducta ilícita y otro no, sólo por el hecho que este último se trate de un ente público

a bienes y servicios de calidad. Ello porque la exclusión de las empresas del Estado de las disposiciones de la Ley Antimonopolio y la consecuente supresión de una competencia efectiva del sector privado reduce la capacidad del Estado de generar *valor público* con los bienes y servicios que presta para atender las necesidades, demandas e intereses de la ciudadanía.[46]

## IV. LA AUSENCIA DE NORMAS ACTUALIZADAS Y ESPECÍFICAS EN MATERIA DE PROTECCIÓN DE DATOS E INTERCAMBIO DE INFORMACIÓN PODRÍA RESULTAR EN EL ABUSO DE POSICIÓN DE DOMINIO DE LAS EMPRESAS TECNOLÓGICAS CON ACCESO A LA INFORMACION PERSONAL DE SUS USUARIOS

En esta sección desarrollaremos por qué y cómo, en nuestro criterio, la ausencia de normas actualizadas y específicas en materia de protección de datos e intercambio de información podría resultar en el abuso de posición de dominio bajo la Ley Antimonopolio.

Lo primero que hay que destacar es que la ausencia de normas actualizadas y específicas en esta materia conduce a que la protección de la información personal en la provisión de bienes y servicios en línea quede principalmente regulada por las cláusulas contenidas en los contratos de adhesión celebrados entre los proveedores y los consumidores, donde estos últimos tienen poco o ningún poder real de negociación.

En este contexto, el titular de la información podría no tener control efectivo sobre el uso que se le da a la información que suministra conscientemente (*e.g.,* mediante la aceptación expresa del contrato) o inconscientemente (*e.g.,* por la recopilación y depuración de los hábitos, modalidades y medios de consumo del servicio). Sobre todo, considerando que, a nivel global, existen miles de millones de usuarios de estos bienes y servicios digitales, pero un número limitado de proveedores de bienes y servicios digitales.

Esto ha llevado al mercado digital global donde la información personal de esos millones de usuarios es un bien valorable (y de muy alto valor) y transable. En otras palabras, tras la recolección de la información personal, las empresas autorizadas para tal recolección y almacenamiento puede utilizarla y enajenarla y ser transada por una empresa solo para ser cedida a entidades relacionadas o terceras partes con fines comerciales. Como han advertido diversos autores[47], la recolección y cesión de información personal se ha vuelto «el nuevo petróleo», permitiendo a las empresas y plataformas digitales acceder a nuevas oportunidades de mercado y usarlo como base para la toma de decisiones de negocio.

Por ejemplo, entre estas oportunidades, encontramos las actividades de mercadeo cruzado entre plataformas y publicidad personalizada y dirigida con base en la propia información personal. Aquí, los proveedores de bienes y servicios pueden acordar entre sí el intercambio de

exceptuado de la aplicación de la Ley Antimonopolio, cuando más bien este tipo de instituciones deberían observar con más razón la ley.» Monaco, Miguel. 2016. «El Derecho de la Competencia...»

[46] Sobre la generación de *valor público* por el Estado en el marco de su actividad empresarial, Andrade Cifuentes, Ignacio Julio, elaboró y presentó el 8 de junio de 2024, un trabajo de investigación para un número especial de la Revista de Facultad de Derecho de la Universidad Católica Andrés Bello referido a las tendencias actuales de las compras públicas, cuyo título es «Valor público, Responsabilidad Social y Compras Públicas: Replanteando el «Compromiso de Responsabilidad Social» del Decreto-Ley de Contrataciones Públicas», el cual está pendiente de publicación. También, se sugiere la revisión de Moore, Mark. 1998. *Gestión estratégica y creación de valor en el sector público*. Barcelona: Paidos.

[47] Fischmann, Brett. 2018. *Here's why tech companies abuse our data: because we let them.* 10 de abril. Último acceso: 16 de julio de 2024. https://www.theguardian.com/commentisfree/2018/apr/10/tech-companies-data-online-transactions-friction.

información para promover los bienes y servicios de cada uno de ellos en la plataforma del otro. También pueden dirigir y personalizar la publicidad con base en, por ejemplo, los hábitos de consumo del usuario, el acceso a publicaciones en redes sociales, historial de navegación en la web y la utilización de dispositivos electrónicos como relojes, para alcanzar directamente a un usuario determinado, quien, muy probablemente, no pueda resistir la publicidad.

