



## GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA

www.imprenta.gov.co

ISSN 0123 - 9066

AÑO XXXIII - N° 2084

Bogotá, D. C., viernes, 29 de noviembre de 2024

EDICIÓN DE 65 PÁGINAS

DIRECTORES:

SAÚL CRUZ BONILLA

SECRETARIO GENERAL DEL SENADO (e)

www.secretariasenado.gov.co

JAIME LUIS LACOUTURE PEÑALOZA

SECRETARIO GENERAL DE LA CÁMARA

www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

## CÁMARA DE REPRESENTANTES

## PONENCIAS

## INFORME DE PONENCIA POSITIVA PARA PRIMER DEBATE EN LA CÁMARA DE REPRESENTANTES DEL PROYECTO DE LEY ESTATUTARIA NÚMERO 152 DE 2024 CÁMARA

por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales.

Bogotá D.C., Noviembre de 2024

Presidente

**ANA PAOLA GARCIA SOTO**

Comisión Primera Constitucional Permanente

Cámara de Representantes

**Ref.:** Ponencia para primer debate en la Cámara de Representantes del Proyecto de Ley Estatutaria No. 152 de 2024 Cámara "Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales"

Respetada Presidenta.

Atendiendo a la designación realizada por la Mesa Directiva de la Comisión Primera Constitucional Permanente de la Cámara de Representantes mediante oficio C.P.C.P. 3.1. - 0166 - 2024 del veintiocho (28) de Agosto de 2024 y atendiendo a lo dispuesto en el artículo 150 de la Ley 5 de 1992 procedo a someter a consideración de la Comisión Primera Constitucional Permanente el informe de **PONENCIA POSITIVA** para primer debate en la Cámara de Representantes del Proyecto de Ley Estatutaria No. 152 de 2024 - Cámara "**Por medio de la cual se dictan disposiciones para el Régimen General de la Protección de Datos Personales**".

El presente Proyecto de Ley cuenta con setenta y uno (71) artículos incluida la vigencia y tiene como objetivo establecer las normas relativas a la protección de las personas naturales en lo que respecta a la protección y tratamiento de sus datos personales y las normas relativas a la libre circulación de tales datos. De igual manera, la presente ley protege los derechos y garantías fundamentales de las personas naturales y, en particular, su derecho fundamental a la protección de los datos personales, en los términos descritos en el artículo 15 de la Constitución Política.

Cordialmente,

DUVALIER SÁNCHEZ ARANGO  
Representante a la Cámara

JUAN CARLOS WILLS OSPINA  
Representante a la Cámara

GERSSEL LUIS PEREZ ALTAMIRANDA  
Representante a la Cámara

CARLOS FELIPE QUINTERO OVALLE  
Representante a la Cámara

HERNAN DARIO CADAVID MARQUEZ  
Representante a la Cámara

ASTRID SÁNCHEZ MONTES DE OCA  
Representante a la Cámara

DIOGENES QUINTERO AMAYA  
Representante a la Cámara

JÓRGE ALEJANDRO OCAMPO GIRALDO  
Representante a la Cámara

LUIS ALBERTO ALBAN URBANO  
Representante a la Cámara

MARELEN CASTILLO TORRES  
Representante a la Cámara

**INFORME DE PONENCIA PARA PRIMER DEBATE EN LA COMISIÓN PRIMERA CONSTITUCIONAL PERMANENTE DE LA CÁMARA DE REPRESENTANTES**

**Proyecto de Ley Estatutaria No. 152 de 2024 Cámara**

**“Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales”**

**I. TRÁMITE LEGISLATIVO.**

El veintiocho (28) de agosto de 2024 mediante oficio C.P.C.P. 3.1. – 0166 – 2024 la Comisión Primera Constitucional Permanente nos notificó de la designación como ponentes del Presente de Ley Estatutaria en mención.

Este Proyecto de Ley es de autoría principal del Representante a la Cámara María Fernanda Carrascal, en el cual son coautores los Representantes: Duvalier Sánchez Arango, María Fernanda Carrascal Rojas, Luis David Suárez Chadid, Juan Camilo Londoño Barrera, María del Mar Pizarro GarcíaSantiago Osorio Marín, Alejandro García Ríos, Jhon Fredi Valencia Caicedo, Cristóbal Caicedo Angulo, Héctor David Chaparro Chaparro, Cristian Danilo Avendaño Fino, Álvaro Leonel Rueda Caballero, Alirio Uribe Muñoz y los Senadores Ana Carolina Espitia Jerez, Pablo Catatumbo Torres Victoria y Yuly Esmeralda Hernández Silva

Esta ponencia se fundamenta atendiendo a lo dispuesto en los artículos 150, 153 y 156 de la Ley 5 de 1992; por lo anterior se procede a rendir **PONENCIA POSITIVA** ante la Comisión Primera Constitucional Permanente en los siguientes términos:

**II. OBJETO DE LA INICIATIVA.**

La iniciativa legislativa cuenta con setenta y un (71) artículos que tienen como objetivo establecer las normas relativas a la protección y tratamiento de los datos personales de las personas naturales y las normas relativas a la libre circulación de tales datos. De igual manera, la presente ley protege los derechos y garantías fundamentales de las personas naturales y, en particular, su derecho fundamental a la protección de los datos personales, en los términos descritos en el artículo 15 de la Constitución Política.

*la protección de datos, busca que las organizaciones y entidades responsables del tratamiento de datos personales evalúen los posibles riesgos para la privacidad de los titulares y tomen medidas proporcionales para mitigarlos. De esta manera, se promueve una cultura de responsabilidad y se garantiza la implementación de medidas adecuadas para salvaguardar la información personal.*

*El proyecto de ley introduce nuevas bases jurídicas para el tratamiento de datos, eliminando la obligación de depender exclusivamente del consentimiento como único mecanismo. Esto permite a los responsables del tratamiento adaptar sus deberes de información a la realidad del país y al contexto global. Como resultado, el proyecto establece requisitos más efectivos para obtener el consentimiento de los titulares en el tratamiento de sus datos personales, restableciendo su papel como garantes de la voluntad del titular. Esto asegura un mayor control por parte de las personas sobre sus datos personales.*

**3. Justificación del Proyecto de Ley.**

En Colombia hablar de *habeas data* ha tenido un importante desarrollo, existiendo una pluralidad de conceptos, dentro de los cuales se destacan:

- Según el Doctor Liévano<sup>1</sup>, citado por Pérez, el *habeas data* es un instituto jurídico procesal especial que contempla el acceso, conocimiento, renovación, rectificación y supresión de la información por parte de la persona.

Posteriormente, el autor Flórez, citado por Pérez, señala que el *Habeas Data* se considera un instrumento constitucional al que la sociedad puede recurrir para preservar sus datos personales, los cuales están adscritos a distintos tipos de entidades financieras y de telecomunicaciones, y que tienen la obligación de dar un buen uso a los mismos.

Por su parte, la Corte Constitucional, Sala Tercera de Revisión, Sentencia T-443, 1994 considera que:

<sup>1</sup> Pérez, O. (2016). El *habeas data* en Colombia: su desarrollo y conexión con los derechos fundamentales. [Trabajo de grado, Universidad Católica de Colombia]. Repositorio Institucional U Católica. <https://repository.ucatolica.edu.co/server/api/core/bitstreams/348b132d-3ec1-6e71-b6ba-4b592252b1a/content#text=FILE%20desarrollo%20de%20Habeas%20Data%20datos%20y%20archivos%20de%20las>

Con la presente iniciativa legislativa, se realiza la actualización del régimen de protección de datos dispuesto en la Ley 1581 de 2012 y sus decretos reglamentarios; siendo esta una iniciativa con un artículo bastante amplio, que representa un paso firme hacia un futuro donde la privacidad y la protección de datos son más que simples términos legales: son principios fundamentales que deben guiar nuestras acciones y decisiones.

**III. CONSIDERACIONES.**

**1. Antecedentes del Proyecto de Ley.**

Con posterioridad a la Ley 1581 de 2012 no se han emitido leyes que realicen modificaciones de fondo al articulado de esta disposición rectora del marco normativo en materia de *habeas data*; lo que han existido son Decreto Reglamentarios que desarrollan los mandatos y disposiciones de este Reglamento General de Protección de Datos Personales.

**2. Consideraciones del Autor de la Iniciativa.**

Los autores de la iniciativa expresan que:

*El presente proyecto de ley busca desarrollar y ampliar el alcance del artículo 15 de la Constitución Política de Colombia, reconociendo y protegiendo el derecho fundamental a la privacidad mediante el establecimiento de medidas concretas para asegurar que los datos personales sean tratados de manera adecuada y transparente, acorde con la era digital.*

*Colombia se enfrenta a un gran problema debido a la existencia de múltiples normativas y la protección de datos no es un tema que se escape a esta realidad, la dispersión normativa dificulta el cumplimiento por parte de las empresas y deja en situación de vulnerabilidad a los titulares de datos. Ante esta situación, el presente proyecto de ley tiene como objetivo unificar y armonizar a nivel nacional la normativa de protección de datos, alineándose con los estándares internacionales, esto permitirá mejorar las oportunidades comerciales y fomentará la cooperación internacional en materia de protección de datos.*

*Además, este proyecto de ley propone un enfoque acorde con el entorno digital actual, que se caracteriza por los avances tecnológicos y la creciente interconectividad. Basado en la gestión de riesgos para*

*“Las personas o entidades que recogen, procesan y transmiten datos tienen, por lo tanto, el deber de conservar y custodiar debidamente los bancos de datos o archivos que los contienen, como una condición necesaria para el goce y la eficacia del derecho al Hábeas Data. El derecho al Hábeas Data cumple, entonces, la función de proteger a toda persona contra el peligro del abuso de la información, de manera que se garantice a toda persona el derecho a la autodeterminación informativa”.* (Pérez,2016).

- Como afirma Zambrano citado por Mora<sup>2</sup>, el *habeas data* garantiza que la información contenida en las distintas entidades debe preservarse y mantenerse discretamente, en relación con las creencias políticas o religiosas, información académica o laboral, entre otros. Por lo tanto, nadie puede conocer, ni las entidades pueden usar esta información en detrimento del individuo.

**3.1. Antecedentes históricos.**

Según Iguarán y Muñoz<sup>3</sup>, las limitaciones en el acceso a las comunicaciones durante la época llevaron a que la constitución de 1886, no incluyera afirmaciones explícitas sobre el derecho a la privacidad. A pesar de esto, en el artículo 19, se menciona que las autoridades deben proteger la vida, honra, bienes y derechos naturales de los colombianos, lo que sugiere una aproximación inicial al derecho a la privacidad como un derecho natural.

La Asociación Bancaria y de Entidades Financieras de Colombia señala que, antes de que el estado elaborará reglamentos más concretos para garantizar la seguridad de los datos de la población, el sector privado comenzó a recopilar datos personales. Un ejemplo de esto fue la creación de la central de riesgos del sector financiero en 1964, con el objetivo de obtener información sobre la situación de endeudamiento de las personas en el país<sup>4</sup>. (Barbosa, 2022)

En el mismo año, Losano citado por Barbosa, resaltó que la Universidad de los Andes, en colaboración con el Centro de Investigación de la Facultad de

<sup>2</sup> Mora, E. (2019). De la Identidad al *Habeas Data*. Conocimiento Libre y Licenciamiento, (20), p. 128. <https://convite.cenditel.gov.co/revistaclac/index.php/revistaclac/article/view/986954>

<sup>3</sup> Iguarán, M y Muñoz, R. (2012). *Habeas Data: Desarrollo Normativo y Jurisprudencial en Colombia*. [Trabajo de grado, Universidad EAFIT]. Repositorio Institucional EAFIT. <https://repository.eafit.edu.co/server/api/core/bitstreams/e6501400-703f-4c1f-808b-e7b76b72751f/content>

<sup>4</sup> Barbosa, S. (2022). Protección de datos personales en tiempos del Big Data. [Trabajo de grado, Universidad del Rosario]. Repositorio Institucional U Rosario. <https://repository.urosario.edu.co/server/api/core/bitstreams/6a0718aa-72df-42cf-acda-2635d1b4d272/content>

Ingeniería y la Facultad de Derecho, presentó un proyecto de ley para garantizar la seguridad de los datos personales. Este proyecto se basó en la normativa de varios países que abogan por la implementación de un órgano administrativo para controlar rigurosamente las bases de datos. Además, se estableció que tanto las personas naturales y jurídicas eran propietarias de sus datos, y que su uso requería de su aprobación. A pesar de estos esfuerzos, el proyecto nunca fue convertido en ley.

Pese a esto, el tratamiento de datos se regía por la “presunción de legalidad”, según lo establecido en la constitución de 1886 en el artículo 20; esto permitía a los particulares actuar con mayor libertad, ya que el marco legal no imponía restricciones estrictas. Sin embargo, esta situación también implicaba una vulnerabilidad para las personas que eran propietarias de su información, ya que no existían medidas claras de protección al respecto.

La Constitución de 1886 no establecía derechos específicos para proteger la información persona<sup>5</sup>. Lo más cercano a esta protección era el artículo 23, que interpretaba el derecho a la intimidad de forma que ninguna persona debía ser molestada o arrestada sin justificación legal. Además, el artículo 38 señalaba la importancia de preservar la privacidad de las comunicaciones escritas, excepto en casos judiciales en los que las autoridades debían revisarlas sin infringir la normativa.

En este sentido, antes de la Constitución de 1991, se promulgaron normativas que guardaban cierta similitud con el concepto de Habeas Data; por ejemplo la Ley 23 de 1981 que establecía en el artículo 34 que la Historia Clínica debía ser privada, y solo podría ser revelada con el consentimiento del paciente o en circunstancias autorizadas por la ley. Asimismo, la Ley 96 de 1985 en su artículo 51 consideraba como datos públicos los contenidos en el registro civil, como el número, fecha y lugar de expedición del documento de identidad de otros, mientras que los datos referidos a la identidad de las personas eran considerados privados.

Con la entrada en vigencia de la Constitución Política de 1991 se habla al interior del mandato constitucional del derecho a la información y a la privacidad desarrollando el habeas data y estableciendo en el artículo 15 que:

<sup>5</sup> Cote, L. (2016). Hábeas data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001. [Trabajo de grado, Universidad Santo Tomás]. Repositorio Institucional USTA. <https://repositorio.usta.edu.co/handle/11634/965>

*“Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.”*

Según Remolina citado por Barbosa<sup>6</sup>, en la elaboración del artículo de Habeas Data en la Constitución de 1991, se presentaron diversas iniciativas. María Mercedes Carranza y Francisco Rojas Birry, propusieron el término “Habeas Data”, que, aunque no fue incluido en la constitución, sí se utilizó posteriormente en la práctica jurisprudencial. Guillermo Perry Rubio, sugirió el término de libertad informática, pero en la constitución, en su segundo apartado, sólo tuvo en cuenta el término de libertad como uno de los principios fundamentales para garantizar este derecho. Jaime Álvaro Fajardo propuso regular el uso de la informática y otros desarrollos tecnológicos, pero esta propuesta no tuvo avances, y se mantuvo la “presunción de legalidad” estipulada en la constitución de 1886.

Por su parte, Alfredo Vásquez Carrizosa y Misael Pastrana Borrero sugirieron el término de consentimiento como fundamental para la gestión de datos personales, pero esta sugerencia no fue considerada en el texto final de la constitución, aunque sí influyó en la práctica jurisprudencial.

Carlos Lleras, recomendó que el manejo de datos, no necesariamente se incorporara en la misma regulación del derecho a la intimidad, pero esta propuesta tampoco se materializó. Estas sugerencias enriquecieron la reflexión sobre la construcción del artículo 15 de la constitución política de 1991.

Se detalla, que después de diversas discusiones, se creó la Ley 1266 de 2008 conocida como la ley de habeas data financiero, que regula la información

<sup>6</sup> Barbosa, S. (2022). Protección de datos personales en tiempos del Big Data. [Trabajo de grado, Universidad del Rosario]. Repositorio Institucional U Rosario. <https://repositorio.urosario.edu.co/server/api/core/bitstreams/5a0718aa-72df-42cf-acda-2635f4df4e22/content>

almacenada en sistemas digitales, especialmente en temas económicos a nivel individual, dejando de lado su protección a nivel macro<sup>7</sup>. Esta ley cuenta con los decretos reglamentarios: Decreto 1727 de 2009 y Decreto 2952 de 2010.

En la actualidad, según la Corte Constitucional en la Sentencia C-748, 2011, este derecho se interpreta como autónomo, por lo que su efectivo cumplimiento depende no solo del poder judicial, sino también de los entes administrativos que supervisan a las organizaciones que obtienen información de los ciudadanos.

Posteriormente, con la Ley 1581 de 2012 se delega la responsabilidad frente al cumplimiento en la protección de los datos personales a la Superintendencia de Industria y Comercio -SIC-; quien además de establecer lo que la norma dispone sobre el Habeas Data, crea el Registro Nacional de Bases de Datos a cargo de la SIC, para el registro correcto de los datos personales y la imposición de sanciones monetarias a quienes no cumplan con la normativa.

En 2012, Colombia fue reconocida como uno de los países que cuenta con una normativa integral para el manejo de datos de sus ciudadanos en consonancia con otros derechos constitucionales. La Ley 1581 de 2012, parcialmente reglamentada por el Decreto 1377 de 2013, establece que es el usuario quien debe dar su consentimiento y cómo la entidad maneja esos datos.

**3.2. Importancia**

El surgimiento de distintas generaciones de Derechos Humanos se dio a partir de la proliferación de diversos fenómenos en el mundo. Si bien esto era de suma importancia debido a los peligros que estos nuevos acontecimientos podían acarrear, también era necesario que los derechos se actualizarán y se adaptaran a las necesidades del contexto<sup>8</sup>

Es así, como las relaciones del ser humano con su entorno y la sociedad en general han estado marcadas con el crecimiento de la tecnología y los retos que ésta impone para el desarrollo de la sociedad y la necesidad de regular las nuevas disposiciones que impone la globalización.

<sup>7</sup> Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. Revista Especializada en Sociología Jurídica y Política, 8 (1), pp. 107-139. <http://dx.doi.org/10.14718/NovumJus.2014.8.16>

<sup>8</sup> Pérez, A. (1992). Del habeas corpus al habeas data. Revista Iberoamericana de derecho informático, (1), pp 153-161. <https://dialnet.unirioja.es/servlet/articulo?codigo=4482974>

Las nuevas tecnologías, suponen un riesgo para el habeas data y los derechos que se relacionan con estos tales como la libertad, dado que se introducen prácticas que pueden comprometer la información de las personas, tanto de forma individual como colectiva, e inciden en el derecho a la igualdad, dado que no todos tienen la posibilidad de acceder a mecanismos que les permita obtener conocimiento de sus datos y otro tipo de información. Esta situación, ha generado atención en los estados, quienes deben asegurarse de crear un marco jurídico que garantice el derecho al Habeas Data, en donde no se permita una invasión a la privacidad y el cual se actualice con las nuevas tecnologías.

Con lo anteriormente mencionado, se podría decir que la importancia de la implementación del derecho al Habeas Data en el marco jurídico colombiano radica en que los ciudadanos pueden conocer de manera más profunda cómo las entidades manejan sus datos personales. Esto podría otorgar confianza y legitimidad a las entidades que obtienen los datos de las personas, creando vínculos estrechos para la comunicación, ya que los ciudadanos pueden expresarse en caso de que se presente algún tipo de inconvenientes con sus datos.

Así mismo, el portal web Protecdata<sup>9</sup>, afirma que la normativa existente genera obligatoriedad en todas las empresas que almacenan los datos, sin distinción de ningún tipo. Esto demuestra que puede generar un compromiso y mayores esfuerzos por parte de estas entidades que buscan ofrecer un buen servicio y especialmente, una buena imagen ante la opinión pública.

**4. Marco Jurídico.**

La **Constitución Política de 1991** desarrolla en los artículos 15 y 20 el derecho a la intimidad personal y familiar, el buen nombre y la libertad de expresión; siendo el artículo 15 clave para el desarrollo del presente proyecto de ley, dado que en este se establece la recolección, tratamiento y circulación de los datos personales.

Por su parte, el marco normativo dispone:

- **Ley 1581 de 2012** que desarrolla el artículo 15 constitucional y establece

<sup>9</sup> Ley de Habeas Data: de qué se trata, quién la aplica y cuál es su importancia. (s.f). Protecdata. <https://protecdatajatam.com/blog/ley-de-habeas-data-de-que-se-trata-quien-la-aplica-y-cual-es-su-importancia/>