De esta forma, mucha información personal es recolectada y utilizada con fines comerciales en formas y momentos que los usuarios quizás no conozcan, no estén conscientes o no comprendan del todo cuando aceptan los términos y condiciones de cada plataforma. Por eso, organizaciones como la Unión Europea han tomado cartas en el asunto y ejecutados proyectos normativos para asegurar que la información recolectada durante el comercio electrónico sea debidamente protegida por instrumentos.

En el caso de la Unión Europea, estos instrumentos incluyen el *General Data Protection Regulation* (*GDPR*) que es una regulación especializada y actualizada en la materia y la Carta de la Unión Europea de Derechos Fundamentales, la cual establece la protección expresa de la data de los ciudadanos en su artículo 8. Un breve vistazo a las regulaciones del *GDPR* en cuanto al consentimiento del usuario en el uso de sus datos revelan el espíritu *preventivo* del instrumento, algo que contrasta con el carácter *ex post* o reactivo de muchas de las disposiciones venezolanas en la materia.

En relación con el consentimiento para la recolección y uso de datos personales regulado en el *GDPR*, este instrumento requiere que el consentimiento sea específico, informado, no ambiguo y revocable, además de resultar una manifestación inequívoca de intención. En este sentido, «las empresas no podrán obtener consentimiento válido utilizando un modelo de optación-negativa, en el cual la ausencia de rechazo del usuario supuestamente indica su consentimiento» (traducción libre).[48]

Adicionalmente, el GDPR exige que el consentimiento se haya otorgado libremente o con intención. Este requisito restringe, por ejemplo, la posibilidad de establecer contractualmente condiciones «todo-o-nada» con respecto a la privacidad[49], dentro de las cuales encontramos, por ejemplo, aquellas que permiten ingresar a un sitio web solo si el usuario acepta «ser rastreado» por terceros.

Asimismo, autores han señalado que, con base en el GDPR, el empleo de frases genéricas como «su data será utilizada para propósitos comerciales» no son suficientes para obtener consentimiento válido. En cambio, la normativa exige que los usuarios sean debida y completamente informados sobre los usos de su información, con quién se compartirá y deben tener opciones para rechazar o aceptar estas disposiciones.

Ante la derogatoria de la Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios, en Venezuela no existe, actualmente, normas parecidas al GDPR, e incluso esa normativa resultaría insuficiente para satisfacer las demandas actuales en materia de protección de datos que el acelerado crecimiento de la provisión de bienes y servicios digitales. De esta forma, las compañías dedicadas al comercio digital pueden fácilmente recopilar y compartir datos «sin fricción»[50] por parte de los consumidores, con poco riesgo de que las autoridades intervengan y con cierta facilidad para utilizar, ceder y comercializar esta información.

---

[48] Hoofnagle, Chris Jay, Bart van der Sloot, y Frederik Zuiderveen Borgesius. 2019. «The European Union General Data Protection Regulation: what it is and what it means» *Information & Communications Technology Law* 28 (1). Último acceso: 16 de julio de 2024.

[49] *Ibid.*

[50] Fischmann, Brett. 2018. *Here's why tech companies…*

En nuestro criterio, esta situación fomenta las posiciones de dominio. Siendo la información un activo tan valioso, las empresas digitales tendrán una posición de dominio en la medida de que acumulen mayores cantidades de información de sus usuarios. Recordando lo estipulado en los artículos 12 y 13 de la Ley Antimonopolio que se transcriben en pie de página a fines referenciales[51], la ausencia de normas de protección de datos podría generar una situación en la que, aun existiendo más de una persona para la realización de una actividad, no haya competencia efectiva entre ellas. De esta forma, se genera una posición de dominio, la cual puede ser abusada mediante la explotación de la información con pocas o sin restricciones, obteniendo así ventajas competitivas injustificadas sobre su competencia sin acceso a tantos datos.

De esta forma, la ausencia de normas de protección de datos podría permitir a las empresas en posición dominante a crear barreras de entrada a los demás competidores. En efecto, el control de grandes cantidades de información les permitiría obstaculizar la capacidad de nuevos actores o actores más pequeños a ingresar al mercado o competir efectivamente. El establecimiento de normas robustas en materia de protección de datos podría ayudar a aliviar estas barreras de entrada garantizando un acceso equitativo a, y uso controlado de, la información.

Asimismo, las empresas en posición de dominio pueden hacer uso indebido o no autorizado de la información de los usuarios para, por ejemplo, elaborar perfiles de los clientes de la competencia y diseñar ofertas personalizadas y dirigidas directamente a ellos para atraerlos. También podrían diseñar un esquema discriminatorio de precios de productos basado en el análisis de datos. En general, podría crear ventajas competitivas que los nuevos actores o actores más pequeños difícilmente superarán en el desarrollo y comercialización de bienes y servicios.

Por otro lado, el consumidor y el mercado en general también podrían verse afectados. Las empresas que almacenan y usan la información y los datos pueden infringir, hasta sin intención, la privacidad de los usuarios. También pueden, como mencionamos arriba, ejecutar actividades de publicidad selectiva basada en la recolección invasiva y desproporcionada de datos. Adicionalmente, las empresas podrían pretender manipular el mercado basado en la gran cantidad de datos recogidos, lo cual podría eventualmente conducir a limitar la capacidad de elección del consumidor. Finalmente, el abuso de una posición de dominio podría conducir a un alza en los precios o una reducción en la calidad del bien y servicio prestado, precisamente por la disminución de competencia efectiva.

---

[51] Artículo 12 – Ley Antimonopolio. Se prohíbe el abuso por parte de uno o varios de los sujetos de aplicación del presente Decreto con Rango, valor y Fuerza de Ley, de su posición de dominio, en todo o parte del mercado nacional y, en particular, quedan prohibidas las siguientes prácticas: 1. La imposición discriminatoria de precios y otras condiciones de comercialización o de servicios. 2. La limitación injustificada de la producción, de la distribución o del desarrollo técnico o tecnológico en perjuicio de las empresas o de los consumidores. 3. La negativa injustificada a satisfacer las demandas de compra de productos o de prestación de servicios. 4. La aplicación, en las relaciones comerciales o de servicios, de condiciones desiguales para prestaciones equivalentes que coloquen a unos competidores en situación de desventaja frente a otros. 5. La subordinación de la celebración de contratos a la aceptación de prestaciones suplementarias que, por su naturaleza o con arreglo a los usos del comercio, no guarden relación con el objeto de tales contratos.

Artículo 13 – Ley Antimonopolio. Existe posición de dominio: 1. Cuando determinada actividad económica es realizada por una sola persona o grupo de personas vinculadas entre sí, tanto en condición de comprador como de vendedor y tanto en su condición de prestador de servicios como en su calidad de usuario de los mismos. 2. Cuando existiendo más de una persona para la realización de determinado tipo de actividad, no haya entre ellas competencia efectiva. Cuando exista posición de dominio, las personas que se encuentren en esa situación, se ajustarán a las disposiciones previstas en este Decreto con Rango, Valor y Fuerza de Ley, en cuanto no se hayan establecido condiciones distintas en los cuerpos normativos que la regulen, conforme a lo dispuesto en el artículo 113 de la Constitución de la República Bolivariana de Venezuela.

No es muy difícil imaginar un operador de una plataforma de mercado en línea con posición de dominio que, al poder ver los patrones de compra de sus usuarios en tiempo real, decide invertir en empresas que satisfagan esas necesidades comerciales o constituyan competidores directos a las empresas que habitan su plataforma. El operador podría fácilmente determinar qué productos quedan a la vista de los usuarios, mientras esconde a sus rivales. Así, el operador del mercado podría volverse competidor en el mercado que controla de forma completa.

También podría ocurrir que una plataforma de redes sociales con posición de dominio pretenda recoger grandes cantidades de información de sus usuarios sin su consentimiento expreso ni con transparencia y utilizar esos datos para, por ejemplo, (i) diseñar campañas publicitarias dirigidas y muy selectivas, dándole una ventaja injustificada sobre sus competidores; (ii) estudiar los datos recogidos para entender las debilidades de su competencia más pequeña y, con base en ello, pretender adquirirlos; o (iii) fijar precios discriminatorios basados en la información y datos de los usuarios.