<p>los elementos para proteger los datos personales.</p> <ul style="list-style-type: none"> <li>- <b>Decreto 1377 de 2013</b> que reglamenta la Ley 1581 de 2012.</li> <li>- <b>Decreto 767 de 2022</b> que regula la Política de Gobierno Digital.</li> </ul> <p>La <b>Corte Constitucional</b> a desarrollado ampliamente la regulación y el desarrollo del habeas data, expresando que:</p> <ul style="list-style-type: none"> <li>- Sentencia T-857, 1999 considera que:             <p><i>"[L]a información que se almacena y se encuentra a disposición del público, debe atender a una información veraz, que se corresponda con los hechos que la originan, que sea dinámica, es decir, que se encuentre en permanente actualización, pues de esta manera refleja su veracidad implícita y finalmente, es susceptible de ser rectificada, cada vez que así se requiera".</i></p> </li> <li>- Sentencia T-657, 2005 afirma que:             <p><i>"[L]os datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos de manera ilícita (ya sea sin la previa autorización del titular o en ausencia de mandato legal o judicial) [...] Entonces, la Corte ha establecido que las personas antes de ser reportadas tienen el derecho y las entidades el deber de solicitar la autorización del titular del dato".</i></p> </li> <li>- Sentencia T-684, 2006 expresa que:             <p><i>"[L]as entidades administradoras de bases de datos financieros son responsables de que el ejercicio de recolección, tratamiento y circulación de datos sea razonable y no lesione los derechos fundamentales de los titulares de la información".</i></p> </li> <li>- Sentencia SU – 528, 1993, abordó cuestiones relacionadas con la información personal en las centrales de riesgo, en conflicto con el derecho a la información. Esta sentencia resolvió este asunto desde la perspectiva jurídica del derecho a la intimidad. Señalando que:             <p><i>"En casos de conflicto entre ambos, esta Sala no vacila en reconocer que la prevalencia del derecho a la intimidad sobre el derecho a la</i></p> </li> </ul>	<p><i>información, es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial, a la vez, del Estado social de derecho en que se ha transformado hoy Colombia, por virtud de lo dispuesto en el artículo primero de la Carta de 1991 (...) Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de «personas virtuales» que afecten negativamente a sus titulares, vale decir, a las personas reales".</i></p> <ul style="list-style-type: none"> <li>- Sentencia C-748, 2011, planteaba otras interpretaciones al Habeas Data:             <p><i>"[C]onsideraba el Hábeas Data una manifestación del libre desarrollo de la personalidad. Según esta línea, el Hábeas Data tiene su fundamento último (...) en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad".</i></p> </li> </ul> <p><b>5. Importancia de la Iniciativa.</b></p> <p>Vivimos en una era digital, donde la información fluye a través de las fronteras y donde la privacidad se convierte en un bien preciado. Este proyecto de ley es un paso firme hacia un futuro donde la privacidad y la protección de datos son más que simples términos legales: son principios fundamentales que deben guiar nuestras acciones y decisiones.</p> <p>Este proyecto de ley no solo busca actualizar nuestro marco normativo frente al derecho al Habeas Data, sino que también pretende reforzar el derecho fundamental a la protección de datos. Es una oportunidad para preparar a Colombia para los desafíos de la Revolución Industrial, dotando al país de un marco normativo robusto que pueda hacer frente a los riesgos que implica el uso de nuevas tecnologías en la privacidad de los individuos.</p> <p>Este proyecto de ley representa un paso crucial hacia una mayor protección de los derechos fundamentales en la era digital. Confío en que, con su apoyo y colaboración, podremos avanzar hacia un futuro donde la privacidad de nuestros ciudadanos esté debidamente protegida.</p> <p><b>5.1. Particularidades de la iniciativa legislativa.</b></p>
<p>La iniciativa legislativa busca abordar una problemática fundamental en nuestra sociedad: los desafíos de la protección de datos personales de los ciudadanos en la era digital.</p> <p>Desde la promulgación de los artículos 15 y 20 de la Constitución Política de 1991, se han sentado las bases para salvaguardar derechos fundamentales como la intimidad personal y familiar, así como el buen nombre, junto con la libertad de expresión e información. La evolución jurisprudencial ha reforzado estos derechos reconociendo en el Habeas Data una herramienta crucial para proteger la intimidad y la autodeterminación informática.</p> <p>Con la Ley 1581 de 2012 se marcó un hito importante al reconocer de forma autónoma el derecho a la protección de datos y abordar las necesidades y preocupaciones del momento. No obstante, la ley aparece en un momento de transición tecnológica, en pleno auge del comercio electrónico y la migración de formas de trabajo más tradicionales a un espacio digital, por lo que muchas de las instituciones jurídica previstas en la ley 1581, encuentran fuertes desafíos para aplicarse sobre los constantes desarrollos de tecnología de información y comunicaciones.</p> <p>Todas las referencias internacionales que adoptamos en el 2012 y que fueron consideradas en su momento, como por ejemplo la Directiva de Protección de Datos de la Unión Europea de 1995, el Convenio 108 de 1981, la Resolución 45/95 de la ONU y el catálogo de directrices de la OEA, han sido derogados o actualizados, de acuerdo con el estado de la técnica y los desafíos tecnológicos actuales.</p> <p>El contexto axiológico establecido en la Ley 1581, dentro del cual debe enmarcarse el tratamiento de los datos en Colombia fue elaborado con base en los referentes internacionales más importantes de la época y estaba enfocado en incluir unos principios mínimos que debe regir el manejo de los datos que las empresas realizan. Sin embargo, muchos de esos principios no fueron materializados en su totalidad en la Ley 1581, dejando por fuera de la conversación nacional principios tan importantes como, la limitación del plazo de conservación y minimización de los datos. Por tanto, este proyecto de ley busca subsanar esa omisión del legislador y agregar al marco axiológico que rige el tratamiento de la información, principios que interpelan a directrices internacionales y establecen estándares de protección más actualizados.</p> <p>Es claro, que el Reglamento General de Protección de Datos ha transformado el panorama global en materia de privacidad y seguridad de datos, y se ha</p>	<p>convertido en un referente en cuanto a estándares internacionales en la materia. Colombia, sin embargo, aún se encuentra rezagada en este aspecto, y es imperativo que actualicemos y fortalezcamos nuestra normativa para cumplir con los estándares internacionales y proteger eficazmente la privacidad de nuestros ciudadanos en la era digital.</p> <p>Este proyecto de ley no sólo persigue la alineación con los estándares internacionales, sino que va más allá, aspirando a que Colombia sea reconocido como un país con un nivel comparable a naciones que podrían ser importantes socios económicos. Es crucial tener en cuenta que los datos constituyen un activo fundamental en la era digital, y restringir la libre circulación de datos obstaculiza el progreso de las empresas colombianas. El camino debe ser actualizar nuestro marco jurídico para garantizar la protección de los datos y evitar afectaciones a los derechos fundamentales de los individuos.</p> <p>Es por ello, que la iniciativa plantea:</p> <ul style="list-style-type: none"> <li>- Un enfoque desde los riesgos y que su medición depende de la capacidad y contexto de cada empresa; es decir, se crea un marco normativo con un manejo de los riesgos proporcionado y que no supone cargas desmedidas para las pequeñas y grandes industrias en Colombia.</li> <li>- Se establecen medidas para que el tratamiento de datos se garantice desde la adopción de medidas para revisar y actualizar la naturaleza, el contexto y las finalidades del tratamiento de los datos que lleva a cabo cada organización.</li> <li>- Se dota a las empresas de una herramienta valiosa para adaptar sus prácticas y políticas de protección de datos a su situación en específico. Permittedo identificar que no todos los tratamientos de datos son iguales y que las medidas de cumplimiento deben ser flexibles y ajustadas en función del contexto.</li> <li>- Este proyecto de Ley permite no solo cumplir con las obligaciones legales, sino también priorizar la protección de los derechos y libertades de las personas en un panorama empresarial diverso y en constante cambio.</li> <li>- Esta iniciativa legislativa representa una convergencia de intereses tanto para las empresas como para los individuos, fortaleciendo nuestra</li> </ul>

<p>posición económica al proporcionar un impulso significativo a ambos sectores.</p> <ul style="list-style-type: none"> <li>- Con este proyecto de ley se desarrolla el principio de transparencia, lo cual se exige que las cláusulas sean sencillas de leer y entender. No queremos que la gente se vea atrapada en una maraña de términos legales; queremos que comprendan exactamente en qué condiciones se están tratando sus datos personales.</li> <li>- Este proyecto de ley otorga un mayor control a los ciudadanos, resaltando derechos frente a sus datos personales tales como el de oposición, limitación del tratamiento y el no ser objeto a tratamientos automatizados no autorizados y a la toma de decisiones con base en el análisis de perfiles, sino que también fortalece los derechos ya existentes, otorgando a las personas un control material sobre su información personal.</li> <li>- Se introduce el concepto de neurodatos como un dato de carácter personal que comprende lo dispuesto por las Naciones Unidas en la Resolución A/HRC/RES/51/3 del Consejo de Derechos Humanos, aprobada el 6 de octubre de 2022 (Consejo de Derechos Humanos, 2022) que como bien lo señala el concepto remitido por la Fundación Universitaria del Área Andina, esta Resolución se “encarga un estudio sobre las repercusiones de la neurotecnología en los derechos humanos. A nivel regional, la Organización de los Estados Americanos emitió en 2021 una declaración sobre los neuroderechos que contiene una serie de recomendaciones (Comité Jurídico Interamericano, 2021), seguida de una declaración de Principios Interamericanos sobre Neurociencias y Derechos Humanos aprobada en 2023 (Comité Jurídico Interamericano, 2023)”.</li> </ul> <p>Ante las reiteradas preocupaciones por la aplicación de la norma, es preciso señalar un análisis detallado de lo dispuesto en el artículo 3 sobre el ámbito territorial de la iniciativa legislativa. De esta forma, por consulta realizada al abogado Julian Paez Vargas, este realiza un detallado análisis sobre la aplicación extraterritorial de la iniciativa legislativa, expresando que en atención a lo dispuesto por la Corte Constitucional en la Sentencia C-1189 de 2000, hay tres conceptos que tienen que ser analizados para comprender la aplicación de la norma:</p>	<ul style="list-style-type: none"> <li>- <b>Principio de territorialidad</b> entendido como:             <p>“[F]undamento esencial de la soberanía, de acuerdo con el cual cada Estado puede prescribir y aplicar normas dentro de su respectivo territorio, por ser éste su “natural” ámbito espacial de validez. Forman parte integral de este principio, las reglas de “territorialidad subjetiva” (según la cual el Estado puede asumir jurisdicción sobre actos que se iniciaron en su territorio pero culminaron en el de otro Estado) y “territorialidad objetiva” (en virtud de la cual cada Estado puede aplicar sus normas a actos que se iniciaron por fuera de su territorio, pero culminaron o tuvieron efectos sustanciales y directos dentro de él”.</p> </li> <li>- <b>Principio de Nacionalidad</b> en virtud del cual:             <p>“[E]l Estado puede asumir jurisdicción sobre sus propios ciudadanos, donde quiera que éstos se encuentren. Este principio tiene dos manifestaciones: el de “nacionalidad activa”, que habilita al Estado para dictar normas de conducta de obligatoria observancia para sus nacionales, así estén en el exterior, y el de “nacionalidad pasiva”, según el cual el Estado puede ejercer jurisdicción sobre personas, actos o cosas que lesionen los intereses de uno de sus nacionales en territorio extranjero”.</p> </li> <li>- <b>Principio Real o De Protección</b> el cual:             <p>“[F]aculta a los Estados para ejercer jurisdicción sobre personas, actos o situaciones que, si bien se encuentran o se generan en el exterior, lesionan bienes jurídicos que son de importancia crucial para su existencia y su soberanía, como la seguridad nacional, la salud pública, la fe pública, el régimen constitucional, etc.”</p> </li> </ul> <p>Cada uno de estos principios tienen en las conclusiones realizadas por Paez Vargas unos puntos subjetivos y objetivos que se desarrollan así:</p> <ul style="list-style-type: none"> <li>- <b>Principio de Territorialidad:</b> <ul style="list-style-type: none"> <li>● Subjetiva: El Estado ejerce control sobre acciones que comenzaron en su territorio, pero tuvieron efectos posteriores en territorio de otro Estado.</li> <li>● Objetiva: El Estado aplica sus leyes a acciones que iniciaron fuera de su territorio, pero tuvieron efectos posteriores dentro de su territorio.</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>- <b>Principio de Nacionalidad:</b> <ul style="list-style-type: none"> <li>● Activa: El Estado dicta normas de conducta de obligatoria observancia para sus nacionales, aunque se encuentren en territorio extranjero.</li> <li>● Pasiva: El Estado ejerce jurisdicción sobre personas, actos o cosas que lesionen los intereses de sus nacionales en territorio extranjero.</li> </ul> </li> </ul> <p>De esta forma, concluye Paez Vargas al realizar el análisis del artículo 3 de la iniciativa legislativa que:</p> <ul style="list-style-type: none"> <li>- <i>El artículo no enfrentaría problemas de constitucionalidad, bajo el juicio de aplicación extraterritorial de la norma, durante el control derivado de la facultad expresa en el numeral 8 del artículo 241 de la Constitución Política, en virtud del reconocimiento y aplicación de los principios de territorialidad (subjetiva y objetiva), nacionalidad (activa y pasiva) y de protección.</i></li> <li>- <i>La Corte Constitucional reconoce la importancia de los estándares europeos en materia de protección de datos y los considera necesarios para que Colombia alcance un nivel adecuado de protección de datos. Esta premisa debe considerarse a la hora de defender el Proyecto de ley en el trámite legislativo.</i></li> <li>- <i>En la oportunidad legislativa adecuada valdría la pena incorporar las subreglas creadas por la Corte Constitucional en materia de protección de datos, tanto en el articulado como en la exposición de motivos del proyecto.</i></li> </ul> <p><b>6. Espacios de Participación Ciudadana.</b></p> <p>El día siete (07) de marzo de 2024 se realizó en la Comisión Primera Constitucional Permanente de la Cámara de Representantes audiencia pública de la iniciativa legislativa que se archiva por falta de trámite legislativo, dado que no se cumplieron los términos para la aprobación del mismo (Proyecto de Ley Estatutaria No. 156 de 2023 Cámara). Los insumos recolectados de esta audiencia pública y los conceptos recibidos fueron claves para el nuevo texto que se radico y en el que se acogen los comentarios y sugerencias dadas.</p> <p>A la audiencia pública fueron citados el Ministerio de las TIC’s, las Superintendencia Financiera de Colombia y la de Industria y Comercio; igualmente fueron invitados gremios, organizaciones, cámaras de comercio,</p>	<p>universidades, académicos expertos y ciudadanía en general. <u>Es de resaltar que atendiendo a que el objetivo de la presente norma es adecuarnos a los estándares internacionales participo de forma virtual LEONARDO CERVERA CERVERA NAVAS -Secretario General Supervisor Europeo de Protección de Datos -SEPD-</u></p> <p><b>También participaron en la audiencia pública integrantes de la sociedad civil, entre ellos ALEIDA LEGALTECH COLOMBIA, quienes han sido apoyo fundamental en la construcción de la iniciativa legislativa.</b></p> <p>Se destacan algunas participaciones en la audiencia pública que son insumos claves para el texto que se radico.</p> <p><b>1. Leonardo Cervera Navas - Supervisor europeo de protección de datos</b></p> <p>“El Reglamento General de Protección de Datos, fue aprobado por la Unión Europea en el año 2018 y desde entonces se ha convertido en una especie de faro que ilumina al mundo sobre lo que es la protección de la dignidad de las personas en la esfera digital. Es lo que se ha venido en denominar el efecto Bruselas en lo que se refiere a los derechos digitales, porque desde que aprobamos esto hace ya varios años, cada vez son más los países que se unen a este club de países que se toman en serio la protección de las personas en el ámbito digital. Por eso, me llena de satisfacción ver que en un país hermano y aliado como Colombia, esté modernizando la legislación del año 2012”(Canal Comisión Primera, 2024, 9m50s).</p> <p>“Es una legislación que se ha quedado un poco viejita, estaba bien cuando se aprobó, pero desde entonces han habido muchas modificaciones a nivel internacional y se ve que la ley le faltan muchos derechos que están internacionalmente reconocidos, no está, los datos sensibles por ejemplo, o no se no se cubre como es debido el tema de la transferencia internacional de datos. La Comisión Europea está haciendo un trabajo muy bueno con los países iberoamericanos, también la Agencia Española de Protección de Datos, la secretaria de la Red Iberoamericana de Protección de Datos. Y desde ese punto de vista, lo que están haciendo ustedes aquí es crucial para su país y crucial para los que estamos trabajando en el mundo para que la protección de datos se imponga”(Canal Comisión Primera, 2024, 10m41s).</p> <p>“Muy importante, es velar por que la autoridad de protección de datos en Colombia pueda gozar de una satisfactoria autonomía e independencia en el mundo de la protección de datos. La independencia de las autoridades de control es central para el buen funcionamiento del mecanismo, porque los ciudadanos tienen que poder</p>



<p>confiar que, si en un momento dado, alguien está usando mal sus datos, va a haber una autoridad independiente que va a poder defender sus derechos"(Canal Comisión Primera, 2024, 11m41s).</p> <p>¿Cuáles son sus recomendaciones para que esta ley sea implementada de manera efectiva en Colombia?</p> <p>"Mi recomendación es mirar el Reglamento Europeo y tomar en consideración sus principios y sus artículos más importantes. El reglamento funciona como un todo, es decir, no puede cogerse un artículo de aquí y otro artículo de allí porque el sistema que nosotros tenemos montado es consolidado. Por eso es tan importante mi recomendación, es que colaboren estrechamente con la Comisión Europea, que tiene un equipo especialista en este tipo de cuestiones y que es la que se encarga de dar el visto bueno a cualquier ley internacional, en lo que nosotros llamamos la decisión de adecuación. Desde el momento que un país se considera adecuado en la transferencia de datos internacionales entre ese país y la Unión Europea, es sin ningún tipo de barrera. Es igual mandar los datos desde Madrid a París que desde Madrid a Bogotá desde el punto y hora que esa ley cumple con los estándares europeos"(Canal Comisión Primera, 2024, 13m30s).</p> <p>"Yo, por eso, he querido enfatizar el tema de la independencia de la autoridad de control, y también decir que muchas de las cosas que vienen en la propuesta de ley, que la hemos mirado aquí en Bruselas, ya se vienen aplicando en la jurisprudencia de los tribunales colombianos, también en las resoluciones de la Superintendencia. Es decir, que no es un salto tan grande. Yo les recomendaría que, si van a cambiar la ley, no lo dejen a medio camino, que hagan el trayecto hacia el Reglamento General de Protección de Datos, porque ya es un estándar internacional. Es decir, se ha impuesto a nivel global. Hay más de 100 países alrededor todo del mundo que tiene normativa similar al reglamento, y por supuesto, lo pueden adaptar un poco a sus peculiaridades nacionales, al tenor de su Constitución. Eso es normal, pero lo que son los principios de aplicación deben, yo les recomiendo, que se alineen lo máximo posible con lo que tiene en el reglamento"(Canal Comisión Primera, 2024, 14m47s).</p> <p><b>2. Heidy Balanta - Directora de la escuela de privacidad</b></p> <p>"Lo primero es excluir del proyecto de ley todo lo relacionado con la ley 1266. Todo lo que tiene que ver con Habeas Data financiero, digamos, meter varias cosas una cosa con la otra, lo que hace es complejizar el asunto. Segundo, digamos que veo positivamente que se incluyan nuevas bases legales. Uno de los principales problemas que tiene Colombia es que tiene una única base legal, que es el consentimiento. Eso dificulta nuevos modelos de negocios, nuevo intercambio de</p>	<p>información personal. Es relevante que esas bases legales queden, así como nuevos derechos como la portabilidad de datos. Todo lo que tiene que ver con el derecho a la portabilidad de datos, el uso, la reutilización de los datos, es muy importante en este caso. Pero es importante también que se reconozca este derecho, también derechos como el derecho a no ser objeto de decisiones automatizadas. Si estamos hablando de Inteligencia artificial, es lo mínimo que también se le garantice estos derechos a los titulares. Y algo muy importante que han abordado los que me han antecedido y es el tema del sector público"(Canal Comisión Primera, 2024, 45m32s).</p> <p>"Hay un problema muy grave y es que en el sector público no hay quien regule o quién supervise datos personales. Solo cifras muy rápidamente de la SIC del año pasado el 45.2% de las entidades públicas no cuentan con procedimiento para la gestión de usuarios con acceso a información personal; el 57.6% no ha implementado políticas de acceso a la información personal con datos sensibles; el 69,4% no hacen auditorías a sus sistemas de información con datos personales; el 44% no tienen una política de datos; y el 55.2% no tienen una política de gestión de incidentes de seguridad. Sin contar temas de rama judicial, yo les invito a que se den una consulta en la relatoría de las altas Cortes y busquen anonimización. Los ciudadanos rogando que, por favor, les eliminen datos hipermega desactualizados, que no pueden acceder a oportunidades de empleo, porque aparece información que debería estar suprimida o, por lo menos, oculta, pero no lo está"(Canal Comisión Primera, 2024, 46m38s).</p> <p>"Entonces es un llamado, el Estado es la principal entidad que maneja los datos de la ciudadanía y es relevante que urgentemente la ley tenga en cuenta eso. Es decir, una autoridad ya sea independiente pero que pueda también entrar a vigilar o inspeccionar adecuadamente estos aspectos. La ley dice que la procuraduría es la encargada, sin embargo, hace dos años solicitamos en un derecho de petición a la Procuraduría y en lo que va corrido de la ley solo ha adelantado 110 investigaciones, de las cuales 98 se han archivado, es decir cero. En las entidades privadas vemos que hay una importante gestión por parte de la SIC, que lo hace muy bien en materia de protección de datos, cantidad de sanciones, pero cuando vamos a mirar para el lado público, cero. Entonces, esa es nuestra principal observación: importante el concepto de dato personal. Yo considero que tenemos que tener muy presente un concepto amplio de dato personal, tenemos que migrar ese concepto de dato público, semiprivado, privado, sensible. Hoy un dato puede ser público en algún contexto, semiprivado en otro, privado en otro. Entonces, tener esos conceptos tradicionales cuando hoy, por temas de economía digital, se maneja otro concepto de dato, es relevante. Entonces yo sí creo que hay que mirar muy bien, hoy por hoy, lo importante es quién emite el dato quién lo recibe y para qué se utiliza, más que esas clasificaciones tradicionales"(Canal Comisión Primera, 2024, 47m49s).</p>
<p><b>3. Sara Mora - Socia Fundadora de Aledia Legaltech Colombia</b></p> <p>"Este proyecto no solo resguarda un derecho fundamental, sino que también ofrece un marco regulatorio atractivo para nuestros empresarios y empresarias. Buscamos que Colombia se equipare a estándares internacionales, proporcionando a nuestros emprendedores un entorno normativo que les permita establecer acuerdos comerciales con empresas extranjeras. En cuanto a los aspectos que, desde mi punto de vista, requieren mejoras, es fundamental reconocer la preocupación respecto a la amplitud del proyecto. Específicamente, se propone la exclusión de parte especial y procedimental que abarca los artículos 81 al 88 en relación al tratamiento de recursos humanos, línea ética, entre otros"(Canal Comisión Primera, 2024, 50m15s).</p> <p>"Esta consideración subraya también la necesidad de abordar con seriedad el hecho de que, aunque se opte por omitir estos elementos para aligerar el proyecto, surge la imperante necesidad de establecer un compromiso firme por parte del legislativo para la elaboración de unas normas reglamentarias subsiguientes. Dicho compromiso no solo garantizará la coherencia en el proyecto de ley que nos ocupa en el día de hoy, sino también su eficacia dentro del marco legal propuesto"(Canal Comisión Primera, 2024, 51m01s).</p> <p>"En cuanto al segundo punto de mejora, me gustaría destacar el título séptimo relativo a la indemnización y régimen sancionatorio, donde se evidencia una divergencia de opiniones en diversos ámbitos académicos. Dada la sensibilidad de este tema y su impacto directo tanto en entidades públicas como privadas, considero fundamental abrir un espacio para que la Superintendencia de Industria y Comercio, con un profundo conocimiento del tema, pueda contribuir al congreso. Esta colaboración permitiría enriquecer el proyecto de manera más efectiva, alineando sus disposiciones con los intereses de los diferentes sectores gracias a la experiencia y a la objetividad que aporta la Superintendencia"(Canal Comisión Primera, 2024, 51m31s).</p> <p>"Como último punto de mejora, resaltó la conveniencia de excluir la referencia de la Superintendencia Financiera. Coincidió con la doctora Heidy, dado que su ámbito de aplicación se suscribe específicamente a entidades financieras. Los expertos con los que he consultado sobre este tema sugieren omitir esta mención a este ente regulador en la ley. Esta exclusión permitiría una delimitación más clara y coherente de los espacios de competencia, diferenciando así la Superintendencia de Industria y Comercio y la Superintendencia Financiera"(Canal Comisión Primera, 2024, 52m18s).</p>	<p>"Paso ahora a exponer las cuestiones positivas de este proyecto desde mi punto de vista. Por un lado, se destaca el fortalecimiento del derecho fundamental de las personas naturales y, por el otro, el fortalecimiento de nuestras empresas gracias a la libre circulación de los datos. En cuanto al primer punto, es magnífico observar cómo el proyecto de ley sitúa a la persona en el centro de la legislación en lugar de ser un satélite que gira alrededor de las empresas, ya sea estas responsables o encargadas del tratamiento. Asimismo destaco la importancia de la introducción de una nueva base jurídica y la aplicación de aspectos para abrir el espectro de la autorización, así como la incorporación de nuevos principios que establece un marco armonizado para la protección de datos alineándonos con otros países como Ecuador, Chile, Brasil, Reino Unido y los integrantes de la Unión Europea entre otros"(Canal Comisión Primera, 2024, 52m55s).</p> <p>"La segunda cuestión que deseo resaltar como aspecto positivo de este proyecto de ley radica en el enfoque global y la contribución que ofrece al ámbito empresarial del país. La armonización de la normativa actual con estándares internacionales facilita la interoperatividad y el intercambio seguro de datos entre Colombia y otros países, que también sigue las directrices internacionales"(Canal Comisión Primera, 2024, 53m52s).</p> <p>"Para cerrar mi intervención, quiero resaltar el principio del derecho que establece que quien puede lo más, puede lo menos. No es cierto que este proyecto de ley nos restrinja a trabajar con legislaciones menos rigurosas, como se ha mencionado en algunos entornos. Tampoco es preciso afirmar que representa una carga desproporcional para las empresas, ya que las medidas de seguridad se ajustan al tipo de empresa y a la naturaleza de los datos. Lo que ocurre es que aquellos que generan esos temores en Colombia buscan que continuemos con una normativa débil, lo cual está generando grandes ingresos a expensas de nuestros derechos fundamentales. Por lo tanto, animo a todos a sumar esfuerzos en pro de un proyecto común. Estamos aquí para sumar y no dividir. Los legisladores deben tomar nota para que todos podamos presenciar en el debate una ley integral acorde con los tiempos actuales, merecida para Colombia así como para todos los ciudadanos del mundo"(Canal Comisión Primera, 2024, 54m36s).</p> <p><b>4. Lucía Camacho - Coordinadora de Políticas Públicas en Derechos Digitales</b></p> <p>"En primer lugar, cómo el proyecto diseñado, aún cuando persigue un fin loable, fallan satisfacer las expectativas que promete, al menos por dos motivos: En primer lugar, porque amplía sustancialmente las facultades y tareas a cargo de la autoridad de protección de datos sin fortalecer sus capacidades operativas, es decir, no reviste</p>

a la autoridad de una estructura interna mucho más robusta. En segundo lugar, porque deja sin tocar aspectos como la autonomía independencia de la autoridad, así como no mejora el escenario actual de coexistencia de múltiples autoridades con competencia en esta materia lo cual es inconveniente, por motivos que explicaré ahora”(Canal Comisión Primera, 2024, 1h02m07s).