En Venezuela deben dictarse normas que busquen prevenir este tipo de situaciones; es decir, con mayor énfasis la *prevención* de daños derivados del uso comercial indiscriminado de la información personal, que en la reparación de un daño ya ocurrido. Una Ley que podría ser interesante estudiar por disponer normas preventivas es la Ley de Protección de Datos Personales (PDPL)[52] de la República Argentina. En particular, esta Ley establece limitaciones a la transferencia de la información recopilada[53], incluye la obligación de facilitar a las personas acceso a sus datos almacenados, establece mecanismos para corregir los registros de la información en caso de error[54] y establece obligaciones de confidencialidad de la información[55].

---

[52] Ley No. 25.326, Ley de Protección de Datos Personales, publicada en Boletín Nacional del 2 de noviembre de 2000 (PDPL).

[53] Artículo 12 – PDPL. 1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. 2. La prohibición no regirá en los siguientes supuestos: a) Colaboración judicial internacional; b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior; c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

[54] Artículo 21 – PDPL. 1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control. 2. El registro de archivos de datos debe comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos. 3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley.

[55] Artículo 16 – PDPL. 1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. 2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. 3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley. 4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del

De esta forma, una norma que contemple tanto mecanismos de prevención como mecanismos de reparación es fundamental al momento de diseñar y dictar una norma local.

## V. CONCLUSIONES

En la economía digital venezolana, urge una legislación robusta en protección de datos que mitigue riesgos para los usuarios y asegure una competencia justa. Sin estas normas, las empresas con acceso a grandes volúmenes de información seguirán acumulando ventajas competitivas injustificadas, obstaculizando la libre competencia y afectando negativamente a los consumidores. Actualmente existe un ordenamiento jurídico que busca reparar daños en vez de prevenirlos y, por tanto, surgen situaciones en las que una o varias empresas utilizan la información personal de los consumidores para obtener ventajas competitivas injustificadas sobre su competencia más pequeña, obteniendo una posición de dominio y posiblemente abusando de ella.

De esta forma, en Venezuela deben dictarse normas que busquen prevenir este tipo de situaciones. Esto es: con mayor énfasis la *prevención* de daños derivados del uso comercial indiscriminado de la información personal, que en la reparación de un daño ya ocurrido (como lo hace la Ley de Protección de Datos Personales (PDPL)[56] de la República Argentina). En efecto, una regulación sólida de protección de datos puede prevenir daños derivados de la recopilación y el tratamiento de datos, exigir claridad y transparencia en cuanto al uso de los datos, dar a las personas el control sobre el uso de sus datos personales, imponer sanciones por el uso indebido de los datos y promover una competencia justa y honesta.

Ello contribuiría a evitar prácticas anticompetitivas mediante el uso indiscriminado de los datos y, en particular, el abuso de posiciones dominantes en el mercado. Todo ello es fundamental para mantener un ecosistema digital saludable al fomentar la competencia honesta y proteger los datos personales.

## BIBLIOGRAFÍA


- 2005. Sentencia Nº 182 (Sala Constitucional del Tribunal Supremo de Justicia, 8 de marzo).
- Arenas, Vanessa. 2022. *La app venezolana de delivery, Yummy, levanta US$ 47 millones para expandirse en Latinoamérica.* 2 de junio. Último acceso: 16 de julio de 2024. https://forbes.cl/negocios/2022-06-02/la-app-venezolana-de-delivery-yummy-levanta-us-47-millones-para-expandirse-en-latinoamerica.
- Brewer Carías, Allan. s.f. «El proceso constitucional de las acciones de habeas data en Venezuela: las sentencias de la Sala Constitucional como fuente del derecho procesal constitucional.» Último acceso: 14 de julio de 2024. https://allanbrewercarias.net/Content/449725d9-f1cb-474b-8ab2-


quinto día hábil de efectuado el tratamiento del dato. 5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión. 7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

[56] Ley No. 25.326, Ley de Protección de Datos Personales, publicada en Boletín Nacional del 2 de noviembre de 2000 (PDPL).