“Sobre el primer punto, creo que es preciso señalar que el proyecto le otorga nuevos poderes consultivos, poderes de asesoramiento a los responsables de datos, poderes de revisión para dictaminar sobre proyectos de códigos de conducta, poderes de acreditación de los organismos de certificación a la SIC, otros poderes de aprobar normas corporativas vinculantes, entre otras tareas que ya ejercí en materia investigativa de corrección, sanción y vigilancia. Al tiempo, el artículo 72 enfatiza que su estructura, la de la SIC, se mantendrá intocada, es decir, que la dirección de Habeas Data y la dirección de investigación seguirán ejerciendo su trabajo, pero con muchas más tareas a cargo”(Canal Comisión Primera, 2024, 1h02m49s).

“Este es un problema del que adolece también el reglamento europeo de protección de datos, que imita este proyecto muy de cerca. Allí, la vigencia del reglamento se pretendía como un marco robusto con diversas garantías, pero en sus casi más de 6 años de funcionamiento, ha merecido críticas fundadas en tanto que las autoridades de datos de los países europeos ejercen sus tareas de manera excesivamente lenta, entorpeciendo la protección rápida y efectiva de un derecho amenazado por factores como la velocidad, el ritmo y la gran escala en su tratamiento mediado por tecnologías digitales”(Canal Comisión Primera, 2024, 1h03m31s).

“El punto de partida sobre las capacidades de la SIC hoy tampoco parece muy favorecedor al respecto. Solo quisiera mencionar un caso anecdótico y personal, pero ejemplificador: en 2022, decidí acudir a la SIC para exigir que esta entidad ordenase al Ministerio de Salud la protección de mi derecho a la eliminación de mis datos registrados en CoronApp durante la pandemia. Mi caso tardó dos años en ser resuelto y pudo haber tardado mucho más si no me hubiese quejado en Twitter y el funcionario encargado de decir mi caso hubiese visto mi queja pública. En mi caso, decidí esperar de manera paciente, pero quienes hubiesen decidido no hacerlo habrían tenido que exigir la garantía de su derecho a través de la acción de tutela, congestionando el sistema de Justicia. Entonces, una ley garante del derecho a la protección de datos deben evaluar el punto de partida a las facultades y competencias de la autoridad para, en primer lugar, incrementar sus facultades en consonancia también con sus capacidades”(Canal Comisión Primera, 2024, 1h04m06s).

“Ahora, el segundo punto que mencioné, quisiera remarcar la importancia que tiene para la garantía del derecho a la protección de datos contar con una única autoridad

creemos que esto permite que se adapte la legislación a la realidad digital actual, en donde los adolescentes están cada vez más presentes”(Canal Comisión Primera, 2024, 1h13m02s).

“No obstante, creemos que el proyecto también tiene oportunidades de mejora que, de no atenderse, podrían comprometer el desarrollo digital del país y además afectar la calidad de la democracia. Esto se debe a que algunas disposiciones representan cargas excesivas para la economía digital, generan incertidumbre jurídica y, en algunos casos, ponen en riesgo la libertad de expresión y el acceso a la información. Entre los puntos críticos, encontramos la aplicación extraterritorial de la ley, que podría generar incertidumbre sobre todo para empresas que prestan servicios desde el exterior. Este enfoque contradice el principio de territorialidad y puede aislar al mercado colombiano del flujo global de información y de servicios”(Canal Comisión Primera, 2024, 1h13m56s).

“Otro aspecto que nos preocupa es la prohibición del tratamiento de datos parciales, incompletos o fraccionados, tal cual lo dice el artículo sexto, debido a la dificultad técnica que pueden tener las empresas para monitorear datos fragmentados. Esto excede las capacidades de las empresas y prácticamente hace que la medida sea muy difícil de cumplir técnicamente. Además, vemos que la libertad de expresión y la neutralidad de las plataformas se ve coartada en la medida que el proyecto establece que las plataformas de redes sociales serán responsables del contenido publicado por sus usuarios. Estas disposiciones, además, pueden ir en contra del principio de unidad de materia del proyecto, puesto que no es un tema de rectificación de datos personales, sino de información publicada por medios de comunicación”(Canal Comisión Primera, 2024, 1h14m41s).

“También vemos que la libertad de expresión se podría ver vulnerada por el derecho al olvido, sobre todo si se tiene en cuenta las pautas de la CIDH y de la OEA, que indican que este derecho puede ir en contra de la neutralidad de la red, pero también de la responsabilidad limitada de los intermediarios de internet. Finalmente, consideramos que, como lo ha dicho el Ministerio de las Tecnologías, restringir el uso de tecnologías emergentes como la inteligencia artificial mediante mecanismos de anonimización limita su progreso sin justificación alguna, y además, dar a la SIC, entidad que respetuosamente no tiene el expertise en este tipo de tecnologías emergentes, el poder discrecional para prohibirlas, vuelve básicamente el principio de neutralidad de red que asegura que las personas puedan acceder libremente a los contenidos es bastante limitado”(Canal Comisión Primera, 2024, 1h15m31s).

“En nombre de ALAI, quisiera invitar a todas las partes interesadas acá presentes para colaborar en el desarrollo de una visión de privacidad en línea que refleje las particularidades del país. Vemos con frecuencia que las autoridades de nuestra

de protección de datos que sea independiente frente a los actores del sector público, así como autónoma. Déjenme recordar muy brevemente qué tenemos hoy. Contamos con tres autoridades: la Superfinanciera, la Superintendencia de Industria y Comercio y la Procuraduría General de la Nación. Este escenario, que el proyecto de ley no resuelve, es problemático por dos razones: primera, porque atomiza la protección del derecho en razón al tipo de dato o del tipo de tratamiento y en razón al tipo de actor en cuestión, cuando la tendencia global en materia de protección de datos es que haya una única entidad que vigile todo del ecosistema sin importar qué tipo de sectores suceda el tratamiento”(Canal Comisión Primera, 2024, 1h05m05s).

“Además, en la práctica, supone un obstáculo para su titular porque puede ver el debilitamiento en el ejercicio de su derecho según el tipo de autoridad que le toque. La pregunta es, ¿por qué deberíamos perpetuar este estado de cosas? Por último, quisiera cerrar mi intervención haciendo una invitación a que revisemos los aprendizajes de estos 10 años de vigencia de la 1581 y a que corrijamos el camino en razón a ellos solo será esto posible si entendemos Cuáles son los vacíos y los retos que tenemos que corregir ahora”(Canal Comisión Primera, 2024, 1h06m11s).

**5. Pablo Nieto - Gerente Regional de Políticas Públicas de la Asociación Latinoamericana de Internet**

“Estamos totalmente de acuerdo con la importancia de implementar soluciones que salvaguarden la privacidad de los ciudadanos en los diversos entornos digitales, así como también creemos que el uso responsable y dinámico de los datos es crucial para impulsar la innovación, el desarrollo tecnológico y la productividad del país. En ese sentido desde ALAI apoyamos estos enfoques intermedios que equilibren la protección de los datos con la facilidad de su uso innovador y transfronterizo. De esta manera, consideramos que el país puede lograr políticas públicas integrales que protejan la seguridad de la información de los ciudadanos, pero también que promuevan ambientes favorables para el crecimiento y la competitividad, el desarrollo de nuevas tecnologías y la expansión de la economía digital”(Canal Comisión Primera, 2024, 1h12m11s).

“En cuanto al contenido del proyecto, en primera medida resaltamos aspectos positivos como la ampliación de las bases legales para el tratamiento de datos, incluido en el artículo séptimo. Creemos que esto ofrece una mayor flexibilidad y practicidad en el uso de la información personal, y puede permitir que las empresas puedan explorar nuevas formas de usos de datos para mejorar productos, servicios y procesos. Por otro lado, también celebramos la posición un poco más racional que se refleja en el uso de datos de menores de edad, lo cual, sin duda favorece también el acceso de esta población a servicios de salud y educación, entre otros. Pero además,

región adoptan legislaciones de otras partes del mundo que, tal vez, no responden a las realidades latinoamericanas”(Canal Comisión Primera, 2024, 1h16m41s).

**6. Grenfieth Sierra - Superintendente de Industria y Comercio**

“Quisiera iniciar con esta frase, que evidentemente refleja la importancia que le damos: los datos son el petróleo del siglo XXI. En ese contexto, la Superintendencia siempre ha visto la dinámica de los datos como un elemento esencial. Para ello, el marco legal sobre el cual se fundamenta la discusión, que asumimos que manifiesta, como todos sabemos, en la ley 1581, los decretos reglamentarios 1377 y 1075, varias sentencias de la Corte Constitucional, sobre la cual vale la pena resaltar la T-032 del 2021, que recoge la idea de guía de responsabilidad demostrada. Este marco legal le ha permitido al estado colombiano generar un marco regulatorio proactivo que ha respondido a una serie de desafíos. Sin embargo, se hace evidente la necesidad de la actualización en el marco de la Unión Europea frente a su directiva del 2016, frente a desarrollos regulatorios como en China o en América Latina (Brasil y Argentina), donde se ha debatido con bastante ahínco la idea de localización de la información y movilidad de esta información, que evidentemente responde a las dinámicas que podríamos denominar del capitalismo del siglo XXI, y aspectos tan fundamentales como la idea de Open Data y Open Finance, que define la construcción de las dinámicas de las clásicas economías financieras con las nuevas”(Canal Comisión Primera, 2024, 1h22m54s).

“Dentro de la delegada de datos con nuestro equipo, al estudiar la ley, hemos definido cuatro grandes áreas que consideramos deben ser tenidas en cuenta. Una, que la ley debe apostarle a un contenido y estabilidad del sistema jurídico. Esto básicamente es recoger lo más positivo del marco que hemos construido a partir de la 1581, es decir, un marco que se ha fundamentado en una naturaleza del dato, un modo de tratar el dato, la lógica del tamaño de la empresa y los riesgos sobre los cuales se ha fundamentado este contenido. Evidentemente, debe ser actualizado en estos nuevos desafíos y estas nuevas dinámicas”(Canal Comisión Primera, 2024, 1h24m52s).

“El segundo escenario es un marco de protección y reglas que responde a tres criterios que consideramos importantes. Una idea de flexibilidad en el marco interpretativo, es decir, normas amplias a partir de principios. Un segundo elemento es evitar la idea de obsolescencia normativa, es decir, no caer en la trampa de una simple reglamentación taxativa que termina siendo superada por la realidad. Algo que consideramos fundamental es la idea de anticipación por el derecho. Esto significa que la ley debe permitirle a los entes reguladores que el derecho anticipe escenarios tecnológicos. El tercer elemento es la sencillez y claridad jurídica, garantizando un elemento de cultura jurídica fundamental. Es decir, que el lenguaje

jurídica, que la semántica jurídica sobre la cual se ha construido la cultura jurídica colombiana, se mantenga”(Canal Comisión Primera, 2024, 1h25m43s).

“Por último, la idea de régimen sancionatorio, que para nosotros resulta muy importante, es mantener la idea de deberes de los actores del mercado y no caer en la trampa de ideas de conductas típicas, sobre lo cual la idea de niveles de riesgo resulta fundamental. Y para concluir, sin duda, la discusión más importante se fundamenta en la idea de portabilidad del dato: quién porta el dato y cómo se porta ese dato. Sobre este escenario, evidentemente, la discusión deberá llevar a un consenso entre los grandes actores. Primero el actor que es la persona; segundo, el actor que explota ese dato como actor económico. Tal vez la respuesta esté en determinar qué tipo de datos estamos hablando, de datos estructurados o datos no estructurados”(Canal Comisión Primera, 2024, 1h27m02s).

**7. Lorenzo Villegas - Socio de Áreas Tecnología, Medios y Comunicaciones**

“Yo quiero dividir mi intervención en seis puntos principales. En primer lugar, la ley 1581 tiene algunos puntos que hay que modificar, que han mostrado en estos 10 años una evidente dificultad en su aplicación. Es una ley relativamente nueva y es un estándar bastante alto de protección comparado a los demás países, tanto de la región como en otros países del mundo. En esa medida, la necesidad de un cambio normativo no se justifica en este momento, dado que la ley 1581 todavía tiene oportunidad de seguir aplicándose satisfactoriamente por un buen tiempo”(Canal Comisión Primera, 2024, 1h28m38s).

“Los otros temas que ya son de fondo y si hay muchos temas puntuales que son muy favorables en el proyecto de ley quisiera más bien enfocarme en algunos cinco puntos que no son tan favorables. En primer lugar, las afectaciones a la libertad de expresión, particularmente por las referencias al derecho al olvido que se encuentra en el proyecto de ley. La corte constitucional ha zanjado este debate de manera categórica en varias sentencias al determinar que el derecho al olvido en Colombia no es viable porque vulneraría el principio de neutralidad de la red, que es parte esencial del artículo 20 de la Constitución, es decir, de la libertad de expresión. Otro punto importante es que también el artículo 26 del proyecto de ley podría vulnerar la libertad de expresión al incluir el derecho de libre expresión de los periodistas y medios de comunicación como parte de los datos personales que están sujetos a la ley. Esto implicaría una afectación grave a nuestro derecho de libertad de expresión, que es uno de los derechos fundamentales, pilar de nuestra democracia”(Canal Comisión Primera, 2024, 1h29m19s).

“El segundo punto al que me quisiera referir es el ámbito de aplicación territorial. La ley tiene una pretensión de aplicación extraterritorial, lo cual es inadecuado no solo porque va en contravía de la constitución política, que establece que las leyes colombianas se aplican en el territorio colombiano para las personas que se encuentran en el territorio colombiano, salvo que haya tratados internacionales como los tratados consulares o diplomáticos. No obstante lo anterior, el proyecto de ley tiende a buscar que haya una aplicación extraterritorial y esto puede generar un conflicto de leyes que no se resolvería fácilmente con los principios del derecho internacional privado. Por otro lado, un desincentivo al tratamiento de datos, particularmente en el mundo digital, desde el exterior hacia Colombia”(Canal Comisión Primera, 2024, 1h30m28s).

“El tercer punto que quisiera traer a colación son las cargas desproporcionadas para las empresas que hagan el tratamiento de datos personales así como unas restricciones al derecho a la libertad de empresa. El artículo 9.3 dispone que los responsables del tratamiento a datos personales deben verificar, en el tratamiento de menores de edad, quién es el que otorga realmente el tratamiento de datos por parte del menor. Esta es una carga desproporcionada, porque eso también existe en la ley 1581. Es una carga desproporcionada y realmente imposible cumplir, porque el tratamiento de datos personales en un mundo, por ejemplo digitalizado, o donde intermedian las telecomunicaciones, es imposible determinar que la persona que está al otro lado de una comunicación es el representante legal de un menor. No podemos determinar claramente esto”(Canal Comisión Primera, 2024, 1h31m19s).

“Finalmente, creo que estamos en un momento donde es difícil establecer regulaciones a la inteligencia artificial. No sabemos muy bien qué es lo que se pretende todavía regular con eso y esto podría, por un lado, vulnerar el principio de neutralidad tecnológica, que es la intervención del estado en la definición y aplicación de una tecnología en específico. Por otro lado también el hecho de que se le establezca que la SIC define cuáles son las tecnologías de inteligencia artificial. Pensaría que primero la SIC no tiene la capacidad y la competencia actualmente para hacerlo, no la competencia legal, sino la cantidad de personas y estructura para poder definir cuáles son las tecnologías de inteligencia artificial que estarían tratando datos personales Y si podrían hacerse o no”(Canal Comisión Primera, 2024, 1h32m49s).

**IV. POTENCIALES CONFLICTOS DE INTERÉS.**

El artículo 3 de la Ley 2003 de 2019 que modificó el artículo 291 de la Ley 5 de 1992 señala que: “el autor del proyecto y el ponente presentarán en el cuerpo

de la exposición de motivos un acápite que describa las circunstancias o eventos que podrían generar un conflicto de interés para la discusión y votación del proyecto, de acuerdo con el artículo 286. Estos serán criterios guías para que los otros congresistas tomen una decisión en torno a si se encuentran en una causal de impedimento, no obstante, otras causales que el Congresista pueda encontrar”.

De esta forma, la Ley 2003 de 2019 en su artículo 1 señala que:

“[...] El artículo 286 de la Ley 5ª de 1992 quedará así:

Artículo 286. Régimen de conflicto de interés de los congresistas. Todos los congresistas deberán declarar los conflictos de intereses que pudieran surgir en ejercicio de sus funciones.

[...] Para todos los efectos se entiende que no hay conflicto de interés en las siguientes circunstancias:

- a) **Cuando el congresista participe, discuta, vote un proyecto de ley o de acto legislativo que otorgue beneficios o cargos de carácter general, es decir cuando el interés del congresista coincide o se fusione con los intereses de los electores [...].** (Negrilla y Subrayado Fuera del Texto)

Es así, como la iniciativa legislativa sometida a discusión no configura un beneficio particular, actual o directo a favor de un congresista, de su cónyuge, compañero o compañera permanente o pariente dentro del segundo grado de consanguinidad, segundo de afinidad o primero civil, ya que se trata de una acción de carácter general.

Es menester señalar que la descripción de los posibles conflictos de interés que se puedan presentar frente al trámite o votación del presente Proyecto de Ley, conforme a lo dispuesto en el artículo 291 de la Ley 5 de 1992 modificado por la Ley 2003 de 2019, no exime al Congresista de identificar causales adicionales en las que pueda estar incurso.

**V. IMPACTO FISCAL.**

La Ley 819 de 2003 “Por la cual se dictan normas orgánicas en materia de presupuesto, responsabilidad y transparencia fiscal y se dictan otras disposiciones”, establece, en su artículo 7 que “el impacto fiscal de cualquier proyecto de ley, ordenanza o acuerdo, que ordene gasto o que otorgue beneficios tributarios, deberá hacerse explícito y deberá ser compatible con el

Marco Fiscal de Mediano Plazo. Para estos propósitos, deberá incluirse expresamente en la exposición de motivos y en las ponencias de trámite respectivas los costos fiscales de la iniciativa y la fuente de ingreso adicional generada para el financiamiento de dicho costo”.

En este sentido, es pertinente señalar que la iniciativa legislativa objeto de la presente ponencia, no tiene impacto fiscal, dado que este tiene como objetivo establecer estrategias para actualizar el régimen de protección de datos personales en Colombia.

**VI. Pliego de Modificaciones.**

Atendiendo a las reuniones y comentarios dados por diversos sectores, entidades públicas, la academia y organizaciones sociales, se realizan modificaciones que permiten disminuir el número de artículos y fortalecer la iniciativa legislativa.

Atendiendo a las comentarios recibidos por la Asociación Colombiana de Administradoras de Fondos de Pensiones y de Cesantías -ASOFONDOS-, la Cámara Colombia de Informática y Telecomunicaciones -CCIT- y la Fundación Universitaria del Área Andina -AREANDINA-;se realizan modificaciones al artículo 1,2,3,4,5,6,8,13,14,15,20,28,42,47 y 58.

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
Proyecto de Ley Estatutaria No. 152 de 2024 Cámara *Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales*	Proyecto de Ley Estatutaria No. 152 de 2024 Cámara *Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales*	SIN MODIFICACIONES
<b>ARTÍCULO 1. Objeto.</b> La presente ley establece las normas relativas a la protección de las personas naturales en lo que respecta a la protección y tratamiento de sus datos personales y las normas relativas a la libre circulación de tales datos.  De igual manera, la presente ley protege los derechos y garantías fundamentales de las personas naturales y, en particular, su derecho fundamental a la	<b>ARTÍCULO 1. Objeto.</b> La presente ley establece las normas relativas a la protección de las personas naturales en materia <del>de lo que respecta</del> a la protección y tratamiento de sus datos personales <del>y las normas relativas a</del> <b>y su</b> libre circulación <del>de tales datos</del> .  De igual manera, la presente ley protege los derechos y garantías fundamentales de las personas naturales y, en particular, su	Se realizan precisiones en la redacción.



Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
protección de los datos personales, en los términos descritos en el artículo 15 de la Constitución Política.	derecho fundamental a la protección de los datos personales, en los términos descritos en el artículo 15 de la Constitución Política.	
<b>ARTÍCULO 2. Ámbito de la aplicación material.</b> 1. La presente ley se aplica al tratamiento de los datos personales. 2. El régimen de protección de datos personales establecido en la presente ley no será de aplicación: a) A los tratamientos efectuados por una persona natural en un ámbito exclusivamente personal o doméstico. b) A los tratamientos realizados por parte de las autoridades competentes con fines de prevención, investigación, detección, o procesamiento judicial de actos delictivos incluido el lavado de activos y el financiamiento del terrorismo, la ejecución de sanciones penales, así como la de protección frente a amenazas a la seguridad y defensa nacional y su prevención. c) A los tratamientos que tengan como finalidad cumplir con la actividad periodística y otros	<b>ARTÍCULO 2. Ámbito de la aplicación material.</b> 1. La presente ley se aplica al tratamiento de los datos personales. 2. El régimen de protección de datos personales establecido en la presente ley no será de aplicación: a) A los tratamientos efectuados por una persona natural en un ámbito exclusivamente personal o doméstico. b) A los tratamientos realizados por parte de las autoridades competentes con fines de prevención, investigación, detección, o procesamiento judicial de actos delictivos incluido el lavado de activos y el financiamiento del terrorismo, la ejecución de sanciones penales, así como la de protección frente a amenazas a la seguridad y defensa nacional y su prevención. c) A los tratamientos que tengan como finalidad cumplir con la actividad	Se realizan ajustes de redacción para mayor comprensión y aplicación de la ley.

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
contenidos editoriales. d) A los tratamientos que tengan como fin y contengan información de inteligencia y coninteligencia. e) A los tratamientos realizados en virtud de la Ley 1266 de 2008	periodística y otros contenidos editoriales. d) A los tratamientos que tengan como fin y contengan información de inteligencia y coninteligencia. e) A los tratamientos realizados en virtud de la Ley 1266 de 2008	
<i>Parágrafo primero.</i> Cuando se traten datos de personas fallecidas, los causahabientes, que acrediten tal calidad, podrán dirigirse al responsable o encargado del tratamiento con el objeto de solicitar el acceso a los datos personales de la persona fallecida y, en su caso, su rectificación o supresión.  <i>Parágrafo segundo.</i> El Gobierno Nacional, reglamentará sobre el tratamiento de datos personales tratados para fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos, la financiación del terrorismo y la ejecución de sanciones penales.  <i>Parágrafo tercero.</i> Los principios sobre protección de datos serán aplicables a todos los tratamientos de datos personales, incluidos los exceptuados en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial regule los tratamientos de datos personales exceptuados prevea principios que tengan en consideración la naturaleza	<i>Parágrafo primero.</i> Cuando se traten datos de personas fallecidas, los causahabientes, que acrediten tal calidad, podrán dirigirse al responsable o encargado del tratamiento con el objeto de solicitar el acceso a los datos personales de la persona fallecida y, en su caso, su rectificación o supresión.  <i>Parágrafo segundo.</i> El Gobierno Nacional, reglamentará sobre el tratamiento de datos personales <del>tratados</del> para fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos, la financiación del terrorismo y la ejecución de sanciones penales.  <i>Parágrafo tercero.</i> Los principios sobre protección de datos serán aplicables a todos los tratamientos de datos personales, incluidos los exceptuados en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial regule los tratamientos de datos personales exceptuados <del>se</del> <b>deben establecer</b> <del>prevea</del>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
especial de los datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.	principios que tengan en consideración la naturaleza especial de los datos; <b>y los cuales serán aplicables</b> los mismos aplicarán de manera concurrente a los previstos en la presente ley.	
<b>ARTÍCULO 3. Ámbito territorial.</b> 1. La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de los responsables o del encargado con domicilio y/o residencia en territorio nacional, independientemente de que el tratamiento tenga lugar o no en Colombia. 2. La presente ley se aplica al tratamiento de datos personales de titulares que residan en territorio nacional por parte de un responsable o encargado no establecido en Colombia, cuando las actividades de tratamiento estén relacionadas con: a) La oferta de bienes o servicios a dichos titulares con residencia en Colombia, independientemente de si estos son de carácter oneroso o no. b) El control del comportamiento, en la medida en que este tenga lugar en Colombia. 3. Por un responsable o encargado que no esté establecido en Colombia, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud	<b>ARTÍCULO 3. Ámbito territorial.</b> 1. La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de los responsables o del encargado con domicilio y/o residencia en territorio nacional, independientemente de que el tratamiento tenga lugar o no en Colombia. 2. La presente ley se aplica al tratamiento de datos personales de titulares que residan en territorio nacional por parte de un responsable o encargado no establecido en Colombia, cuando las actividades de tratamiento estén relacionadas con: a) La oferta de bienes o servicios a dichos titulares con residencia en Colombia, <b>independientemente de si estos son de carácter oneroso o no.</b> b) El control del comportamiento, en la medida en que este tenga lugar en Colombia. 3. Por un responsable o encargado que no esté establecido en Colombia, pero le resulte aplicable la legislación nacional,	Se acepta la modificación propuesta por la Asociación Colombiana de Administradoras de Fondos de Pensiones y de Cesantías -ASOFONDOS- en la cual disponen la eliminación del carácter oneroso, señalando que: "La naturaleza onerosa o gratuita de los bienes o servicios no debería influir en el tratamiento de los datos, ya que el régimen de protección de datos no distingue esta condición".

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
del derecho internacional público.	derivado de la celebración de un contrato o en virtud del derecho internacional público.	
<b>ARTÍCULO 4. Definiciones. A efectos de la presente ley se entenderá por:</b> 1. «Anonimización»: procedimiento técnico que modifica de manera irreversible los datos personales con el fin que no pueda atribuirse a un titular; 2. «Autoridad de Protección de Datos»: entidad pública que tiene como objetivo principal inspeccionar, vigilar y controlar la aplicación del Régimen General de Protección de Datos establecido en esta ley y las demás disposiciones que la desarrollen, modifiquen, adicionen o complementen, garantizando la protección de los derechos de los titulares y el efectivo cumplimiento de los deberes de quienes intervengan en el tratamiento de los datos personales. 3. «Base de datos»: todo conjunto de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado. 4. «Bloqueo de datos»: medidas técnicas y organizativas adoptadas por parte del responsable o encargado del tratamiento, que permitan la identificación y reserva de	<b>ARTÍCULO 4. Definiciones. A efectos de la presente ley se entenderá por:</b> 1. «Anonimización»: procedimiento técnico que modifica de manera irreversible los datos personales con el fin que no pueda atribuirse a un titular; 2. «Autoridad de Protección de Datos»: entidad pública que tiene como objetivo principal inspeccionar, vigilar y controlar la aplicación del Régimen General de Protección de Datos establecido en esta ley y las demás disposiciones que la desarrollen, modifiquen, adicionen o complementen, garantizando la protección de los derechos de los titulares y el efectivo cumplimiento de los deberes de quienes intervengan en el tratamiento de los datos personales. 3. «Base de datos»: todo conjunto de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado. 4. «Bloqueo de datos»: medidas técnicas y organizativas adoptadas por parte del responsable o encargado del tratamiento, que permitan la identificación y reserva de	Se acepta la modificación propuesta por ASOFONDOS al numeral 21 de la disposición normativa; señalando que: "la definición de servicio de sociedad de la información es poco clara y no entiende su inclusión".  Se realizan ajustes atendiendo a las recomendaciones dadas por la Cámara Colombiana de Informática y Telecomunicaciones -CCIT-, expresando que: "con el fin de garantizar la seguridad jurídica y dotar al proyecto de ley de total claridad y cohesión en el texto" se procede a realizar la precisión sobre el uso de la "cesión de datos" y su definición.

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>los datos para impedir y/o evitar su tratamiento.</p> <p>5. «Comunicación de datos»: tratamiento de datos que implica su revelación a una persona distinta del titular y/o encargado de tratamiento.</p> <p>6. «Consentimiento del titular»: Toda manifestación de la voluntad expresa, libre, inequívoca, informada y específica por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.</p> <p>7. «Corresponsabilidad»: Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento.</p> <p>8. «Datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural, que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.</p> <p>9. «Datos genéticos»: datos personales relativos a la información sobre las características hereditarias de una persona natural, obtenidas por análisis de ácidos nucleicos u otros análisis científicos de una muestra biológica, que proporcionen una información única sobre la</p>	<p>de los datos para impedir y/o evitar su tratamiento.</p> <p>5. «<b>Cesión</b> Comunicación de datos»: tratamiento de datos que implica su revelación a una persona distinta del titular y/o encargado de tratamiento.</p> <p>6. «Consentimiento del titular»: Toda manifestación de la voluntad expresa, libre, inequívoca, informada y específica por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.</p> <p>7. «Corresponsabilidad»: Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento.</p> <p>8. «Datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural, que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.</p> <p>9. «Datos genéticos»: datos personales relativos a la información sobre las características hereditarias de una persona natural, obtenidas por análisis de ácidos nucleicos u otros análisis científicos de una muestra biológica, que proporcionen una información única sobre la</p>		<p>fisiología o la salud de esa persona.</p> <p>10. «Datos personales»: toda información sobre una persona natural identificada o identificable (el titular) se considerará persona natural 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.</p> <p>11. «Datos relativos a la salud»: datos que revelan aspectos relativos al estado de bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades de una persona natural. Estos datos incluyen, aunque no limitado a, la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud; la información recolectada por dispositivos tecnológicos que busquen hacer mediciones sobre la condición física de su usuario, entre otros.</p> <p>12. «Datos sensibles»: son los que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como</p>	<p>fisiología o la salud de esa persona.</p> <p>10. «Datos personales»: toda información sobre una persona natural identificada o identificable (el titular) se considerará persona natural 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.</p> <p>11. «Datos relativos a la salud»: datos que revelan aspectos relativos al estado de bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades de una persona natural. Estos datos incluyen, aunque no limitado a, la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud; la información recolectada por dispositivos tecnológicos que busquen hacer mediciones sobre la condición física de su usuario, entre otros.</p> <p>12. «Datos sensibles»: son los que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como</p>	
<p>aqueellos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características biológicas, identidad o expresión de género y orientación sexual de una persona natural.</p> <p>13. «Destinatario o tercero»: persona natural o jurídica, pública o privada, a la que se comuniquen datos personales, distinta del titular, responsable de tratamiento y encargado. Una vez el destinatario se le cedan los datos se convierte en responsable. No se considerarán destinatarios a las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el artículo 2, numeral 2, literal b) y d) de la presente ley.</p> <p>14. «Elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales con el fin de evaluar determinados aspectos de una persona natural. En particular, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud,</p>	<p>aqueellos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características biológicas, identidad o expresión de género y orientación sexual de una persona natural.</p> <p>13. «Destinatario o tercero»: persona natural o jurídica, pública o privada, a la que se comuniquen datos personales, distinta del titular, responsable de tratamiento y encargado. Una vez el destinatario se le cedan los datos se convierte en responsable. No se considerarán destinatarios a las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el artículo 2, numeral 2, literal b) y d) de la presente ley.</p> <p>14. «Elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales con el fin de evaluar determinados aspectos de una persona natural. En particular, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica,</p>		<p>preferencias personales, intereses, fiabilidad, comportamiento, ubicación, movimientos, entre otros, de dicha persona natural.</p> <p>15. «Encargado del tratamiento» o «Encargado»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.</p> <p>16. «Incidente de seguridad»: cualquier violación de los códigos de seguridad que resulte en el daño, la destrucción, pérdida o alteración accidental o intencional de datos personales, que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado, y que impacte en la confidencialidad, integridad y/o disponibilidad de dichos datos.</p> <p>17. «Limitación del tratamiento»: aplicación de medidas por parte del responsable de <b>manera</b> que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse.</p> <p>18. «Neurodatos»: para los efectos de la presente ley, se refiere al conjunto de información obtenida a partir de la actividad cerebral y el sistema nervioso, así como la información inferida de estos datos, de una persona</p>	<p>salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, movimientos, entre otros, de dicha persona natural.</p> <p>15. «Encargado del tratamiento» o «Encargado»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.</p> <p>16. «Incidente de seguridad»: cualquier violación de los códigos de seguridad que resulte en el daño, la destrucción, pérdida o alteración accidental o intencional de datos personales, que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado, y que impacte en la confidencialidad, integridad y/o disponibilidad de dichos datos.</p> <p>17. «Limitación del tratamiento»: aplicación de medidas por parte del responsable de manera que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse.</p> <p>18. «Neurodatos»: para los efectos de la presente ley, se refiere al conjunto de información obtenida a partir de la actividad cerebral y el sistema nervioso, así como la</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>natural identificada o identificable.</p> <p>19. «Representante»: persona natural o jurídica designada por escrito por parte del responsable o el encargado del tratamiento, de conformidad con esta ley, para que los represente en lo que respecta a sus obligaciones en virtud de la presente ley.</p> <p>20. «Responsable del tratamiento» o «responsable»: persona natural o jurídica, pública o privada, que por sí misma o en asociación con otros determine los fines y medios del tratamiento.</p> <p>21. «Servicio de la sociedad de la información»: para efectos de la presente ley se entenderá como todo servicio prestado por solicitud de un consumidor de servicios, a través de equipos electrónicos y/o tecnologías que facilitan la creación, distribución y manipulación de la información, sin que las partes estén presentes simultáneamente.</p> <p>22. «Seudonimización»: tratamiento de datos personales que ya no puedan atribuirse a un titular sin utilizar información adicional. Dicha información debe figurar por separado, estar sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.</p>	<p>información inferida de estos datos, de una persona natural identificada o identificable.</p> <p>19. «Representante»: persona natural o jurídica designada por escrito por parte del responsable o el encargado del tratamiento, de conformidad con esta ley, para que los represente en lo que respecta a sus obligaciones en virtud de la presente ley.</p> <p>20. «Responsable del tratamiento» o «responsable»: persona natural o jurídica, pública o privada, que por sí misma o en asociación con otros determine los fines y medios del tratamiento.</p> <p>21. «Servicio de la sociedad de la información»: para efectos de la presente ley se <del>Se</del> entenderá como <u>cuales</u> <del>este</del> <u>servicio que, a solicitud de un usuario, sea mediante el uso por solicitud de un consumidor de servicios, a través de equipos electrónicos y/o tecnologías de la información y las comunicaciones, permitiendo la que</u> <del>facilitan</del> <u>la</u> <del>creación,</del> <u>la</u> <del>distribución y manipulación de la información, sin requerir la presencia simultánea de</del> <u>que las partes involucradas. Estos servicios pueden incluir, entre otros, el comercio electrónico, plataformas</u></p>	
<p>23. «Titular»: persona natural cuyos datos personales son objeto de Tratamiento.</p> <p>24. «Transferencia internacional de datos personales»: tratamiento que supone un flujo de datos, en el que un responsable y/o encargado del tratamiento ubicado en el territorio nacional, envía y/o habilita accesos a datos personales a destinatarios y/o encargados que se encuentran fuera del territorio nacional.</p> <p>25. «Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como pueden ser, la recogida, registro, organización, estructuración, conservación, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.</p> <p>26. «Tratamiento a gran escala»: es aquel que afecta a una gran cantidad de datos que se refieren a un elevado número de titulares y que entraña un alto riesgo. Su valoración dependerá de la proporción de la población correspondiente, el volumen de datos o la variedad de elementos de</p>	<p><del>de redes sociales, aplicaciones móviles y servicios de almacenamiento en la nube, estén presentes simultáneamente.</del></p> <p>22. «Seudonimización»: tratamiento de datos personales que ya no puedan atribuirse a un titular sin utilizar información adicional. Dicha información debe figurar por separado, estar sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.</p> <p>23. «Titular»: persona natural cuyos datos personales son objeto de Tratamiento.</p> <p>24. «Transferencia internacional de datos personales»: tratamiento que supone un flujo de datos, en el que un responsable y/o encargado del tratamiento ubicado en el territorio nacional, envía y/o habilita accesos a datos personales a destinatarios y/o encargados que se encuentran fuera del territorio nacional.</p> <p>25. «Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como pueden ser, la recogida, registro, organización, estructuración, conservación,</p>	
<p>datos que son objeto de tratamiento, el alcance geográfico y la duración o permanencia del tratamiento.</p> <p>ARTÍCULO 5. Principios relativos al tratamiento.</p> <p>1. El tratamiento de datos personales debe darse en virtud de los siguientes principios:</p> <p>a) «Principio de Legalidad»: el tratamiento de los datos personales debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.</p> <p>b) «Principio de lealtad»: las finalidades con la que se recolectan datos personales encontrarán sus límites en la</p>	<p>almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.</p> <p>26. «Tratamiento a gran escala»: es aquel que afecta a una gran cantidad de datos que se refieren a un elevado número de titulares y que entraña un alto riesgo. Su valoración dependerá de la proporción de la población correspondiente, el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento, el alcance geográfico y la duración o permanencia del tratamiento.</p> <p>ARTÍCULO 5. Principios relativos al tratamiento.</p> <p>1. El tratamiento de datos personales debe darse en virtud de los siguientes principios:</p> <p>a) «Principio de Legalidad»: el tratamiento de los datos personales debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.</p> <p>b) «Principio de lealtad»: las finalidades con la que se recolectan datos personales encontrarán sus</p>	<p>Se aceptan las modificaciones expuestas por ASOFONDO para el numeral d) en relación a la redacción del principio de "limitación de la finalidad", con el objetivo de que la redacción se comprenda de mejor manera.</p>
<p>presente ley y no podrán obtenerse por vías fraudulentas, engañosas, ni por acciones que puedan calificarse como dolosas.</p> <p>c) «Principio de transparencia»: exige que la información facilitada a los titulares sea concisa, accesible e inteligible, utilizando un lenguaje claro y sencillo.</p> <p>d) «Principio de limitación de la finalidad»: los datos deben ser recogidos con fines determinados, y no serán tratados ulteriormente de manera incompatible con dichos fines; el tratamiento ulterior de los datos personales con fines de archivo en interés público, investigación científica, histórica o estadística no se considerará incompatible con los fines iniciales.</p> <p>e) «Principio de minimización de datos»: sólo se deben recabar los datos adecuados, pertinentes y</p>	<p>límites en la presente ley y no podrán obtenerse por vías fraudulentas, engañosas, ni por acciones que puedan calificarse como dolosas.</p> <p>c) «Principio de transparencia»: exige que la información facilitada a los titulares sea concisa, accesible e inteligible, utilizando un lenguaje claro y sencillo.</p> <p>d) «Principio de limitación de la finalidad»: los datos deben ser <b>recogidos con fines determinados únicamente para fines específicos, recogidos con fines determinados, explícitos y legítimos, No podrán ser y ni serán</b> <del>tratados</del> <b>posteriormente para otros</b> <del>ulteriormente de manera incompatible con dichos fines que no se ajusten a los objetivos originales. Sin embargo, el uso posterior</del> <del>el</del> <b>tratamiento</b> <del>ulterior</del> de los</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>limitados a lo necesario en relación con los fines para los que son tratados.</p> <p>f) «Principio de exactitud»: los datos de carácter personal deberán ser exactos de tal forma que respondan con veracidad a la situación actual del titular. Si fuera necesario, se actualizarán; se adoptarán todas las medidas razonables para rectificar o suprimir, sin demora injustificada, los factores que introducen las inexactitudes en los datos personales con respecto a los fines para los que se tratan. Los datos facilitados directamente por el titular se considerarán exactos.</p> <p>g) «Principio de limitación del plazo de conservación»: los datos deben ser mantenidos de forma que se permita la identificación de los titulares durante no más tiempo del necesario para los fines del</p>	<p>datos <del>de</del> <del>personales</del> <del>en</del> fines de archivo en interés público, investigación científica, histórica o estadística <del>no</del> se considerará <del>adecuado</del> <del>y</del> <del>permitido, incluso si no coincide exactamente con el propósito inicial.</del> <del>incompatible con los fines iniciales.</del></p> <p>e) «Principio de minimización de datos»: sólo se deben recabar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.</p> <p>f) «Principio de exactitud»: los datos de carácter personal deberán ser exactos de tal forma que respondan con veracidad a la situación actual del titular. Si fuera necesario, se actualizarán; se adoptarán todas las medidas razonables para rectificar o suprimir, sin demora injustificada, los factores que introducen las</p>		<p>tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se trate exclusivamente en cumplimiento de un deber legal o contractual, atendiendo a las disposiciones aplicables a los aspectos administrativos, contables, fiscales, jurídicos, con fines de archivo en interés público, investigación científica, histórica o estadística, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente ley a fin de proteger los derechos y garantías de los titulares.</p> <p>h) «Principio de integridad»: consiste en implantar las medidas de seguridad técnicas y organizativas que garantice que el dato no sea alterado de manera no autorizada. Se prohíbe el tratamiento de datos parciales, incompletos,</p>	<p>inexactitudes en los datos personales con respecto a los fines para los que se tratan. Los datos facilitados directamente por el titular se considerarán exactos.</p> <p>g) «Principio de limitación del plazo de conservación»: los datos deben ser mantenidos de forma que se permita la identificación de los titulares durante no más tiempo del necesario para los fines para los que se tratan; los datos personales podrán conservarse durante períodos más largos siempre que se trate exclusivamente en cumplimiento de un deber legal o contractual, atendiendo a las disposiciones aplicables a los aspectos administrativos, contables, fiscales, jurídicos, con fines de archivo en interés público, investigación científica, histórica</p>	
<p>fracionados o que induzcan a error.</p> <p>i) «Principio de confidencialidad»: los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase del tratamiento, tendrán el deber de garantizar que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. El responsable y/o encargado del tratamiento están obligados a garantizar la reserva de la información, inclusive después de finalizado el tratamiento. El principio señalado será complementario de los deberes de secreto profesional de conformidad con su normativa aplicable.</p> <p>j) «Principio de seguridad»: los sujetos que participen en cualquier etapa del tratamiento deberán realizar análisis de riesgos, orientado a determinar las</p>	<p>o estadística, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente ley a fin de proteger los derechos y garantías de los titulares.</p> <p>h) «Principio de integridad»: consiste en implantar las medidas de seguridad técnicas y organizativas que garantice que el dato no sea alterado de manera no autorizada. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.</p> <p>i) «Principio de confidencialidad»: los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase del tratamiento, tendrán el deber de garantizar que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. El</p>		<p>medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten, con el fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.</p> <p>k) «Principio de proporcionalidad»: durante el ciclo de vida de los datos, el responsable velará porque el tratamiento sea idóneo respecto a los fines; necesario en cuanto no existan otras medidas para conseguir el fin perseguido; y equilibrado respecto al beneficio que dicho tratamiento proporciona y su impacto sobre los derechos y garantías fundamentales de los titulares.</p> <p>l) «Principio de explicabilidad»: los responsables del tratamiento deben ser capaces de explicar de manera clara y comprensible a los titulares cómo se</p>	<p>responsable y/o encargado del tratamiento están obligados a garantizar la reserva de la información, inclusive después de finalizado el tratamiento. El principio señalado será complementario de los deberes de secreto profesional de conformidad con su normativa aplicable.</p> <p>j) «Principio de seguridad»: los sujetos que participen en cualquier etapa del tratamiento deberán realizar análisis de riesgos, orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten, con el fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.</p> <p>k) «Principio de proporcionalidad»: durante el ciclo de vida de los datos, el responsable velará</p>	



Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>están utilizando sus datos personales y cómo se toman las decisiones en función de ellos. Los encargados del tratamiento asistirán al responsable en el cumplimiento de esta obligación.</p> <p>m) «Principio de responsabilidad demostrada» «accountability»: El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en la presente ley, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de protección de datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.</p>	<p>porque el tratamiento sea idóneo respecto a los fines; necesario en cuanto no existan otras medidas para conseguir el fin perseguido; y equilibrado respecto al beneficio que dicho tratamiento proporciona y su impacto sobre los derechos y garantías fundamentales de los titulares.</p> <p>l) «Principio de explicabilidad»: los responsables del tratamiento deben ser capaces de explicar de manera clara y comprensible a los titulares cómo se están utilizando sus datos personales y cómo se toman las decisiones en función de ellos. Los encargados del tratamiento asistirán al responsable en el cumplimiento de esta obligación.</p> <p>m) «Principio de responsabilidad demostrada» «accountability»: El responsable implementará los mecanismos necesarios para acreditar el</p>	
<p>relación relevante entre el titular y el responsable, en particular cuando el titular sea un menor de edad. Se debe realizar un examen de ponderación que garantice que el tratamiento sea lícito, necesario y equilibrado en relación con los derechos del titular.</p> <p>Lo dispuesto en este literal no será aplicable al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.</p> <p>2. Cuando la base jurídica que legitima el tratamiento sea el cumplimiento de un deber legal o el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas la finalidad de este debe estar fundamentada en normativa con rango de ley vigente.</p> <p><i>Parágrafo primero:</i> La normativa vigente a la que se refiere el numeral 2 del presente artículo podrá contener disposiciones específicas para adaptar la aplicación de la presente ley, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los titulares afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para</p>	<p>relación relevante entre el titular y el responsable, en particular cuando el titular sea un menor de edad. Se debe realizar un examen de ponderación que garantice que el tratamiento sea lícito, necesario y equilibrado en relación con los derechos del titular.</p> <p>Lo dispuesto en este literal no será aplicable al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.</p> <p>2. Cuando la base jurídica que legitima el tratamiento sea el cumplimiento de un deber legal o el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas la finalidad de este debe estar fundamentada en normativa con rango de ley vigente.</p> <p><i>Parágrafo primero:</i> La normativa vigente a la que se refiere el numeral 2 del presente artículo podrá contener disposiciones específicas para adaptar la aplicación de la presente ley, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los titulares afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para</p>	<p>Se realizan ajustes atendiendo a las recomendaciones dadas por la Cámara Colombia de Informática y Telecomunicaciones - CCIT-, expresando que: "con el fin de garantizar la seguridad jurídica y dotar al proyecto de ley de total claridad y cohesión en el texto" se procede a realizar la precisión sobre el uso de la "cesión de datos" y su definición.</p>
<p>solicitudes por el titular. .</p> <p>c) El tratamiento es necesario para el cumplimiento de un deber legal aplicable al responsable del tratamiento.</p> <p>d) El tratamiento es necesario en casos de urgencia médica o sanitaria del titular o de otra persona natural.</p> <p>e) El tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución y la ley.</p> <p>f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan sobre los intereses, derechos y garantías fundamentales del titular que requieran la protección de datos personales. Es fundamental que exista una</p>	<p>solicitudes por el titular. .</p> <p>c) El tratamiento es necesario para el cumplimiento de un deber legal aplicable al responsable del tratamiento.</p> <p>d) El tratamiento es necesario en casos de urgencia médica o sanitaria del titular o de otra persona natural.</p> <p>e) El tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución y la ley.</p> <p>f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan sobre los intereses, derechos y garantías fundamentales del titular que requieran la protección de datos personales. Es fundamental que exista una</p>	
<p>están utilizando sus datos personales y cómo se toman las decisiones en función de ellos. Los encargados del tratamiento asistirán al responsable en el cumplimiento de esta obligación.</p> <p>m) «Principio de responsabilidad demostrada» «accountability»: El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en la presente ley, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de protección de datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.</p>	<p>porque el tratamiento sea idóneo respecto a los fines; necesario en cuanto no existan otras medidas para conseguir el fin perseguido; y equilibrado respecto al beneficio que dicho tratamiento proporciona y su impacto sobre los derechos y garantías fundamentales de los titulares.</p> <p>l) «Principio de explicabilidad»: los responsables del tratamiento deben ser capaces de explicar de manera clara y comprensible a los titulares cómo se están utilizando sus datos personales y cómo se toman las decisiones en función de ellos. Los encargados del tratamiento asistirán al responsable en el cumplimiento de esta obligación.</p> <p>m) «Principio de responsabilidad demostrada» «accountability»: El responsable implementará los mecanismos necesarios para acreditar el</p>	
<p>relación relevante entre el titular y el responsable, en particular cuando el titular sea un menor de edad. Se debe realizar un examen de ponderación que garantice que el tratamiento sea lícito, necesario y equilibrado en relación con los derechos del titular.</p> <p>Lo dispuesto en este literal no será aplicable al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.</p> <p>2. Cuando la base jurídica que legitima el tratamiento sea el cumplimiento de un deber legal o el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas la finalidad de este debe estar fundamentada en normativa con rango de ley vigente.</p> <p><i>Parágrafo primero:</i> La normativa vigente a la que se refiere el numeral 2 del presente artículo podrá contener disposiciones específicas para adaptar la aplicación de la presente ley, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los titulares afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para</p>	<p>relación relevante entre el titular y el responsable, en particular cuando el titular sea un menor de edad. Se debe realizar un examen de ponderación que garantice que el tratamiento sea lícito, necesario y equilibrado en relación con los derechos del titular.</p> <p>Lo dispuesto en este literal no será aplicable al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.</p> <p>2. Cuando la base jurídica que legitima el tratamiento sea el cumplimiento de un deber legal o el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas la finalidad de este debe estar fundamentada en normativa con rango de ley vigente.</p> <p><i>Parágrafo primero:</i> La normativa vigente a la que se refiere el numeral 2 del presente artículo podrá contener disposiciones específicas para adaptar la aplicación de la presente ley, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los titulares afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para</p>	<p>Se realizan ajustes atendiendo a las recomendaciones dadas por la Cámara Colombia de Informática y Telecomunicaciones - CCIT-, expresando que: "con el fin de garantizar la seguridad jurídica y dotar al proyecto de ley de total claridad y cohesión en el texto" se procede a realizar la precisión sobre el uso de la "cesión de datos" y su definición.</p>
<p>solicitudes por el titular. .</p> <p>c) El tratamiento es necesario para el cumplimiento de un deber legal aplicable al responsable del tratamiento.</p> <p>d) El tratamiento es necesario en casos de urgencia médica o sanitaria del titular o de otra persona natural.</p> <p>e) El tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución y la ley.</p> <p>f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan sobre los intereses, derechos y garantías fundamentales del titular que requieran la protección de datos personales. Es fundamental que exista una</p>	<p>solicitudes por el titular. .</p> <p>c) El tratamiento es necesario para el cumplimiento de un deber legal aplicable al responsable del tratamiento.</p> <p>d) El tratamiento es necesario en casos de urgencia médica o sanitaria del titular o de otra persona natural.</p> <p>e) El tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución y la ley.</p> <p>f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan sobre los intereses, derechos y garantías fundamentales del titular que requieran la protección de datos personales. Es fundamental que exista una</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo. La normativa vigente cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.</p> <p><i>Parágrafo segundo:</i> Las normativas expedidas con posterioridad a la presente ley podrán introducir disposiciones que cumplan con los criterios establecidos en el presente Régimen General de Protección de Datos con respecto al tratamiento, en cumplimiento del numeral 1, literal c) y e), fijando de manera precisa requisitos específicos de tratamiento y otras medidas de conformidad con la presente ley.</p>	<p>garantizar un tratamiento lícito y equitativo. La normativa vigente cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.</p> <p><i>Parágrafo segundo:</i> Las normativas expedidas con posterioridad a la presente ley podrán introducir disposiciones que cumplan con los criterios establecidos en el presente Régimen General de Protección de Datos con respecto al tratamiento, en cumplimiento del numeral 1, literal c) y e), fijando de manera precisa requisitos específicos de tratamiento y otras medidas de conformidad con la presente ley.</p>	
<p><b>ARTÍCULO 7. Tratamientos con finalidades diferentes a las iniciales.</b></p> <p>Cuando se quiera tratar los datos personales para una finalidad diferente a la que fueron recogidos, y ese nuevo tratamiento no esté basado en el consentimiento del titular o en una norma específica que sea necesaria y proporcional en una sociedad democrática, el responsable del tratamiento deberá considerar si el nuevo tratamiento es compatible con la finalidad original. Para ello, tomará en cuenta lo siguiente:</p> <p>a) La relación entre la finalidad original y la nueva finalidad de tratamiento de los datos personales.</p> <p>b) El contexto en que se recogieron los datos personales, especialmente la relación entre los titulares</p>	<p><b>ARTÍCULO 7. Tratamientos con finalidades diferentes a las iniciales.</b></p> <p>Cuando se quiera tratar los datos personales para una finalidad diferente a la que fueron recogidos, y ese nuevo tratamiento no esté basado en el consentimiento del titular o en una norma específica que sea necesaria y proporcional en una sociedad democrática, el responsable del tratamiento deberá considerar si el nuevo tratamiento es compatible con la finalidad original. Para ello, tomará en cuenta lo siguiente:</p> <p>f) La relación entre la finalidad original y la nueva finalidad de tratamiento de los datos personales.</p> <p>g) El contexto en que se recogieron los datos personales, especialmente la relación entre los</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>fácil acceso, utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente ley.</p> <p>4. El responsable establecerá mecanismos o procedimientos que permitan al titular manifestar su consentimiento mediante un acto afirmativo que refleje una manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.</p> <p>5. Si el responsable del tratamiento solicita el consentimiento del titular durante la ejecución de un contrato y este no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al titular que manifieste expresamente su negativa al tratamiento.</p> <p>6. El titular tendrá derecho a revocar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará la legalidad del tratamiento basada en el consentimiento previo a la revocatoria. Será tan fácil revocar el consentimiento como darlo.</p>	<p>fácil acceso, utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente ley.</p> <p>4. El responsable establecerá mecanismos o procedimientos que permitan al titular manifestar su consentimiento mediante un acto afirmativo que refleje una manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. El silencio, las casillas <del>no</del> marcadas o la inacción no deben constituir consentimiento.</p> <p>5. Si el responsable del tratamiento solicita el consentimiento del titular durante la ejecución de un contrato y este no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al titular que manifieste expresamente su negativa al tratamiento.</p> <p>6. El titular tendrá derecho a revocar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará la legalidad del tratamiento basada en el consentimiento previo a la revocatoria. Será tan fácil revocar el consentimiento como darlo.</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>y el responsable del tratamiento.</p> <p>c) La naturaleza de los datos personales, especialmente si son datos sensibles o relacionados con antecedentes penales, anotaciones judiciales o contravencionales.</p> <p>d) Las posibles consecuencias para los titulares por el nuevo tratamiento de sus datos.</p> <p>e) La existencia de garantías adecuadas, como el cifrado o la seudonimización de los datos.</p>	<p>titulares y el responsable del tratamiento.</p> <p>h) La naturaleza de los datos personales, especialmente si son datos sensibles o relacionados con antecedentes penales, anotaciones judiciales o contravencionales.</p> <p>i) Las posibles consecuencias para los titulares por el nuevo tratamiento de sus datos.</p> <p>j) La existencia de garantías adecuadas, como el cifrado o la seudonimización de los datos.</p>	
<p><b>ARTÍCULO 8. Condiciones para el consentimiento.</b></p> <p>1. Cuando el tratamiento se base en el consentimiento del titular, el responsable deberá ser capaz de demostrar que aquel otorgó el consentimiento de forma previa el tratamiento de sus datos personales.</p> <p>2. Corresponderá al responsable del tratamiento, demostrar la existencia del consentimiento del titular por cualquier medio de prueba admisible en derecho.</p> <p>3. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, debiendo constar cada finalidad de forma separada, inteligible y de</p>	<p><b>ARTÍCULO 8. Condiciones para el consentimiento.</b></p> <p>1. Cuando el tratamiento se base en el consentimiento del titular, el responsable deberá ser capaz de demostrar que aquel otorgó el consentimiento de forma previa el tratamiento de sus datos personales.</p> <p>2. Corresponderá al responsable del tratamiento, demostrar la existencia del consentimiento del titular por cualquier medio de prueba admisible en derecho.</p> <p>3. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, debiendo constar cada finalidad de forma separada, inteligible y de</p>	<p>Se afecta la solicitud para el numeral 4 realizado por ASOFONDO en el sentido de que: "se debe eliminar que las casillas "ya marcadas" no constituyen consentimiento, ya que puede ocurrir que estén pre marcadas pero el titular puede desactivarlas, así mismo al continuar con la navegación se entiende como una acción afirmativa inequívoca del consentimiento de tratamiento de datos".</p>

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p><b>ARTÍCULO 9. Consentimiento de niños, niñas y adolescentes.</b></p> <p>1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de dieciséis años. Se exceptúan los supuestos en que la ley exija la asistencia del representante legal para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.</p> <p>2. El tratamiento de los datos de los menores de dieciséis años, fundado en el consentimiento, sólo será lícito si consta el consentimiento del representante legal, con el alcance que determine el mismo.</p> <p>3. En relación con la oferta directa a menores de edad de servicios de la sociedad de la información, le serán aplicables las reglas establecidas en el numeral 1 y 2 del presente artículo teniendo en cuenta la tecnología disponible. Cuando concorra la situación descrita en el numeral 2, el responsable del tratamiento adoptará todas las medidas razonables con los recursos que dispone, para verificar que el consentimiento fue dado o autorizado por el representante legal del menor.</p> <p>4. El numeral 1 no afectará las disposiciones especiales referentes al establecimiento de edades</p>	<p><b>ARTÍCULO 9. Consentimiento de niños, niñas y adolescentes.</b></p> <p>6. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de dieciséis años. Se exceptúan los supuestos en que la ley exija la asistencia del representante legal para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.</p> <p>7. El tratamiento de los datos de los menores de dieciséis años, fundado en el consentimiento, sólo será lícito si consta el consentimiento del representante legal, con el alcance que determine el mismo.</p> <p>8. En relación con la oferta directa a menores de edad de servicios de la sociedad de la información, le serán aplicables las reglas establecidas en el numeral 1 y 2 del presente artículo teniendo en cuenta la tecnología disponible. Cuando concorra la situación descrita en el numeral 2, el responsable del tratamiento adoptará todas las medidas razonables con los recursos que dispone, para verificar que el consentimiento fue dado o autorizado por el representante legal del menor.</p> <p>9. El numeral 1 no afectará las disposiciones especiales referentes al</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>minimas para efectos civiles y penales, respecto de la validez y consecuencias de ciertos actos jurídicos.</p> <p>5. El tratamiento de datos personales de menores de edad siempre debe responder al interés superior del menor y asegurar el respeto de sus derechos fundamentales.</p> <p><i>Parágrafo:</i> En caso de lo dispuesto en el numeral 2, cuando la representación legal del menor de dieciséis años es ejercida por más de una persona, se presume que el consentimiento de uno obedece a la voluntad de todos. En el supuesto de que, uno de los representantes no esté de acuerdo, puede revocar el consentimiento ante el responsable del tratamiento, y sólo podría concederse nuevamente por el mutuo acuerdo de los representantes, o mediante decisión judicial que declare su representación legal.</p>	<p>establecimiento de edades mínimas para efectos civiles y penales, respecto de la validez y consecuencias de ciertos actos jurídicos.</p> <p>10. El tratamiento de datos personales de menores de edad siempre debe responder al interés superior del menor y asegurar el respeto de sus derechos fundamentales.</p> <p><i>Parágrafo:</i> En caso de lo dispuesto en el numeral 2, cuando la representación legal del menor de dieciséis años es ejercida por más de una persona, se presume que el consentimiento de uno obedece a la voluntad de todos. En el supuesto de que, uno de los representantes no esté de acuerdo, puede revocar el consentimiento ante el responsable del tratamiento, y sólo podría concederse nuevamente por el mutuo acuerdo de los representantes, o mediante decisión judicial que declare su representación legal.</p>		<p>biológicas, identidad o expresión de género y orientación sexual de una persona natural.</p> <p>2. El numeral 1 no será de aplicación cuando concurra alguna de las siguientes excepciones:</p> <p>a) Cuando el titular dio su consentimiento previo y expreso para el tratamiento de dichos datos personales para uno o más fines específicos, excepto cuando la ley impida al titular levantar la prohibición mencionada en el numeral 1.</p> <p>b) Cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral o de la seguridad social, en la medida en que así lo autorice la ley o una convención colectiva de trabajo con arreglo a la normatividad vigente, que establezca garantías adecuadas del respeto de los derechos fundamentales y</p>	<p>biológicas, identidad o expresión de género y orientación sexual de una persona natural.</p> <p>5. El numeral 1 no será de aplicación cuando concurra alguna de las siguientes excepciones:</p> <p>k) Cuando el titular dio su consentimiento previo y expreso para el tratamiento de dichos datos personales para uno o más fines específicos, excepto cuando la ley impida al titular levantar la prohibición mencionada en el numeral 1.</p> <p>l) Cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral o de la seguridad social, en la medida en que así lo autorice la ley o una convención colectiva de trabajo con arreglo a la normatividad vigente, que establezca garantías adecuadas del respeto de los</p>	
<p><b>ARTÍCULO 10. Tratamiento de datos sensibles.</b></p> <p>1. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características</p>	<p><b>ARTÍCULO 10. Tratamiento de datos sensibles.</b></p> <p>4. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características</p>	SIN MODIFICACIONES			
<p>de los intereses del titular.</p> <p>c) Cuando el tratamiento sea necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto que el titular se encuentre incapacitado física o jurídicamente para autorizar dicho tratamiento.</p> <p>d) Cuando el tratamiento sea realizado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otra organización sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el</p>	<p>derechos fundamentales y de los intereses del titular.</p> <p>m) Cuando el tratamiento sea necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto que el titular se encuentre incapacitado física o jurídicamente para autorizar dicho tratamiento.</p> <p>n) Cuando el tratamiento sea realizado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otra organización sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se</p>		<p>consentimiento de los titulares.</p> <p>e) Cuando el tratamiento se refiera a datos personales que el titular de forma libre y voluntaria decida hacer públicos. No debe ser una divulgación de datos accidental, inadvertida o involuntaria.</p> <p>f) Cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones y/o procedimientos administrativos y/o judiciales, así como procedimientos extrajudiciales o cuando sea un órgano judicial que actúe en ejercicio de su función.</p> <p>g) Cuando el tratamiento sea necesario por razones de interés público, para la prestación de servicios públicos o por parte de entidades que ejerzan funciones públicas, sobre la base de la normativa que los faculta para ejercer dichas funciones; el tratamiento debe ser proporcional al objetivo</p>	<p>comuniquen fuera de ellos sin el consentimiento de los titulares.</p> <p>o) Cuando el tratamiento se refiera a datos personales que el titular de forma libre y voluntaria decida hacer públicos. No debe ser una divulgación de datos accidental, inadvertida o involuntaria.</p> <p>p) Cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones y/o procedimientos administrativos y/o judiciales, así como procedimientos extrajudiciales o cuando sea un órgano judicial que actúe en ejercicio de su función.</p> <p>q) Cuando el tratamiento sea necesario por razones de interés público, para la prestación de servicios públicos o por parte de entidades que ejerzan funciones públicas, sobre la base de la normativa que los faculta para ejercer dichas</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>perseguido, respetando el derecho a la protección de datos, <b>estableciendo</b> medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del titular.</p> <p>h) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluaciones médicas ocupacionales del trabajador, diagnóstico médico, prestación de asistencia o tratamiento médico, gestión de los sistemas y prestación de servicios de salud, sobre la base de la normativa o en virtud de un contrato con un profesional de la salud, sin perjuicio de las condiciones y garantías contempladas en el numeral 3 del presente artículo.</p> <p>i) Cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud</p>	<p>funciones; el tratamiento debe ser proporcional al objetivo perseguido, respetando el derecho a la protección de datos, estableciendo medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del titular.</p> <p>r) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluaciones médicas ocupacionales del trabajador, diagnóstico médico, prestación de asistencia o tratamiento médico, gestión de los sistemas y prestación de servicios de salud, sobre la base de la normativa o en virtud de un contrato con un profesional de la salud, sin perjuicio de las condiciones y garantías contempladas en el numeral 3 del presente artículo.</p> <p>s) Cuando el tratamiento sea</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>pública, como la protección frente a amenazas transnacionales graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de la norma, que establezca medidas adecuadas y específicas para proteger los derechos y garantías del titular, en particular el secreto profesional. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y garantías de las personas naturales.</p> <p>j) El tratamiento es necesario con fines de archivo en interés público, investigación científica, histórica o estadística; este debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos, establecer</p>	<p>necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transnacionales graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de la norma, que establezca medidas adecuadas y específicas para proteger los derechos y garantías del titular, en particular el secreto profesional. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y garantías de las personas naturales.</p> <p>t) El tratamiento es necesario con fines de archivo en interés público, investigación científica, histórica o estadística; este debe ser</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.</p> <p>3. Los datos personales a los que se refiere el numeral 1 podrán tratarse a los fines citados en el numeral 2, literal h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto profesional de acuerdo con el artículo 74 de La Constitución Política de Colombia.</p> <p><i>Parágrafo:</i> Cuando por alguna de las causales a las que se refiere el numeral segundo se deban tratar datos sensibles referentes al sexo, identidad o expresión de género y orientación sexual, deberán hacer uso de todas las categorías identitarias diversas, como personas intersexuales y no binarias. En el supuesto de que el titular del dato haya dado su consentimiento para el tratamiento de los datos aquí referidos y ejercite los derechos de rectificación y supresión, no se le exigirán requisitos adicionales para comprobar esta información.</p>	<p>proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos, establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.</p> <p>6. Los datos personales a los que se refiere el numeral 1 podrán tratarse a los fines citados en el numeral 2, literal h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto profesional de acuerdo con el artículo 74 de La Constitución Política de Colombia.</p> <p><i>Parágrafo:</i> Cuando por alguna de las causales a las que se refiere el numeral segundo se deban tratar datos sensibles referentes al sexo, identidad o expresión de género y orientación sexual, deberán hacer uso de todas las categorías identitarias diversas, como personas intersexuales y no binarias. En el supuesto de que el titular del dato haya dado su consentimiento para el tratamiento de los datos aquí</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
	<p>referidos y ejercite los derechos de rectificación y supresión, no se le exigirán requisitos adicionales para comprobar esta información.</p>	
<p><b>ARTÍCULO 11. Tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.</b> El tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales, así como las medidas de seguridad conexas, además de cumplir con las obligaciones establecidas en la presente ley, sólo podrá realizarse bajo la supervisión de las entidades competentes, quienes deberán garantizar la protección adecuada de los derechos y garantías de los titulares.</p>	<p><b>ARTÍCULO 11. Tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.</b> El tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales, así como las medidas de seguridad conexas, además de cumplir con las obligaciones establecidas en la presente ley, sólo podrá realizarse bajo la supervisión de las entidades competentes, quienes deberán garantizar la protección adecuada de los derechos y garantías de los titulares.</p>	SIN MODIFICACIONES
<p><b>ARTÍCULO 12. Tratamiento de datos relativos a sanciones administrativas y/o disciplinarias.</b> 1. El tratamiento de datos relativo a sanciones administrativas y/o disciplinarias, incluido el mantenimiento de registros relacionados con las mismas, exigirá:</p> <p>a) Que los responsables de dichos tratamientos sean los organismos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.</p> <p>b) Que el tratamiento se limite a los datos estrictamente necesarios para la</p>	<p><b>ARTÍCULO 12. Tratamiento de datos relativos a sanciones administrativas y/o disciplinarias.</b> 1. El tratamiento de datos relativo a sanciones administrativas y/o disciplinarias, incluido el mantenimiento de registros relacionados con las mismas, exigirá:</p> <p>a) Que los responsables de dichos tratamientos sean los organismos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.</p> <p>b) Que el tratamiento se limite a los datos estrictamente necesarios para la</p>	SIN MODIFICACIONES



Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>finalidad perseguida por aquel.</p> <p>2. Cuando no se cumpla alguna de las condiciones previstas en el numeral anterior, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias, habrán de contar con el consentimiento del titular o estar autorizados por una norma, en la que se regularán, en su caso, garantías adicionales para los derechos de los titulares.</p> <p>3. Fuera de los supuestos señalados en los numerales anteriores, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias sólo serán posibles cuando sean llevados a cabo por abogados y/o agentes oficiosos y que tengan por objeto recoger la información facilitada por sus representados para el ejercicio de sus funciones.</p> <p><i>Parágrafo:</i> Lo descrito en el presente artículo se aplicará igualmente a las sanciones disciplinarias de los servidores públicos.</p> <p><b>ARTÍCULO 13. Transparencia e información al titular.</b></p> <p>1. El responsable del tratamiento tomará las medidas pertinentes para facilitar al titular toda la información indicada en los artículos 14 y 15, así como cualquier comunicación <b>correspondiente</b> a los ejercicios de los derechos o</p>	<p>finalidad perseguida por aquel.</p> <p>2. Cuando no se cumpla alguna de las condiciones previstas en el numeral anterior, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias, habrán de contar con el consentimiento del titular o estar autorizados por una norma, en la que se regularán, en su caso, garantías adicionales para los derechos de los titulares.</p> <p>3. Fuera de los supuestos señalados en los numerales anteriores, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias sólo serán posibles cuando sean llevados a cabo por abogados y/o agentes oficiosos y que tengan por objeto recoger la información facilitada por sus representados para el ejercicio de sus funciones.</p> <p><i>Parágrafo:</i> Lo descrito en el presente artículo se aplicará igualmente a las sanciones disciplinarias de los servidores públicos.</p> <p><b>ARTÍCULO 13. Transparencia e información al titular.</b></p> <p>1. El responsable del tratamiento tomará las medidas pertinentes para facilitar al titular toda la información indicada en los artículos 14 y 15, así como cualquier comunicación correspondiente a los</p>	<p>Se acepta lo dispuesto por ASOFONDOS para el numeral 4, en el cual se recomienda que: <i>"la potestad de presentar queja ante la autoridad debe estar sujeta al agotamiento previo de reclamación directa ante el responsable, esto evitará la congestión de</i></p>
<p>de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un menor. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. A petición del titular, la información podrá facilitarse verbalmente siempre que se acredite la identidad del mismo por medios adecuados.</p> <p>2. El responsable del tratamiento facilitará al titular mecanismos sencillos y ágiles para el ejercicio de sus derechos en virtud de la presente ley. En caso de que el responsable no esté en condiciones de identificar al titular, no se aplicarán los artículos relativos al ejercicio de derechos de los artículos 18 al 23, salvo que el titular facilite información adicional que permita su identificación.</p> <p>3. El responsable del tratamiento facilitará al titular información <b>relativa</b> a sus actuaciones sobre la base de una solicitud de ejercicio de derechos, dentro de los 15 días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro</p>	<p>ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un menor. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. A petición del titular, la información podrá facilitarse verbalmente siempre que se acredite la identidad del mismo por medios adecuados.</p> <p>2. El responsable del tratamiento facilitará al titular mecanismos sencillos y ágiles para el ejercicio de sus derechos en virtud de la presente ley. En caso de que el responsable no esté en condiciones de identificar al titular, no se aplicarán los artículos relativos al ejercicio de derechos de los artículos 18 al 23, salvo que el titular facilite información adicional que permita su identificación.</p> <p>3. El responsable del tratamiento facilitará al titular información relativa a sus actuaciones sobre la base de una solicitud de ejercicio de derechos, dentro de los 15 días hábiles contados a partir del día siguiente a la fecha de su recibo.</p>	<p>tramites de la autoridad competente y la solución eficiente de solicitudes".</p>
<p>de dicho término, se informará al titular los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.</p> <p>Cuando el titular presente la solicitud por medios electrónicos, la información se facilitará por dichos medios cuando sea posible, a menos que el titular solicite que se facilite de otro modo que no represente una carga desproporcionada para el responsable.</p> <p>4. El responsable del tratamiento tiene la obligación de contestar las solicitudes de ejercicio de derechos de forma completa y <b>de fondo</b>. En todas las contestaciones de ejercicio de derechos, se deberá informar la posibilidad de presentar una queja ante la autoridad de protección de datos.</p> <p>5. La información facilitada en virtud de los artículos 14 y 15, así como cualquier comunicación correspondiente a los ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, serán a título gratuito. Para tal efecto, se podrá considerar reiterativo el ejercicio del derecho de acceso en más de una ocasión en menos de un mes, a menos que exista</p>	<p>Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al titular los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.</p> <p>Cuando el titular presente la solicitud por medios electrónicos, la información se facilitará por dichos medios cuando sea posible, a menos que el titular solicite que se facilite de otro modo que no represente una carga desproporcionada para el responsable.</p> <p>4. El responsable del tratamiento tiene la obligación de contestar las solicitudes de ejercicio de derechos de forma completa y de fondo. En todas las contestaciones de ejercicio de derechos, se deberá informar la posibilidad de presentar una queja ante la autoridad de protección de datos.</p> <p><u>La potestad de presentar queja ante la autoridad debe estar sujeta al agotamiento previo de reclamación directa ante el responsable de los datos con el fin de obtener una solución eficiente de la solicitud.</u></p> <p>5. La información facilitada en virtud de los artículos 14 y 15, así como cualquier comunicación correspondiente a los</p>	
<p>causa legítima para ello. El responsable deberá demostrar a la autoridad de protección de datos, cuando ésta así lo requiera, que la conducta del titular es carente de fundamento legal, temeraria y/o reiterativa.</p> <p>6. Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad del titular que radicó una solicitud de ejercicio de derechos, podrá requerir a éste información adicional necesaria para confirmar su identidad.</p> <p>7. La información que deba facilitarse a los titulares en virtud de los artículos 14 y 15 podrá compartirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. Los responsables tendrán en cuenta a los titulares con discapacidades.</p> <p>8. La Autoridad de protección de datos establecerá las reglas, símbolos e imágenes mediante las cuales el responsable del tratamiento o el encargado podrán dar cumplimiento al deber de información, comunicación de políticas de tratamiento de la información, divulgación de información sobre</p>	<p>ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, serán a título gratuito. Para tal efecto, se podrá considerar reiterativo el ejercicio del derecho de acceso en más de una ocasión en más de una ocasión en más de un mes, a menos que exista causa legítima para ello. El responsable deberá demostrar a la autoridad de protección de datos, cuando ésta así lo requiera, que la conducta del titular es carente de fundamento legal, temeraria y/o reiterativa.</p> <p>6. Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad del titular que radicó una solicitud de ejercicio de derechos, podrá requerir a éste información adicional necesaria para confirmar su identidad.</p> <p>7. La información que deba facilitarse a los titulares en virtud de los artículos 14 y 15 podrá compartirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. Los responsables tendrán en cuenta a los titulares con discapacidades.</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
seguridad de datos, notificación de derechos de los titulares de datos, así como otras circunstancias en las que sea necesario su aplicación.	8. La Autoridad de protección de datos establecerá las reglas, símbolos e imágenes mediante las cuales el responsable del tratamiento o el encargado podrán dar cumplimiento al deber de información, comunicación de políticas de tratamiento de la información, divulgación de información sobre seguridad de datos, notificación de derechos de los titulares de datos, así como otras circunstancias en las que sea necesario su aplicación.		protección de datos personales. c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento. d) Los destinatarios de los datos personales, si los hubiera. e) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel adecuado de protección de la autoridad de protección de datos. En los casos de las transferencias indicadas en los artículos 49 o 51, la información referente a las garantías adecuadas o apropiadas, y los medios para obtener una copia de estas o al hecho de que se hayan prestado. f) El plazo durante el cual se conservarán los datos personales o, cuando no sea	datos o área encargada de la protección de datos personales. c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento. d) Los destinatarios de los datos personales, si los hubiera. e) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel adecuado de protección de la autoridad de protección de datos. En los casos de las transferencias indicadas en los artículos 49 o 51, la información referente a las garantías adecuadas o apropiadas, y los medios para obtener una copia de estas o al hecho de que se hayan prestado. f) El plazo durante el cual se conservarán los	
<b>ARTÍCULO 14. Información que deberá facilitarse cuando los datos personales se obtengan del titular.</b> 1. Cuando se obtienen de un titular datos personales relativos a este, el responsable del tratamiento, en el momento en que estos se obtienen, le facilitará toda la información indicada a continuación: a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal. b) Los datos de contacto del oficial de protección de datos o área encargada de la	<b>ARTÍCULO 14. Información que deberá facilitarse cuando los datos personales se obtengan del titular.</b> 1. Cuando se obtienen de un titular datos personales relativos a este, el responsable del tratamiento, en el momento en que estos se obtienen, le facilitará toda la información <u>requerida, específica y separada que se describe</u> <del>indicada</del> a continuación: a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal. b) Los datos de contacto del oficial de protección de	Se realizan modificaciones al numeral 1 atendiendo las recomendaciones realizadas por ASOFONDOS en el sentido de dejar claridades sobre la solicitud de autorización de tratamiento de datos.  Se realizan ajustes atendiendo a las recomendaciones dadas por la Cámara Colombia de Informática y Telecomunicaciones - CCIT-, expresando que: "con el fin de garantizar la seguridad jurídica y dotar al proyecto de ley de total claridad y cohesión en el texto" se procede a realizar la precisión sobre el uso de la "cesión de datos" y su definición.			
posible, los criterios utilizados para determinar este plazo. g) La descripción y ejercicio de los derechos que le asisten al titular. h) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación. i) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos. j) Cuando la comunicación de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular	datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo. g) La descripción y ejercicio de los derechos que le asisten al titular. h) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación. i) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos. j) Cuando la <u>cesión</u> <del>comunicación</del> de datos personales sea un requisito legal o contractual, o un requisito necesario para		debe estar informado de las posibles consecuencias de no facilitar tales datos. k) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular. 2. Cuando el responsable proyecte uno o varios tratamientos de datos personales con finalidades diferentes a las iniciales, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 1 del presente artículo. 3. Las disposiciones de los numerales 1 y 2 no serán aplicables en la medida en que el titular ya disponga de la información y exista prueba de ello.	suscribir un contrato, el titular debe estar informado de las posibles consecuencias de no facilitar tales datos. k) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular. 2. Cuando el responsable proyecte uno o varios tratamientos de datos personales con finalidades diferentes a las iniciales, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 1 del presente artículo. 3. Las disposiciones de los numerales 1 y 2 no serán aplicables en la medida en que el titular ya disponga de la información y exista prueba de ello.	
			<b>ARTÍCULO 15. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del titular.</b> 1. Cuando los datos personales no se hayan obtenido del titular, el responsable del	<b>ARTÍCULO 15. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del titular.</b> 1. Cuando los datos personales no se hayan obtenido del titular, el responsable del	Se realizan ajustes atendiendo a las recomendaciones dadas por la Cámara Colombia de Informática y Telecomunicaciones - CCIT-, expresando que: "con el fin de garantizar la