41efb849fea8/Content/II,%204,%20638.%20PROCEDIMIENTO%20EN%20LAS%20ACCIONES%20DE%20HABEAS%20DATA.%201-10.doc.pdf.

- Brewer-Carías, Allan. 2011. «El Amparo Constitucional en Venezuela.» *Revista IUS* (Centro Internacional de Estudios sobre Ley y Derecho) 5 (27). https://www.revistaius.com/index.php/ius/article/view/88.
- Chavero Gazdik, Rafael. 2001. *El Nuevo Régimen de Amparo Constitucional.* Caracas: Editorial Sherwood.
- «Código Civil (Gaceta Oficial Nº 2.990 Extraordinario, 26 de julio de 1982).»
- Comisión Nacional de Telecomunicaciones (CONATEL). «Normas relativas a la recopilación o captación de datos personales de los solicitantes de los servicios de telefonía móvil y telefonía fija, a través de redes inalámbricas o números no geográficos con servicios de voz nómada.» Providencia Nº 171 del 20 de septiembre de 2017 (Gaceta Oficial Nº 41.265, 26 de octubre de 2017).
- «Constitución de la República Bolivariana de Venezuela (Gaceta Oficial Nº 5.908 Extraordinario, 19 de febrero de 2009).»
- «Decreto-Ley Antimonopolio (Gaceta Oficial Nº 40.549, 26 de noviembre de 2014).»
- «Decreto-Ley de Instituciones del Sector Bancario (Gaceta Oficial Nº 40.557, 8 de diciembre de 2014).»
- «Decreto-Ley Orgánica de Precios Justos (Gaceta Oficial Nº 40.340, 23 de enero de 2014).»
- El Interés. 2024. *Más trabajo y mayores sueldos: así es el próspero negocio de delivery en Venezuela.* 23 de abril. Último acceso: 16 de julio de 2024. https://elestimulo.com/elinteres/empresas/2024-04-23/el-negocio-del-delivery-prospera-en-venezuela-estudio/.
- Fischmann, Brett. 2018. *Here's why tech companies abuse our data: because we let them.* 10 de abril. Último acceso: 16 de julio de 2024. https://www.theguardian.com/commentisfree/2018/apr/10/tech-companies-data-online-transactions-friction.
- García, Carilym. 2018. «Habeas Data como mecanismo de protección del derecho al acceso a la información personal en el derecho constitucional venezolano.» *Data Ciencia - Revista Multidisciplinaria Electrónica del Núcleo LUZ - Costa Oriental del Lago* 1 (1). Último acceso: 14 de julio de 2024.
- Herníquez Maionica, Giancarlo. 2003. «El habeas data y el derecho de la persona con trastornos de identidad de género a obtener documentos relativos a su identidad biológica.» *Revista de Derecho Constitucional Nº 8* 67-80. http://www.ulpiano.org.ve/revistas/bases/artic/texto/RDCONS/8/rdcons_2003_8_67-80.pdf.
- Hoofnagle, Chris Jay, Bart van der Sloot, y Frederik Zuiderveen Borgesius. 2019. «The European Union General Data Protection Regulation: what it is and what it means.» *Information & Communications Technology Law* 28 (1). Último acceso: 16 de julio de 2024.
- *Insaca vs. Ministerio de Sanidad y Asistencia Social.* 2001. Sentencia Nº 332 (Sala Constitucional del Tribunal Supremo de Justicia, 14 de mayo).