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>tratamiento le facilitará a este la siguiente información:</p> <p>a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.</p> <p>b) Los datos de contacto del oficial de protección de datos o área encargada de datos personales.</p> <p>c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.</p> <p>d) Las categorías de datos personales de que se trate.</p> <p>e) Los destinatarios de los datos personales, si aplica.</p> <p>f) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel de adecuado de protección de la autoridad de</p>	<p>tratamiento le facilitará a este la siguiente información:}</p> <p>a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.</p> <p>b) Los datos de contacto del oficial de protección de datos o área encargada de datos personales.</p> <p>c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.</p> <p>d) Las categorías de datos personales de que se trate.</p> <p>e) Los destinatarios de los datos personales, si aplica.</p> <p>f) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de protección de la</p>	<p>seguridad jurídica y dotar al proyecto de ley de total claridad y cohesión en el texto" se procede a realizar la precisión sobre el uso de la "cesión de datos" y su definición.</p>	<p>protección de datos, o, en el caso de las transferencias indicadas en la presente ley referente a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.</p> <p>g) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.</p> <p>h) La descripción y ejercicio de los derechos que le asisten al titular.</p> <p>i) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación.</p>	<p>autoridad de protección de datos, o, en el caso de las transferencias indicadas en la presente ley referente a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.</p> <p>g) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.</p> <p>h) La descripción y ejercicio de los derechos que le asisten al titular.</p> <p>i) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación.</p>	
<p>j) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.</p> <p>k) Cuando la comunicación de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles consecuencias de no facilitar tales datos.</p> <p>l) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.</p> <p>2. El responsable del tratamiento facilitará al titular la información indicada en el numeral 1:</p> <p>a) Dentro de un plazo razonable, una vez</p>	<p>j) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.</p> <p>k) Cuando la <del>comunicación</del> <b>cesión</b> de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles consecuencias de no facilitar tales datos.</p> <p>l) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.</p> <p>2. El responsable del tratamiento facilitará al titular la información indicada en el numeral 1:</p> <p>a) Dentro de un plazo razonable, una vez obtenidos los datos</p>		<p>obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se trate dichos datos.</p> <p>b) Si los datos personales han de utilizarse para comunicación con el titular, a más tardar en el momento de la primera comunicación a dicho titular.</p> <p>c) Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.</p> <p>3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 2.</p> <p>4. Las disposiciones de los apartados 1 a 4 no serán aplicables en la medida en que:</p> <p>a) El titular ya disponga de la información.</p>	<p>personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se trate dichos datos.</p> <p>b) Si los datos personales han de utilizarse para comunicación con el titular, a más tardar en el momento de la primera comunicación a dicho titular.</p> <p>c) Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.</p> <p>3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 2.</p> <p>4. Las disposiciones de los apartados 1 a 4 no serán aplicables en la medida en que:</p> <p>a) El titular ya disponga de la información.</p> <p>b) La comunicación de dicha información resulte imposible o suponga una carga desproporcionada, en particular para el tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística, a reserva de las condiciones y garantías indicadas en la presente ley, o en la medida en que la</p>	







Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>b) El titular retire el consentimiento en que se basa el tratamiento de conformidad con la presente ley y este no se fundamente en otra base legitimadora.</p> <p>c) El titular se oponga al tratamiento con arreglo a la presente ley y no prevalezcan otros motivos legítimos.</p> <p>d) Los datos personales hayan sido tratados ilícitamente.</p> <p>e) Los datos personales deben suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.</p> <p>f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de edad mencionados en la presente ley.</p> <p>g) La autoridad de protección de datos determine que en el tratamiento ha incurrido en conductas contrarias a la Constitución o la presente ley.</p> <p>2. Cuando haya cedido los datos personales y esté</p>	<p>tratados de otro modo.</p> <p>b) El titular retire el consentimiento en que se basa el tratamiento de conformidad con la presente ley y este no se fundamente en otra base legitimadora.</p> <p>c) El titular se oponga al tratamiento con arreglo a la presente ley y no prevalezcan otros motivos legítimos.</p> <p>d) Los datos personales hayan sido tratados ilícitamente.</p> <p>e) Los datos personales deben suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.</p> <p>f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de edad mencionados en la presente ley.</p> <p>g) La autoridad de protección de datos determine que en el tratamiento ha incurrido en conductas contrarias a la</p>		<p>obligado, en virtud de lo dispuesto en el numeral 1, a suprimir dichos datos, el responsable del tratamiento teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los destinatarios o terceros que estén tratando los datos personales de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.</p> <p>3. Los numerales 1 y 2 no se aplicarán cuando el tratamiento sea necesario:</p> <p>a) Para ejercer el derecho a la libertad de expresión e información.</p> <p>b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la ley que se aplique al responsable del tratamiento, o para el cumplimiento de una función realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.</p> <p>c) Por razones de interés público en el ámbito de la salud pública de</p>	<p>Constitución o la presente ley.</p> <p>2. Cuando haya cedido los datos personales y esté obligado, en virtud de lo dispuesto en el numeral 1, a suprimir dichos datos, el responsable del tratamiento teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los destinatarios o terceros que estén tratando los datos personales de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.</p> <p>3. Los numerales 1 y 2 no se aplicarán cuando el tratamiento sea necesario:</p> <p>a) Para ejercer el derecho a la libertad de expresión e información.</p> <p>b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la ley que se aplique al responsable del tratamiento, o para el cumplimiento de una función realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.</p> <p>c) Por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 10, numeral 2, literales h) e i), y numeral 3 de la presente ley.</p> <p>d) Con fines de archivo en interés público, investigación científica, o estadística, en la medida en que el derecho de</p>	
<p>conformidad con el artículo 10, numeral 2, literales h) e i), y numeral 3 de la presente ley.</p> <p>d) Con fines de archivo en interés público, investigación científica, o estadística, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.</p> <p>e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.</p> <p>f) <b><u>Para la conservación de los datos personales en el desarrollo del derecho a la seguridad social y a la obligación legal de conservación que tienen las entidades que hacen parte de este sistema.</u></b></p> <p>e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.</p>	<p>supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.</p> <p>e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.</p> <p>f) <b><u>Para la conservación de los datos personales en el desarrollo del derecho a la seguridad social y a la obligación legal de conservación que tienen las entidades que hacen parte de este sistema.</u></b></p>		<p>solicite en su lugar la limitación de su uso.</p> <p>c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de reclamos administrativos o judiciales.</p> <p>d) El titular se haya opuesto al tratamiento en virtud de la presente ley, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular.</p>	<p>solicite en su lugar la limitación de su uso.</p> <p>c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de reclamos administrativos o judiciales.</p> <p>d) El titular se haya opuesto al tratamiento en virtud de la presente ley, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular.</p>	
<p><b>ARTÍCULO 21. Derecho a la limitación del tratamiento.</b></p> <p>1. El titular tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las siguientes condiciones:</p> <p>a) El titular impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.</p> <p>b) El tratamiento sea ilícito y el titular se oponga a la supresión de los datos personales y</p>	<p><b>ARTÍCULO 21. Derecho a la limitación del tratamiento.</b></p> <p>1. El titular tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las siguientes condiciones:</p> <p>a) El titular impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.</p> <p>b) El tratamiento sea ilícito y el titular se oponga a la supresión de los datos personales y</p>	SIN MODIFICACIONES	<p>2. Cuando el tratamiento de datos personales se haya limitado en virtud del numeral 1, dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del titular; o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales; o con miras a la protección de los derechos de otra persona natural o jurídica o por razones de interés público.</p> <p>3. Todo titular que haya obtenido la limitación del tratamiento con arreglo al numeral 1, será informado por el responsable antes del</p>	<p>2. Cuando el tratamiento de datos personales se haya limitado en virtud del numeral 1, dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del titular; o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales; o con miras a la protección de los derechos de otra persona natural o jurídica o por razones de interés público.</p> <p>3. Todo titular que haya obtenido la limitación del tratamiento con arreglo al numeral 1, será informado por el responsable antes del</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
levantamiento de dicha limitación.		
<b>ARTÍCULO 22. Obligación de notificar la rectificación o supresión de datos personales o la limitación del tratamiento.</b> El responsable del tratamiento notificará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo a esta ley, a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado y esté en condición de demostrarlo. El responsable informará al titular acerca de dichos destinatarios, si éste así lo solicita.	<b>ARTÍCULO 22. Obligación de notificar la rectificación o supresión de datos personales o la limitación del tratamiento.</b> El responsable del tratamiento notificará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo a esta ley, a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado y esté en condición de demostrarlo. El responsable informará al titular acerca de dichos destinatarios, si éste así lo solicita.	SIN MODIFICACIONES
<b>ARTÍCULO 23. Derecho a la portabilidad de los datos.</b> 1. El titular tendrá derecho a recibir los datos personales que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común, lectura mecánica e interoperable y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) El tratamiento esté basado en el consentimiento o en un contrato con arreglo a esta ley. b) El tratamiento se efectúe por medios automatizados. 2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos personales se	<b>ARTÍCULO 23. Derecho a la portabilidad de los datos.</b> 1. El titular tendrá derecho a recibir los datos personales que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común, lectura mecánica e interoperable y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) El tratamiento esté basado en el consentimiento o en un contrato con arreglo a esta ley. b) El tratamiento se efectúe por medios automatizados. 2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3. El ejercicio del derecho mencionado en el numeral 1 del presente artículo se entenderá sin perjuicio de lo dispuesto en esta ley. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una función realizada en interés público, en el ejercicio de poderes o funciones públicas conferidas al responsable del tratamiento. 4. El derecho mencionado en el numeral 1 no afectará negativamente los derechos y garantías de otras personas naturales. 5. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.	personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3. El ejercicio del derecho mencionado en el numeral 1 del presente artículo se entenderá sin perjuicio de lo dispuesto en esta ley. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una función realizada en interés público, en el ejercicio de poderes o funciones públicas conferidas al responsable del tratamiento. 4. El derecho mencionado en el numeral 1 no afectará negativamente los derechos y garantías de otras personas naturales. 5. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.	
<b>ARTÍCULO 24. Derecho de oposición.</b>	<b>ARTÍCULO 24. Derecho de oposición.</b>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
1. El titular tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de un tratamiento basado en lo dispuesto en esta ley, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las garantías del titular, o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales. 2. Cuando el tratamiento de datos personales tenga por objeto marketing y publicidad directa, el titular tendrá derecho a oponerse en todo momento al tratamiento de sus datos personales, incluida la elaboración de perfiles en la medida en que esté relacionada con marketing y publicidad. Cuando el titular se oponga al tratamiento con fines de marketing y publicidad directa, los datos personales dejarán de ser tratados para tal fin. 3. A más tardar en el momento de la primera comunicación con el titular, el derecho indicado en los numerales 1 y 2 será mencionado	1. El titular tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de un tratamiento basado en lo dispuesto en esta ley, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las garantías del titular, o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales. 2. Cuando el tratamiento de datos personales tenga por objeto marketing y publicidad directa, el titular tendrá derecho a oponerse en todo momento al tratamiento de sus datos personales, incluida la elaboración de perfiles en la medida en que esté relacionada con marketing y publicidad. Cuando el titular se oponga al tratamiento con fines de marketing y publicidad directa, los datos personales dejarán de ser tratados para tal fin. 3. A más tardar en el momento de la primera comunicación con el titular, el derecho indicado en los numerales 1 y 2 será	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
4. En el contexto de la utilización de servicios de la sociedad de la información, el titular podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas. 5. Cuando los datos personales se traten con fines de investigación científica, histórica o estadística, el titular tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de sus datos personales, salvo que sea necesario, para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas.	mencionado explícitamente al titular y será presentado claramente y al margen de cualquier otra información. 4. En el contexto de la utilización de servicios de la sociedad de la información, el titular podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas. 5. Cuando los datos personales se traten con fines de investigación científica, histórica o estadística, el titular tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de sus datos personales, salvo que sea necesario, para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas.	
<b>ARTÍCULO 25. Decisiones individuales automatizadas, incluida la elaboración de perfiles.</b> 1. Todo titular tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, en los que no medie intervención humana alguna, incluida la elaboración de perfiles, que le produzca efectos jurídicos o le afecte significativamente de modo similar. 2. El numeral 1 no se aplicará, si la decisión:	<b>ARTÍCULO 25. Decisiones individuales automatizadas, incluida la elaboración de perfiles.</b> 1. Todo titular tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, en los que no medie intervención humana alguna, incluida la elaboración de perfiles, que le produzca efectos jurídicos o le afecte significativamente de modo similar. 2. El numeral 1 no se aplicará, si la decisión:	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>a) Es necesaria para la celebración o la ejecución de un contrato entre el titular y un responsable del tratamiento.</p> <p>b) Está autorizada por una ley que se aplique al responsable del tratamiento, siempre que se establezcan medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.</p> <p>c) Se basa en el consentimiento explícito del titular.</p> <p>3. En los casos a que se refiere el numeral 2, literales a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y garantías fundamentales del titular, como mínimo el derecho a obtener intervención humana por parte del responsable, expresar su punto de vista, recibir una explicación de la decisión e impugnar la decisión.</p> <p>4. Las decisiones a las que se refiere el numeral 2, no se basarán en datos sensibles contemplados en esta ley, salvo que se apliquen las excepciones previstas en la presente ley y se hayan tomado medidas adecuadas para salvaguardar los derechos,</p>	<p>a) Es necesaria para la celebración o la ejecución de un contrato entre el titular y un responsable del tratamiento.</p> <p>b) Está autorizada por una ley que se aplique al responsable del tratamiento, siempre que se establezcan medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.</p> <p>c) Se basa en el consentimiento explícito del titular.</p> <p>2. En los casos a que se refiere el numeral 2, literales a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y garantías fundamentales del titular, como mínimo el derecho a obtener intervención humana por parte del responsable, expresar su punto de vista, recibir una explicación de la decisión e impugnar la decisión.</p> <p>3. Las decisiones a las que se refiere el numeral 2, no se basarán en datos sensibles contemplados en esta ley, salvo que se apliquen las excepciones previstas en la presente ley y se hayan tomado medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>garantías e intereses del titular.</p> <p><b>ARTÍCULO 26. Derecho a presentar una queja ante la autoridad de protección de datos.</b></p> <p>1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley, tendrá derecho a presentar una queja ante la autoridad de protección de datos.</p> <p>2. El titular o quien represente sus intereses sólo podrá elevar queja ante la autoridad de protección de datos, una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de una solicitud previa, con ejercicio de derechos, ante el responsable o el encargado según sea el caso siempre que, habiendo transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de existir respuesta, esta no satisfaga los intereses del titular.</p> <p><b>ARTÍCULO 27. Derecho a presentar una denuncia ante la Autoridad de protección de datos.</b></p> <p>1. Quien tenga conocimiento sobre hechos que deriven en el posible incumplimiento de las disposiciones establecidas en esta ley, tendrá derecho</p>	<p><b>ARTÍCULO 26. Derecho a presentar una queja ante la autoridad de protección de datos.</b></p> <p>1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley, tendrá derecho a presentar una queja ante la autoridad de protección de datos.</p> <p>2. El titular o quien represente sus intereses sólo podrá elevar queja ante la autoridad de protección de datos, una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de una solicitud previa, con ejercicio de derechos, ante el responsable o el encargado según sea el caso siempre que, habiendo transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de existir respuesta, esta no satisfaga los intereses del titular.</p> <p><b>ARTÍCULO 27. Derecho a presentar una denuncia ante la Autoridad de protección de datos.</b></p> <p>1. Quien tenga conocimiento sobre hechos que deriven en el posible incumplimiento de las disposiciones establecidas</p>	<p>SIN MODIFICACIONES</p> <p>SIN MODIFICACIONES</p>

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>a presentar una denuncia ante la <b>autoridad de protección</b> de datos, persiguiendo la protección del interés colectivo y el derecho a la protección de los datos personales.</p> <p>2. La denuncia podrá presentarse a nombre propio o de forma anónima. Si quien presenta la denuncia solicita a la autoridad de protección de datos la reserva de su identidad, ésta deberá adoptar las medidas técnicas necesarias para evitar a terceros conocer los datos personales del denunciante.</p> <p>3. La autoridad de protección de datos tendrá la obligación de examinar integralmente las denuncias presentadas por los ciudadanos. Con base en los hechos presentados, los documentos aportados y las indagaciones preliminares que realice, determinará si existe mérito o no para iniciar una investigación administrativa y, como resultado de ellas, establecerá las medidas que sean necesarias para hacer efectivo el derecho a la protección de los datos personales conforme a lo establecido en la presente ley.</p> <p><b>ARTÍCULO 27. Deberes del responsable del tratamiento.</b> Los responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la</p>	<p>en esta ley, tendrá derecho a presentar una denuncia ante la autoridad de protección de datos, persiguiendo la protección del interés colectivo y el derecho a la protección de los datos personales.</p> <p>2. La denuncia podrá presentarse a nombre propio o de forma anónima. Si quien presenta la denuncia solicita a la autoridad de protección de datos la reserva de su identidad, ésta deberá adoptar las medidas técnicas necesarias para evitar a terceros conocer los datos personales del denunciante.</p> <p>3. La autoridad de protección de datos tendrá la obligación de examinar integralmente las denuncias presentadas por los ciudadanos. Con base en los hechos presentados, los documentos aportados y las indagaciones preliminares que realice, determinará si existe mérito o no para iniciar una investigación administrativa y, como resultado de ellas, establecerá las medidas que sean necesarias para hacer efectivo el derecho a la protección de los datos personales conforme a lo establecido en la presente ley.</p> <p><b>ARTÍCULO 282. Deberes del responsable del tratamiento.</b> Los responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la</p>	<p>Se realiza ajuste en la numeración</p>