- Kalra, Aditya, y Steve Stecklow. 2021. *Amazon copied products and rigged search results to promote its own brands, documents show.* 13 de octubre. Último acceso: 16 de julio de 2024. https://www.reuters.com/investigates/special-report/amazon-india-rigging/.
- Kemp, Simon. 2024. *Digital 2024 April Global Statshot Report.* 24 de abril. Último acceso: 14 de julio de 2024. https://datareportal.com/reports/digital-2024-april-global-statshot.
- «Ley de Mensajes de Datos y Firmas Electrónicas (Gaceta Oficial Nº 37.148, 28 de febrero de 2001).»
- «Ley Especial contra los Delitos Informáticos (Gaceta Oficial Nº 37.313, 30 de octubre de 2001).»
- «Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales (Gaceta Oficial Nº 34.060, 27 de septiembre de 1988).»
- «Ley Orgánica de Telecomunicaciones (Gaceta Oficial Nº 39.610, 7 de febrero de 2011).»
- «Ley Orgánica del Tribunal Supremo de Justicia (Gaceta Oficial Nº 6.684 Extraordinario, 19 de enero de 2022).»
- «Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios (Gaceta Oficial Nº 39.358, 1 de febrero de 2010).»
- «Ley No. 25.326, Ley de Protección de Datos Personales, publicada en Boletín Nacional del 2 de noviembre de 2000 (PDPL)»
- Monaco, Miguel. 2016. «El Derecho de la Competencia y la Ley Antimonopolio en la segunda década del Siglo XXI o del Segundo Libro de la Poética de Aristóteles y Guillermo de Baskerville.» *Revista Electrónica de Derecho Administrativo Venezolano Nº 10/2016* 233-246. Último acceso: 16 de julio de 2024. https://redav.com.ve/wp-content/uploads/2017/11/El-derecho-de-la-competencia-y-la-Ley-antimonopolio-_n-la-segunda-de%CC%81cada-del-siglo-XXI-MM.pdf.
- Moncho Stefani, Rodrigo. 2012. «Comentarios sobre la inconstitucionalidad de la Ley de Costo y Precios Justos.» *Anuario de Derecho Público* (Centro de Estudios de Derecho Público de la Universidad Monteávila) (5): 219-242. Último acceso: 16 de julio de 2024. http://ulpiano.org.ve/revistas/bases/artic/texto/ADPUB-MONTEAVILA/5/ADPUB_2012_5_219-242.pdf.
- Moore, Mark. 1998. *Gestión estratégica y creación de valor en el sector público.* Barcelona: Paidos.
- Parlamento Europeo. s.f. *Carta de la Unión Europea de Derechos Fundamentales.* Último acceso: 16 de julio de 2024. https://www.europarl.europa.eu/charter/pdf/text_es.pdf.
- Peterson, Michael P. 2005. «A decade of maps and the internet.» Editado por Global Congresos. *XXII International Cartographic Conference*. Coruña: The International Cartographic Association (ICA-ACI). Último acceso: 14 de julio de 2024. https://shorturl.at/9aLZM.
- «Reglamento para la Protección de los Derechos de los Usuarios en la Prestación de los Servicios de Telecomunicaciones (Gaceta Oficial Nº 41.533, 27 de noviembre de 2018).»

- Reuters. 1999. «Internet users now exceed 100 million.» *sitio web de The New York Times*. Último acceso: 1 de julio de 2024. https://www.nytimes.com/1999/11/12/business/internet-users-now-exceed-100-million.html.
- Rondón de Sansó, Hildegaard. 1994. *Amparo Constitucional.* Caracas: Arte.
- —. 2001. *Análisis de la Constitución Venezolana de 1999 (parte orgánica y sistemas)*. Caracas: Ex Libris.
- *Ruth Capriles y otros.* 2000. Sentencia Nº 1050 (Sala Constitucional del Tribunal Supremo de Justicia, 23 de agosto).
- Sagües, Nestor. 1995. *Derecho Procesal Constitucional. Acción de Amparo*. Buenos Aires: Astrea.
- Singh, Shubham. 2024. *How Many Emails Are Sent Per Day in 2024?* 21 de mayo. Último acceso: 14 de julio de 2024. https://www.demandsage.com/how-many-emails-are-sent-per-day/.
- Snyder, Kristy. 2024. *35 e-Commerce statistics of 2024*. 28 de marzo. Último acceso: 14 de julio de 2024. https://shorturl.at/Y8bhC.
- Unión Europea. 2016. *General Data Protection Regulation - GDPR*. Último acceso: 16 de julio de 2024. https://gdpr-info.eu/.
- *Veedores de la UCAB.* 2000. (Sala Constitucional del Tribunal Supremo de Justicia, 23 de agosto).