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>presente ley y en otras que rijan su actividad:</p> <p>1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.</p> <p>2. Establecer una base jurídica que legitime el tratamiento de datos personales de acuerdo con lo establecido en el artículo 6 de la presente ley.</p> <p>3. Implementar medidas de seguridad de conformidad con el artículo 35, a fin de garantizar y demostrar que el tratamiento es conforme con la presente ley. Revisar y actualizar dichas medidas cuando sea necesario.</p> <p>4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley.</p> <p>5. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos a lo que haya tenido acceso y adoptar las demás medidas necesarias para que la información suministrada a este, se mantenga actualizada.</p> <p>6. Garantizar el pleno ejercicio de los derechos que le conciernen a los titulares en los términos previstos en los artículos 18 al 27 de la presente ley y en las demás normas que la modifiquen o adicionen.</p> <p>7. Cumplir con el deber de información contenido en</p>	<p>presente ley y en otras que rijan su actividad:</p> <p>1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.</p> <p>2. Establecer una base jurídica que legitime el tratamiento de datos personales de acuerdo con lo establecido en el artículo 6 de la presente ley.</p> <p>3. Implementar medidas de seguridad de conformidad con el artículo 35, a fin de garantizar y demostrar que el tratamiento es conforme con la presente ley. Revisar y actualizar dichas medidas cuando sea necesario.</p> <p>4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley.</p> <p>5. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos a lo que haya tenido acceso y adoptar las demás medidas necesarias para que la información suministrada a este, se mantenga actualizada.</p> <p>6. Garantizar el pleno ejercicio de los derechos que le conciernen a los titulares en los términos previstos en los artículos 18 al 27 de la presente ley y en las demás normas que la modifiquen o adicionen.</p> <p>7. Cumplir con el deber de información contenido en</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>los artículos 14 y 15 de la presente ley</p> <p>8. Notificar a la autoridad de protección de datos, cuando se presenten incidentes de seguridad de conformidad con el artículo 36 de la presente ley.</p> <p>9. Comunicar los incidentes de seguridad, cuando sea el caso, a los titulares afectados de conformidad con el artículo 37 de la presente ley.</p> <p>10. Cumplir las instrucciones y requerimientos que imparta la autoridad de protección de datos.</p> <p>11. Elaborar evaluaciones de impacto sobre la privacidad, cuando sea el caso, en los términos descritos en el artículo 38 de la presente ley.</p> <p>12. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.</p> <p>13. Llevar un registro de las actividades del tratamiento en los términos descritos en el artículo 33 de la presente ley.</p> <p>14. Realizar una revisión interna o externa, a los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, al menos cada dos años, para verificar el cumplimiento de la presente ley.</p> <p>Con carácter extraordinario deberá realizarse dicha revisión siempre que se realicen modificaciones</p>	<p>los artículos 14 y 15 de la presente ley</p> <p>8. Notificar a la autoridad de protección de datos, cuando se presenten incidentes de seguridad de conformidad con el artículo 36 de la presente ley.</p> <p>9. Comunicar los incidentes de seguridad, cuando sea el caso, a los titulares afectados de conformidad con el artículo 37 de la presente ley.</p> <p>10. Cumplir las instrucciones y requerimientos que imparta la autoridad de protección de datos.</p> <p>11. Elaborar evaluaciones de impacto sobre la privacidad, cuando sea el caso, en los términos descritos en el artículo 38 de la presente ley.</p> <p>12. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.</p> <p>13. Llevar un registro de las actividades del tratamiento en los términos descritos en el artículo 33 de la presente ley.</p> <p>14. Realizar una revisión interna o externa, a los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, al menos cada dos años, para verificar el cumplimiento de la presente ley.</p> <p>Con carácter extraordinario deberá</p>	
<p>sustanciales en el sistema de información que puedan repercutir en el cumplimiento de la presente ley. Con dicha revisión se reiniciará el cómputo de los dos años señalados en el inciso anterior.</p> <p>15. Cooperar con la autoridad de protección de datos cuando lo solicite.</p> <p>16. Elegir un encargado o encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla con los requisitos establecidos en el artículo 32 de la presente ley y garantice la protección de los derechos del titular.</p> <p>17. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.</p> <p>18. Demostrar el cumplimiento del código de conducta al que se haya adherido, de conformidad con el artículo 42 de la presente ley.</p> <p>19. Mantener los compromisos que le ha permitido acceder a un mecanismo de certificación de certificación en los términos descritos en el artículo 45 de la presente ley.</p>	<p>realizarse dicha revisión siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de la presente ley. Con dicha revisión se reiniciará el cómputo de los dos años señalados en el inciso anterior.</p> <p>15. Cooperar con la autoridad de protección de datos cuando lo solicite.</p> <p>16. Elegir un encargado o encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla con los requisitos establecidos en el artículo 32 de la presente ley y garantice la protección de los derechos del titular.</p> <p>17. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.</p> <p>18. Demostrar el cumplimiento del código de conducta al que se haya adherido, de conformidad con el artículo 42 de la presente ley.</p> <p>Mantener los compromisos que le ha permitido acceder a un mecanismo de certificación de certificación en los términos descritos en el artículo 45 de la presente ley.</p>	
<p><b>ARTICULO 29. Deberes del encargado del tratamiento.</b> Los encargados del tratamiento deberán cumplir los siguientes</p>	<p><b>ARTICULO 29. Deberes del encargado del tratamiento.</b> Los encargados del tratamiento deberán cumplir los siguientes</p>	SIN MODIFICACIONES
<p>deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.</p> <p>2. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe alguno de los principios contemplados en la presente ley o cualquier otra disposición en materia de protección, informará inmediatamente al responsable.</p> <p>3. Utilizar los datos personales objeto de tratamiento, sólo para la finalidad del encargo. En ningún caso podrá utilizar los datos para fines propios.</p> <p>4. Llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, de conformidad con el artículo 33 de la presente ley.</p> <p>5. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento.</p> <p>6. No subcontratar ninguna de las prestaciones que formen parte del encargo, salvo que cuente con autorización expresa del responsable.</p>	<p>deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.</p> <p>2. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe alguno de los principios contemplados en la presente ley o cualquier otra disposición en materia de protección, informará inmediatamente al responsable.</p> <p>3. Utilizar los datos personales objeto de tratamiento, sólo para la finalidad del encargo. En ningún caso podrá utilizar los datos para fines propios.</p> <p>4. Llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, de conformidad con el artículo 33 de la presente ley.</p> <p>5. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento.</p> <p>6. No subcontratar ninguna de las prestaciones que formen parte del encargo, salvo que cuente con</p>	
<p>7. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del encargo, incluso después de que finalice el mismo.</p> <p>8. Garantizar que el personal, con acceso a datos personales objeto del encargo reciba formación sobre protección de datos y se comprometa por escrito a mantener la confidencialidad y cumplir con las medidas de seguridad. El encargado debe mantener a disposición del responsable y/o la autoridad competente, la documentación que demuestre el cumplimiento de estas obligaciones.</p> <p>9. El encargado informará al responsable del tratamiento, sobre cualquier incidente de seguridad relacionado con los datos personales objeto del tratamiento, proporcionando toda la información pertinente necesaria para documentar y notificar el incidente a la autoridad de protección de datos.</p> <p>10. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.</p> <p>11. Garantizar que las transferencias internacionales cumplan las condiciones</p>	<p>autorización expresa del responsable.</p> <p>7. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del encargo, incluso después de que finalice el mismo.</p> <p>8. Garantizar que el personal, con acceso a datos personales objeto del encargo reciba formación sobre protección de datos y se comprometa por escrito a mantener la confidencialidad y cumplir con las medidas de seguridad. El encargado debe mantener a disposición del responsable y/o la autoridad competente, la documentación que demuestre el cumplimiento de estas obligaciones.</p> <p>9. El encargado informará al responsable del tratamiento, sobre cualquier incidente de seguridad relacionado con los datos personales objeto del tratamiento, proporcionando toda la información pertinente necesaria para documentar y notificar el incidente a la autoridad de protección de datos.</p> <p>10. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.</p> <p>11. Garantizar que las transferencias internacionales cumplan</p>	



Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>establecidas en el Título VI de la presente ley.</p> <p>12. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando sea el caso, de conformidad con el artículo 38 de la presente ley.</p> <p>13. Poner a disposición del responsable o de la Autoridad de Protección de Datos, toda la información necesaria para demostrar el cumplimiento de sus obligaciones.</p> <p>14. Implantar las medidas de seguridad acordadas con el responsable del tratamiento, así como aquellas que correspondan en función del riesgo asociado a la prestación del servicio.</p> <p>15. Eliminar o devolver al responsable del tratamiento los datos personales, así como los soportes en los que estén almacenados, una vez finalizada la prestación del servicio. La devolución debe incluir la eliminación completa de los datos almacenados en los equipos informáticos utilizados por el encargado, a menos que existan excepciones legales y/ o contractuales.</p> <p>16. Cooperar con la autoridad de protección de datos cuando lo solicite.</p>	<p>las condiciones establecidas en el Título VI de la presente ley.</p> <p>12. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando sea el caso, de conformidad con el artículo 38 de la presente ley.</p> <p>13. Poner a disposición del responsable o de la Autoridad de Protección de Datos, toda la información necesaria para demostrar el cumplimiento de sus obligaciones.</p> <p>14. Implantar las medidas de seguridad acordadas con el responsable del tratamiento, así como aquellas que correspondan en función del riesgo asociado a la prestación del servicio.</p> <p>15. Eliminar o devolver al responsable del tratamiento los datos personales, así como los soportes en los que estén almacenados, una vez finalizada la prestación del servicio. La devolución debe incluir la eliminación completa de los datos almacenados en los equipos informáticos utilizados por el encargado, a menos que existan excepciones legales y/ o contractuales.</p> <p>16. Cooperar con la autoridad de protección de datos cuando lo solicite.</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>particular que, por defecto, los datos personales no sean accesibles. Tendrá acceso únicamente el personal autorizado, salvo que se modifique en razón de las circunstancias del tratamiento.</p> <p>3. Para el cumplimiento de lo establecido en los numerales 1 y 2, el responsable del tratamiento tendrá en cuenta:</p> <p>a) La protección de los datos personales de forma proactiva y no reactiva.</p> <p>b) La protección de los datos personales preventiva y no correctiva.</p> <p>c) La privacidad como configuración predeterminada.</p> <p>d) La protección de los datos en el ciclo de vida completo de su tratamiento, es decir, desde la recolección hasta su posible supresión.</p> <p>e) La transparencia en el tratamiento de los datos.</p> <p>f) La prevalencia de la privacidad como interés del titular.</p> <p>4. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 60, como elemento que acredite el cumplimiento de las obligaciones establecidas</p>	<p>medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles. Tendrá acceso únicamente el personal autorizado, salvo que se modifique en razón de las circunstancias del tratamiento.</p> <p>3. Para el cumplimiento de lo establecido en los numerales 1 y 2, el responsable del tratamiento tendrá en cuenta:</p> <p>a) La protección de los datos personales de forma proactiva y no reactiva.</p> <p>b) La protección de los datos personales preventiva y no correctiva.</p> <p>c) La privacidad como configuración predeterminada.</p> <p>d) La protección de los datos en el ciclo de vida completo de su tratamiento, es decir, desde la recolección hasta su posible supresión.</p> <p>e) La transparencia en el tratamiento de los datos.</p> <p>f) La prevalencia de la privacidad como interés del titular.</p> <p>4. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 60, como elemento que acredite el cumplimiento de las obligaciones</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p><b>ARTÍCULO 30. Protección de datos desde el diseño y por defecto.</b></p> <p>1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y garantías de las personas naturales, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos de la presente ley y proteger los derechos de los titulares.</p> <p>2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en</p>	<p><b>ARTÍCULO 30. Protección de datos desde el diseño y por defecto.</b></p> <p>1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y garantías de las personas naturales, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos de la presente ley y proteger los derechos de los titulares.</p> <p>2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>en los numerales 1 y 2 del presente artículo.</p> <p><b>ARTÍCULO 31. Corresponsables del tratamiento.</b></p> <p>1. Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo, sus respectivas responsabilidades en el cumplimiento de las obligaciones impuestas por la presente ley, en particular, en el ejercicio de los derechos de los titulares y sus obligaciones de suministro de información, a las cuales se refiere la presente ley.</p> <p>2. El acuerdo indicado en el numeral 1, reflejará adecuadamente las funciones y relaciones respectivas de los corresponsables en relación con los titulares. Se pondrán a disposición del titular los aspectos esenciales del acuerdo.</p> <p>3. Independientemente de los términos del acuerdo a que se refiere el numeral 1, los titulares podrán ejercer los derechos que les reconoce la presente ley frente a cada uno de los responsables.</p> <p><b>ARTÍCULO 32. Encargado del tratamiento.</b></p> <p>1. El encargado del tratamiento no recurrirá a otro encargado sin la autorización, específica o</p>	<p>establecidas en los numerales 1 y 2 del presente artículo.</p> <p><b>ARTÍCULO 31. Corresponsables del tratamiento.</b></p> <p>1. Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo, sus respectivas responsabilidades en el cumplimiento de las obligaciones impuestas por la presente ley, en particular, en el ejercicio de los derechos de los titulares y sus obligaciones de suministro de información, a las cuales se refiere la presente ley.</p> <p>2. El acuerdo indicado en el numeral 1, reflejará adecuadamente las funciones y relaciones respectivas de los corresponsables en relación con los titulares. Se pondrán a disposición del titular los aspectos esenciales del acuerdo.</p> <p>3. Independientemente de los términos del acuerdo a que se refiere el numeral 1, los titulares podrán ejercer los derechos que les reconoce la presente ley frente a cada uno de los responsables.</p> <p><b>ARTÍCULO 32. Encargado del tratamiento.</b></p> <p>1. El encargado del tratamiento no recurrirá a otro encargado sin la autorización, específica o</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>general, del responsable ya sea por escrito o por mensajes de datos suficientes y verificables. Cuando la autorización para el subencargo del tratamiento sea general, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.</p> <p>2. El tratamiento debe regirse por un contrato u otro acto jurídico con arreglo a las leyes civiles o mercantiles, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza, la finalidad del tratamiento, el tipo de titulares, categorías de datos personales, las obligaciones y los derechos del responsable. Dicho contrato estipulará, en particular, que el encargado:</p> <p>a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país u organización internacional, salvo que esté obligado a ello en virtud de un mandato legal que se aplique al</p>	<p>general, del responsable ya sea por escrito o por mensajes de datos suficientes y verificables. Cuando la autorización para el subencargo del tratamiento sea general, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.</p> <p>2. El tratamiento debe regirse por un contrato u otro acto jurídico con arreglo a las leyes civiles o mercantiles, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza, la finalidad del tratamiento, el tipo de titulares, categorías de datos personales, las obligaciones y los derechos del responsable. Dicho contrato estipulará, en particular, que el encargado:</p> <p>a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país u organización internacional, salvo que esté obligado a ello en</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>encargado. En tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que dicho mandato lo prohíba por razones importantes de interés público.</p> <p>b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza contractual.</p> <p>c) Tomará todas las medidas necesarias de conformidad a la presente ley.</p> <p>d) Respetará las condiciones indicadas en la presente ley para recurrir a un subencargado del tratamiento.</p> <p>e) Asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir</p>	<p>virtud de un mandato legal que se aplique al encargado. En tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que dicho mandato lo prohíba por razones importantes de interés público.</p> <p>b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza contractual.</p> <p>c) Tomará todas las medidas necesarias de conformidad a la presente ley.</p> <p>d) Respetará las condiciones indicadas en la presente ley para recurrir a un subencargado del tratamiento.</p> <p>e) Asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los titulares o podrá comprometerse a resolver, por cuenta del responsable y dentro de los plazos establecidos en esta ley, las solicitudes de ejercicio de derechos.</p> <p>f) Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en la presente ley, teniendo en cuenta la naturaleza del tratamiento y la información del encargado.</p> <p>g) A elección del responsable, o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud de una disposición legal o por motivos de responsabilidad derivada de su relación.</p>	<p>técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los titulares o podrá comprometerse a resolver, por cuenta del responsable y dentro de los plazos establecidos en esta ley, las solicitudes de ejercicio de derechos.</p> <p>f) Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en la presente ley, teniendo en cuenta la naturaleza del tratamiento y la información del encargado.</p> <p>g) A elección del responsable, o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento y suprimirá las</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>h) Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.</p> <p>3. El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe la presente ley u otras disposiciones en materia de protección de datos.</p> <p>4. Cuando un encargado del tratamiento recurra a un subencargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este subencargado, las mismas obligaciones de protección de datos que las estipuladas en el contrato entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme</p>	<p>copias existentes a menos que se requiera la conservación de los datos personales en virtud de una disposición legal o por motivos de responsabilidad derivada de su relación.</p> <p>h) Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.</p> <p>3. El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe la presente ley u otras disposiciones en materia de protección de datos.</p> <p>4. Cuando un encargado del tratamiento recurra a un subencargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este subencargado, las mismas obligaciones de protección de datos que las estipuladas en el</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>con las disposiciones de la presente ley. Si el subencargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo que respecta al cumplimiento de las obligaciones del otro.</p> <p>5. La adhesión del encargado y/o subencargado del tratamiento a un código de conducta aprobado o a un mecanismo de certificación aprobado como lo indica esta ley, podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a las que se refiere el presente artículo.</p> <p>6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato que menciona los numerales 2 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales modelo, las cuales hacen alusión a los numerales 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable, encargado o subencargado de conformidad con esta ley.</p> <p>7. La autoridad de protección de datos podrá fijar cláusulas contractuales modelo, para los contratos a los que hacen mención</p>	<p>contrato entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones de la presente ley. Si el subencargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo que respecta al cumplimiento de las obligaciones del otro.</p> <p>5. La adhesión del encargado y/o subencargado del tratamiento a un código de conducta aprobado o a un mecanismo de certificación aprobado como lo indica esta ley, podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a las que se refiere el presente artículo.</p> <p>6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato que menciona los numerales 2 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales modelo, las cuales hacen alusión a los numerales 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable, encargado o subencargado de conformidad con esta ley.</p> <p>7. La autoridad de protección de datos podrá fijar cláusulas contractuales modelo, para los contratos a los que hacen mención los numerales 2 y 4 del presente artículo.</p> <p>8. El contrato al cual se refieren los numerales 2 y 4 deberá constar por escrito, inclusive en formato electrónico.</p>		<p>los numerales 2 y 4 del presente artículo.</p> <p>8. El contrato al cual se refieren los numerales 2 y 4 deberá constar por escrito, inclusive en formato electrónico.</p> <p>9. Sin perjuicio de lo dispuesto en esta ley, si un encargado o subencargado del tratamiento infringe la presente ley, al determinar los fines y medios del tratamiento, será considerado responsable con respecto a dicho tratamiento.</p> <p>10. El responsable del tratamiento podrá exigir a los encargados que sean proveedores de servicios tecnológicos, aplicaciones e infraestructura tecnológica, con los que esté adherido o se vaya a adherir a través de condiciones generales de contratación, que demuestre el cumplimiento de la presente ley. En caso de que el proveedor ignore las solicitudes realizadas por los responsables o incumpla con la presente ley, los responsables podrán denunciar dicha situación ante la autoridad de protección de datos, de conformidad con lo establecido en el artículo 27 de la presente ley.</p> <p>Lo anterior no exonera al responsable del tratamiento del cumplimiento de las obligaciones establecidas</p>	<p>9. Sin perjuicio de lo dispuesto en esta ley, si un encargado o subencargado del tratamiento infringe la presente ley, al determinar los fines y medios del tratamiento, será considerado responsable con respecto a dicho tratamiento.</p> <p>10. El responsable del tratamiento podrá exigir a los encargados que sean proveedores de servicios tecnológicos, aplicaciones e infraestructura tecnológica, con los que esté adherido o se vaya a adherir a través de condiciones generales de contratación, que demuestre el cumplimiento de la presente ley. En caso de que el proveedor ignore las solicitudes realizadas por los responsables o incumpla con la presente ley, los responsables podrán denunciar dicha situación ante la autoridad de protección de datos, de conformidad con lo establecido en el artículo 27 de la presente ley.</p> <p>Lo anterior no exonera al responsable del tratamiento del cumplimiento de las obligaciones establecidas en el artículo 28 de la presente ley.</p> <p><i>Parágrafo primero.</i> Las obligaciones establecidas en esta ley para los encargados del tratamiento serán de aplicación directa para quienes, en atención a lo dispuesto en los numerales 2 y 4 del presente artículo, adquieran la calidad de subencargados.</p> <p><i>Parágrafo segundo.</i> El encargado del tratamiento y cualquier persona que actúe bajo el control del responsable o del encargado y tenga acceso a datos personales, sólo podrán tratar dichos datos siguiendo instrucciones del</p>	
<p>en el artículo 28 de la presente ley.</p> <p><i>Parágrafo primero.</i> Las obligaciones establecidas en esta ley para los encargados del tratamiento serán de aplicación directa para quienes, en atención a lo dispuesto en los numerales 2 y 4 del presente artículo, adquieran la calidad de subencargados.</p> <p><i>Parágrafo segundo.</i> El encargado del tratamiento y cualquier persona que actúe bajo el control del responsable o del encargado y tenga acceso a datos personales, sólo podrán tratar dichos datos siguiendo instrucciones del responsable, a menos que no estén obligados a ello en virtud de una disposición legal.</p> <p><b>ARTÍCULO 33. Registro de las actividades de tratamiento.</b></p> <p>1. Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su control. Dicho registro deberá contener toda la información indicada a continuación:</p> <p>a) El nombre y los datos de contacto del responsable y, cuando sea el caso, del corresponsable, y del oficial de protección de datos o área encargada.</p> <p>b) Los fines del tratamiento.</p> <p>c) Una descripción de los tipos de titulares y de las categorías de datos personales.</p>	<p>responsable, a menos que no estén obligados a ello en virtud de una disposición legal.</p> <p><b>ARTÍCULO 33. Registro de las actividades de tratamiento.</b></p> <p>1. Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su control. Dicho registro deberá contener toda la información indicada a continuación:</p> <p>a) El nombre y los datos de contacto del responsable y, cuando sea el caso, del corresponsable, y del oficial de protección de datos o área encargada.</p> <p>b) Los fines del tratamiento.</p> <p>c) Una descripción de los tipos de titulares y de las categorías de datos personales.</p>	SIN MODIFICACIONES	<p>d) Los destinatarios a quienes se cedieron o cederán los datos personales, incluidos los destinatarios en otros países u organizaciones internacionales.</p> <p>e) Los encargados que intervienen en el tratamiento.</p> <p>f) De ser procedente, las transferencias de datos personales a otro país o una organización internacional, incluida la identificación de dicho país u organización internacional y, en el caso de las transferencias indicadas en el artículo 33 de la presente esta ley relativa a la documentación de garantías adecuadas.</p> <p>g) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.</p> <p>h) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la</p>	<p>d) Los destinatarios a quienes se cedieron o cederán los datos personales, incluidos los destinatarios en otros países u organizaciones internacionales.</p> <p>e) Los encargados que intervienen en el tratamiento.</p> <p>f) De ser procedente, las transferencias de datos personales a otro país o una organización internacional, incluida la identificación de dicho país u organización internacional y, en el caso de las transferencias indicadas en el artículo 33 de la presente esta ley relativa a la documentación de garantías adecuadas.</p> <p>g) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.</p> <p>h) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>remisión al documento que las contenga.</p> <p>i) Los responsables del tratamiento, deben inscribir sus registros de actividades ante el Registro Nacional de las Actividades, administrado por la autoridad de protección de datos y de libre consulta para los ciudadanos.</p> <p>2. Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:</p> <p>a) El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y del oficial de protección de datos o área encargada.</p> <p>b) Las categorías de tratamientos efectuados por cuenta de cada responsable.</p> <p>c) Los subencargados autorizados por el responsable, que intervienen en el tratamiento.</p> <p>d) De ser procedente, las transferencias de datos personales a otro país u organización</p>	<p>remisión al documento que las contenga.</p> <p>i) Los responsables del tratamiento, deben inscribir sus registros de actividades ante el Registro Nacional de las Actividades, administrado por la autoridad de protección de datos y de libre consulta para los ciudadanos.</p> <p>2. Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:</p> <p>a) El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y del oficial de protección de datos o área encargada.</p> <p>b) Las categorías de tratamientos efectuados por cuenta de cada responsable.</p> <p>c) Los subencargados autorizados por el responsable, que intervienen en el tratamiento.</p> <p>d) De ser procedente, las transferencias de datos personales a otro país u organización internacional y en el caso de las transferencias indicadas en esta ley, relativo a la</p>		<p>internacional, incluida la identificación de dicho país u organización internacional y en el caso de las transferencias indicadas en esta ley, relativo a la documentación de garantías adecuadas.</p> <p>e) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la remisión al documento que las contenga.</p> <p>3. Los registros a los que se refieren los numerales 1 y 2 constarán por escrito, inclusive en formato electrónico.</p> <p>4. El responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de protección de datos, cuando lo requiera.</p> <p>5. Los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas, harán público el registro de sus actividades de tratamiento</p>	<p>documentación de garantías adecuadas.</p> <p>e) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la remisión al documento que las contenga.</p> <p>3. Los registros a los que se refieren los numerales 1 y 2 constarán por escrito, inclusive en formato electrónico.</p> <p>4. El responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de protección de datos, cuando lo requiera.</p> <p>5. Los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas, harán público el registro de sus actividades de tratamiento accesible por medios electrónicos, en el que constará la información establecida en el presente artículo.</p>	
<p>accesible por medios electrónicos, en el que constará la información establecida en el presente artículo.</p> <p><b>ARTÍCULO 34. Bloqueo de los datos.</b></p> <p>1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.</p> <p>2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los Jueces y Tribunales, Fiscalía General de la Nación o las Administraciones Públicas competentes, en particular de la autoridad de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo, se procederá a la destrucción de los datos.</p> <p>3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.</p> <p>4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se</p>	<p><b>ARTÍCULO 34. Bloqueo de los datos.</b></p> <p>1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.</p> <p>2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los Jueces y Tribunales, Fiscalía General de la Nación o las Administraciones Públicas competentes, en particular de la autoridad de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo, se procederá a la destrucción de los datos.</p> <p>3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.</p> <p>4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que</p>	SIN MODIFICACIONES	<p>procederá a un copiado seguro de la información, de manera que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.</p> <p>5. La autoridad de protección de datos, dentro del ámbito de sus competencias, podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de titulares afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los titulares, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.</p> <p><b>ARTÍCULO 35. Seguridad del tratamiento.</b></p> <p>1. Teniendo en cuenta el estado de la técnica, los costos de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad, variables para los derechos y garantías de los titulares, el responsable y el</p>	<p>implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información, de manera que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.</p> <p>5. La autoridad de protección de datos, dentro del ámbito de sus competencias, podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de titulares afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los titulares, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.</p> <p><b>ARTÍCULO 35. Seguridad del tratamiento.</b></p> <p>1. Teniendo en cuenta el estado de la técnica, los costos de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad, variables para los derechos y garantías de los titulares, el responsable</p>	SIN MODIFICACIONES





Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>de datos, verificar el cumplimiento de lo dispuesto en el presente artículo.</p> <p>6. Los datos personales contenidos en la notificación de un incidente de seguridad y que fueron comunicados a la autoridad de protección de datos, proveedores de tecnologías y servicios de seguridad, podrán ser tratados exclusivamente durante el tiempo y alcance necesario para su análisis, detección, protección y respuesta ante el incidente, adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.</p>	<p>6. Los datos personales contenidos en la notificación de un incidente de seguridad y que fueron comunicados a la autoridad de protección de datos, proveedores de tecnologías y servicios de seguridad, podrán ser tratados exclusivamente durante el tiempo y alcance necesario para su análisis, detección, protección y respuesta ante el incidente, adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.</p>	
<p><b>ARTÍCULO 37. Comunicación de un incidente de seguridad de los datos personales al titular.</b></p> <p>1. Cuando sea probable que el incidente de seguridad de los datos personales entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento lo comunicará al titular sin demora injustificada.</p> <p>2. La comunicación al titular contemplada en el numeral 1 del presente artículo, deberá describir en un lenguaje claro y sencillo la naturaleza del incidente de seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 36, numeral 3, literales b), c) y d).</p>	<p><b>ARTÍCULO 37. Comunicación de un incidente de seguridad de los datos personales al titular.</b></p> <p>1. Cuando sea probable que el incidente de seguridad de los datos personales entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento lo comunicará al titular sin demora injustificada.</p> <p>2. La comunicación al titular contemplada en el numeral 1 del presente artículo, deberá describir en un lenguaje claro y sencillo la naturaleza del incidente de seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 36, numeral 3, literales b), c) y d).</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>3. La comunicación al titular a la que se refiere el numeral 1, no será necesaria si se cumple alguna de las siguientes condiciones:</p> <p>a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por el incidente de seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.</p> <p>b) El responsable del tratamiento ha tomado medidas posteriores que garanticen que ya no exista la probabilidad de que se materialice el alto riesgo para los derechos y garantías del titular.</p> <p>4. Cuando la comunicación a los titulares suponga un esfuerzo desproporcionado para el responsable del tratamiento, éste podrá optar por una comunicación pública o una medida de difusión semejante, de manera que</p>	<p>3. La comunicación al titular a la que se refiere el numeral 1, no será necesaria si se cumple alguna de las siguientes condiciones:</p> <p>a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por el incidente de seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.</p> <p>b) El responsable del tratamiento ha tomado medidas posteriores que garanticen que ya no exista la probabilidad de que se materialice el alto riesgo para los derechos y garantías del titular.</p> <p>4. Cuando la comunicación a los titulares suponga un esfuerzo desproporcionado para el responsable del tratamiento, éste podrá optar por una comunicación pública o una medida de difusión semejante, de manera que se informe efectivamente a los titulares.</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>se informe efectivamente a los titulares.</p> <p>5. Cuando el responsable no haya comunicado al titular el incidente de seguridad de los datos personales, la autoridad de protección de datos, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo comunique o podrá confirmar que se cumple alguna de las condiciones mencionadas en el numeral 3.</p>	<p>5. Cuando el responsable no haya comunicado al titular el incidente de seguridad de los datos personales, la autoridad de protección de datos, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo comunique o podrá confirmar que se cumple alguna de las condiciones mencionadas en el numeral 3.</p>	
<p><b>ARTÍCULO 38. Evaluación de impacto relativa a la protección de datos y consulta previa.</b></p> <p>1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.</p> <p>2. El responsable del tratamiento solicitará asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.</p>	<p><b>ARTÍCULO 38. Evaluación de impacto relativa a la protección de datos y consulta previa.</b></p> <p>1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.</p> <p>2. El responsable del tratamiento solicitará asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>3. La evaluación de impacto relativa a la protección de los datos, a los que se refiere el numeral 1, se requerirá en especial cuando:</p> <p>a) Se realice evaluación sistemática y exhaustiva de aspectos personales de personas naturales, que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que les afecten significativamente de forma similar.</p> <p>b) Tratamiento a gran escala de datos sensibles o de los datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.</p> <p>c) Observación sistemática a gran escala de una zona de acceso público.</p> <p>d) Se efectúen tratamientos sobre neurodatos.</p> <p>4. La autoridad de protección de datos establecerá y publicará una lista de los tipos de operaciones de tratamiento, que requieran una evaluación de impacto</p>	<p>3. La evaluación de impacto relativa a la protección de los datos, a los que se refiere el numeral 1, se requerirá en especial cuando:</p> <p>a) Se realice evaluación sistemática y exhaustiva de aspectos personales de personas naturales, que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que les afecten significativamente de forma similar.</p> <p>b) Tratamiento a gran escala de datos sensibles o de los datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.</p> <p>c) Observación sistemática a gran escala de una zona de acceso público.</p> <p>d) Se efectúen tratamientos sobre neurodatos.</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>relativa a la protección de datos de conformidad con el numeral 1.</p> <p>5. La evaluación a la que se refiere el numeral 1 del presente artículo, deberá incluir como mínimo:</p> <p>a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.</p> <p>b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.</p> <p>c) Una evaluación de los riesgos para los derechos y garantías de los titulares a los que se refiere el numeral 1.</p> <p>d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente ley, teniendo en cuenta los derechos y</p>	<p>4. La autoridad de protección de datos establecerá y publicará una lista de los tipos de operaciones de tratamiento, que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el numeral 1.</p> <p>5. La evaluación a la que se refiere el numeral 1 del presente artículo, deberá incluir como mínimo:</p> <p>a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.</p> <p>b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.</p> <p>c) Una evaluación de los riesgos para los derechos y garantías de los titulares a los que se refiere el numeral 1.</p> <p>d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente ley, teniendo en cuenta los derechos y de otras personas afectadas.</p> <p>6. El cumplimiento de los códigos de conducta aprobados, a los que se refiere el artículo 38, por los responsables o encargados correspondientes se tendrá</p>		<p>garantías de los titulares y de otras personas afectadas.</p> <p>6. El cumplimiento de los códigos de conducta aprobados, a los que se refiere el artículo 38, por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.</p> <p>7. Cuando el tratamiento de datos se base en un deber legal o en un interés público y esté regulado por una ley o normativa específica aplicable al responsable del tratamiento, que detalle la operación específica de tratamiento o conjunto de operaciones, y que ya incluya una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general, los numerales 1 a 6 no se aplicarán, a menos que una ley o normativa posterior lo requiera.</p> <p>8. En caso de ser necesario, el responsable examinará si el tratamiento es conforme a la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.</p> <p>7. Cuando el tratamiento de datos se base en un deber legal o en un interés público y esté regulado por una ley o normativa específica aplicable al responsable del tratamiento, que detalle la operación específica de tratamiento o conjunto de operaciones, y que ya incluya una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general, los numerales 1 a 6 no se aplicarán, a menos que una ley o normativa posterior lo requiera.</p> <p>8. En caso de ser necesario, el responsable examinará si el tratamiento es conforme a la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.</p> <p>9. El responsable del tratamiento consultará previamente a la autoridad de protección de datos antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. Si la autoridad de protección de datos considera que el tratamiento previsto supone un alto riesgo, asesorará por escrito al responsable, y en su caso al encargado, sobre las medidas técnicas y organizativas que se deberán adoptar antes del tratamiento de los datos. La</p>	<p>debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.</p> <p>7. Cuando el tratamiento de datos se base en un deber legal o en un interés público y esté regulado por una ley o normativa específica aplicable al responsable del tratamiento, que detalle la operación específica de tratamiento o conjunto de operaciones, y que ya incluya una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general, los numerales 1 a 6 no se aplicarán, a menos que una ley o normativa posterior lo requiera.</p> <p>8. En caso de ser necesario, el responsable examinará si el tratamiento es conforme a la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.</p> <p>9. El responsable del tratamiento consultará previamente a la autoridad de protección de datos antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. Si la autoridad de protección de datos considera que el tratamiento previsto supone un alto riesgo, asesorará por escrito al responsable, y en su caso al encargado, sobre las medidas técnicas y organizativas que se deberán adoptar antes del tratamiento de los datos. La</p>	
<p>9. El responsable del tratamiento consultará previamente a la autoridad de protección de datos antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. Si la autoridad de protección de datos considera que el tratamiento previsto supone un alto riesgo, asesorará por escrito al responsable, y en su caso al encargado, sobre las medidas técnicas y organizativas que se deberán adoptar antes del tratamiento de los datos. La autoridad de protección de datos deberá emitir un concepto en el menor tiempo posible.</p> <p><i>Parágrafo:</i> La zona de acceso público a la que se refiere el numeral 3 literal c) del presente artículo, hace referencia a cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas naturales, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad.</p>	<p>autoridad de protección de datos deberá emitir un concepto en el menor tiempo posible.</p> <p><i>Parágrafo:</i> La zona de acceso público a la que se refiere el numeral 3 literal c) del presente artículo, hace referencia a cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas naturales, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad.</p>		<p>a) El tratamiento lo lleve a cabo los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas.</p> <p>b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de los titulares a gran escala.</p> <p>c) Las actividades principales del responsable o del encargado, consistan en el tratamiento a gran escala de datos sensibles y de datos relativos a antecedentes penales, anotaciones judiciales o contravencionales,</p>	<p>a) El tratamiento lo lleve a cabo los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas.</p> <p>b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de los titulares a gran escala.</p> <p>c) Las actividades principales del responsable o del encargado, consistan en el tratamiento a gran escala de datos sensibles y de datos relativos a antecedentes penales, anotaciones</p>	
<p><b>ARTÍCULO 39. Designación del Oficial de protección de datos.</b></p> <p>1. El responsable y el encargado del tratamiento designarán un oficial de protección de datos siempre que:</p>	<p><b>ARTÍCULO 39. Designación del Oficial de protección de datos.</b></p> <p>1. El responsable y el encargado del tratamiento designarán un oficial de protección de datos siempre que:</p>	SIN MODIFICACIONES			

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>y/o sanciones administrativas.</p> <p>d) La autoridad de protección de datos podrá definir nuevas indicaciones en las que se deba designar un Oficial de protección de datos y estipulará las condiciones y particularidades para dicha designación.</p> <p>2. Un grupo empresarial podrá nombrar un único oficial de protección de datos, siempre que sea fácilmente accesible desde cada una de las empresas que pertenecen al grupo.</p> <p>3. Cuando el responsable o el encargado del tratamiento sea una entidad u organismo público, se podrá designar un único oficial de protección de datos para varias de estas entidades u organismos, teniendo en cuenta su estructura administrativa y tamaño.</p> <p>4. En casos distintos de los contemplados en el numeral 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a sectores a los que pertenezcan los responsables o encargados, podrán designar de forma voluntaria un oficial de protección de datos.</p> <p>5. El oficial de protección de datos será designado siempre que cuente con un</p>	<p>judiciales o contravencionales, y/o sanciones administrativas.</p> <p>d) La autoridad de protección de datos podrá definir nuevas indicaciones en las que se deba designar un Oficial de protección de datos y estipulará las condiciones y particularidades para dicha designación.</p> <p>2. Un grupo empresarial podrá nombrar un único oficial de protección de datos, siempre que sea fácilmente accesible desde cada una de las empresas que pertenecen al grupo.</p> <p>3. Cuando el responsable o el encargado del tratamiento sea una entidad u organismo público, se podrá designar un único oficial de protección de datos para varias de estas entidades u organismos, teniendo en cuenta su estructura administrativa y tamaño.</p> <p>4. En casos distintos de los contemplados en el numeral 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a sectores a los que pertenezcan los responsables o encargados, podrán designar de forma voluntaria un oficial de protección de datos.</p> <p>5. El oficial de protección de datos será designado siempre que cuente con un perfil interdisciplinario con conocimientos legales y experiencia en protección de datos. Además, se verificará su</p>		<p>perfil legal o un perfil interdisciplinario con conocimientos legales y experiencia en protección de datos. Además, se verificará su capacidad para desempeñar las funciones indicadas en esta ley.</p> <p>6. El oficial de protección de datos podrá vincularse con el responsable o el encargado del tratamiento por medio de un contrato de prestación de servicios o un contrato laboral.</p> <p>7. El responsable o el encargado del tratamiento publicará los datos de contacto del oficial de protección de datos y los comunicará a la autoridad de protección de datos en un plazo de quince (15) días hábiles.</p> <p>Las designaciones, nombramientos y ceses de los oficiales de protección de datos, tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria, también deberán ser notificadas en el mismo término.</p> <p>8. La autoridad de protección de datos, mantendrá en el ámbito de sus competencias, una lista actualizada de oficiales de protección de datos que será accesible a través de medios electrónicos.</p> <p>9. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento, podrán establecer la dedicación</p>	<p>capacidad para desempeñar las funciones indicadas en esta ley.</p> <p>6. El oficial de protección de datos podrá vincularse con el responsable o el encargado del tratamiento por medio de un contrato de prestación de servicios o un contrato laboral.</p> <p>7. El responsable o el encargado del tratamiento publicará los datos de contacto del oficial de protección de datos y los comunicará a la autoridad de protección de datos en un plazo de quince (15) días hábiles.</p> <p>Las designaciones, nombramientos y ceses de los oficiales de protección de datos, tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria, también deberán ser notificadas en el mismo término.</p> <p>8. La autoridad de protección de datos, mantendrá en el ámbito de sus competencias, una lista actualizada de oficiales de protección de datos que será accesible a través de medios electrónicos.</p> <p>9. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento, podrán establecer la dedicación</p>	
<p>completa o a tiempo parcial del oficial, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos y garantías de los titulares.</p> <p><b>ARTÍCULO 40. Posición del oficial de protección de datos.</b></p> <p>1. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relacionadas con la protección de datos personales.</p> <p>2. El responsable y el encargado del tratamiento respaldarán al oficial de protección de datos en el desempeño de las funciones estipuladas en la presente ley, facilitando los recursos necesarios para el desempeño de dichas funciones, el acceso a los datos personales y a las operaciones de tratamiento.</p> <p>3. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurrieren en dolo o negligencia grave en su ejercicio. El oficial de</p>	<p><b>ARTÍCULO 40. Posición del oficial de protección de datos.</b></p> <p>1. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relacionadas con la protección de datos personales.</p> <p>2. El responsable y el encargado del tratamiento respaldarán al oficial de protección de datos en el desempeño de las funciones estipuladas en la presente ley, facilitando los recursos necesarios para el desempeño de dichas funciones, el acceso a los datos personales y a las operaciones de tratamiento.</p> <p>3. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurrieren en dolo o negligencia grave en su</p>	SIN MODIFICACIONES	<p>protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.</p> <p>4. Los titulares podrán ponerse en contacto con el oficial de protección de datos, en relación a todas las cuestiones correspondientes al tratamiento de sus datos personales y al ejercicio de sus derechos y garantías al amparo de la presente ley.</p> <p>5. El oficial de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el artículo 74 de la Constitución Política.</p> <p>6. El oficial de protección de datos podrá desempeñar otras funciones y el responsable o encargado del tratamiento garantizará que estas no den lugar a conflicto de intereses.</p> <p>7. El oficial de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la autoridad de protección de datos. El oficial podrá verificar los procedimientos y emitir recomendaciones en el ámbito de sus competencias.</p> <p><b>ARTÍCULO 41. Funciones del oficial de protección de datos.</b></p>	<p>ejercicio. El oficial de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.</p> <p>4. Los titulares podrán ponerse en contacto con el oficial de protección de datos, en relación a todas las cuestiones correspondientes al tratamiento de sus datos personales y al ejercicio de sus derechos y garantías al amparo de la presente ley.</p> <p>5. El oficial de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el artículo 74 de la Constitución Política.</p> <p>6. El oficial de protección de datos podrá desempeñar otras funciones y el responsable o encargado del tratamiento garantizará que estas no den lugar a conflicto de intereses.</p> <p>7. El oficial de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la autoridad de protección de datos. El oficial podrá verificar los procedimientos y emitir recomendaciones en el ámbito de sus competencias.</p> <p><b>ARTÍCULO 41. Funciones del oficial de protección de datos.</b></p> <p>1. El oficial de protección de datos tendrá como</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>1. El oficial de protección de datos tendrá como mínimo las siguientes funciones:</p> <p>a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones que les competen en virtud de la ley y otras disposiciones referentes a la protección de datos.</p> <p>b) Supervisar el cumplimiento de lo dispuesto en la presente ley.</p> <p>c) Supervisar la implementación y aplicación de un manual interno de políticas y procedimiento en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.</p> <p>d) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto, relativa a la protección de datos y supervisar su aplicación de</p>	<p>mínimo las siguientes funciones:</p> <p>a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones que les competen en virtud de la ley y otras disposiciones referentes a la protección de datos.</p> <p>b) Supervisar el cumplimiento de lo dispuesto en la presente ley.</p> <p>c) Supervisar la implementación y aplicación de un manual interno de políticas y procedimiento en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.</p> <p>d) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto, relativa a la protección de datos y supervisar su aplicación de</p>	
<p>conformidad con la presente ley.</p> <p>e) Cooperar con la autoridad de protección de datos.</p> <p>f) Actuar como punto de contacto de la autoridad de protección de datos, sobre cuestiones relativas al tratamiento, incluida la consulta previa a la que se refiere el artículo 38, numeral 9, así como solicitar instrucciones, en su caso, sobre cualquier otro asunto.</p> <p>g) Cuando el oficial de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos, lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.</p> <p>2. El oficial de protección de datos, desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el</p>	<p>conformidad con la presente ley.</p> <p>e) Cooperar con la autoridad de protección de datos.</p> <p>f) Actuar como punto de contacto de la autoridad de protección de datos, sobre cuestiones relativas al tratamiento, incluida la consulta previa a la que se refiere el artículo 38, numeral 9, así como solicitar instrucciones, en su caso, sobre cualquier otro asunto.</p> <p>g) Cuando el oficial de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos, lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.</p> <p>2. El oficial de protección de datos, desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.</p>	
<p>alcance, el contexto y fines del tratamiento.</p> <p><b>ARTÍCULO 44. Códigos de conducta.</b></p> <p>1. La Autoridad de protección de datos, promoverá la elaboración de códigos de conducta, destinados a contribuir a la correcta aplicación de la presente ley, teniendo en cuenta las características específicas de las distintas actividades de tratamiento y las necesidades específicas de las microempresas, las pequeñas y medianas empresas.</p> <p>2. Las asociaciones y otras entidades representativas de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta, modificar o ampliar dichos códigos con objeto de especificar la aplicación de la presente ley, en lo que respecta a:</p> <p>a) El tratamiento leal y transparente.</p> <p>b) Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos.</p> <p>c) La recogida de datos personales.</p> <p>d) La seudonimización de datos personales.</p> <p>e) La información proporcionada al público y a los titulares.</p>	<p><b>ARTÍCULO 424. Códigos de conducta.</b></p> <p>1. La Autoridad de protección de datos, promoverá la elaboración de códigos de conducta, destinados a contribuir a la correcta aplicación de la presente ley, teniendo en cuenta las características específicas de las distintas actividades de tratamiento y las necesidades específicas de las microempresas, las pequeñas y medianas empresas.</p> <p>2. Las asociaciones y otras entidades representativas de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta, modificar o ampliar dichos códigos con objeto de especificar la aplicación de la presente ley, en lo que respecta a:</p> <p>a) El tratamiento leal y transparente.</p> <p>b) Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos.</p> <p>c) La recogida de datos personales.</p> <p>d) La seudonimización de datos personales.</p> <p>e) La información proporcionada al público y a los titulares.</p>	<p>Se ajusta la numeración</p>
<p>f) El ejercicio de los derechos de los titulares.</p> <p>g) La información proporcionada a los menores y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o representantes legales del menor.</p> <p>h) Las medidas, procedimientos y las acciones para garantizar la seguridad del tratamiento contenidas en esta ley.</p> <p>i) La notificación de incidentes de seguridad de los datos personales a la autoridad de protección de datos y la comunicación de dichos incidentes a los titulares.</p> <p>j) La transferencia de datos personales a terceros países u organizaciones internacionales.</p> <p>k) Los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos, que permitan resolver las controversias entre los responsables y los titulares relativos al</p>	<p>f) El ejercicio de los derechos de los titulares.</p> <p>g) La información proporcionada a los menores y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o representantes legales del menor.</p> <p>h) Las medidas, procedimientos y las acciones para garantizar la seguridad del tratamiento contenidas en esta ley.</p> <p>i) La notificación de incidentes de seguridad de los datos personales a la autoridad de protección de datos y la comunicación de dichos incidentes a los titulares.</p> <p>j) La transferencia de datos personales a terceros países u organizaciones internacionales.</p> <p>k) Los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos, que permitan resolver las controversias entre los responsables y los</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>tratamiento, sin perjuicio del derecho presentar una queja ante la autoridad de protección de datos o acudir ante autoridad judicial.</p> <p>3. Los responsables o encargados del tratamiento a los que se aplica la presente ley, así como también, a los que no se aplica, podrán adherirse también a códigos de conducta aprobados de conformidad con el numeral 5 del presente artículo, con el fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales.</p> <p>Los mencionados responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas las relativas a los derechos de los titulares.</p> <p>4. El código de conducta, contendrá mecanismos que permitan a la entidad supervisora, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados del tratamiento, que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de la autoridad de protección de datos.</p>	<p>titulares relativos al tratamiento, sin perjuicio del derecho presentar una queja ante la autoridad de protección de datos o acudir ante autoridad judicial.</p> <p>3. Los responsables o encargados del tratamiento a los que se aplica la presente ley, así como también, a los que no se aplica, podrán adherirse también a códigos de conducta aprobados de conformidad con el numeral 5 del presente artículo, con el fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales. Los mencionados responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas las relativas a los derechos de los titulares.</p> <p>4. El código de conducta, contendrá mecanismos que permitan a la entidad supervisora, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados del tratamiento, que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de la autoridad de protección de datos.</p> <p>5. Las asociaciones y otras entidades mencionadas en el numeral 2 del presente artículo, que pretendan elaborar un código de conducta, modificar o ampliar un código existente presentarán el proyecto de código, la modificación o ampliación a la autoridad de protección de datos.</p>	
<p>5. Las asociaciones y otras entidades mencionadas en el numeral 2 del presente artículo, que pretendan elaborar un código de conducta, modificar o ampliar un código existente presentarán el proyecto de código, la modificación o ampliación a la autoridad de protección de datos.</p> <p>La autoridad de protección de datos determinará si el proyecto de código, la modificación o ampliación es conforme con la presente ley y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.</p> <p>6. Si el proyecto de código, la modificación o ampliación es aprobado de conformidad con el numeral 5, la autoridad de protección de datos el código.</p> <p>7. La autoridad de protección de datos llevará un registro de todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.</p>	<p>La autoridad de protección de datos determinará si el proyecto de código, la modificación o ampliación es conforme con la presente ley y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.</p> <p>6. Si el proyecto de código, la modificación o ampliación es aprobado de conformidad con el numeral 5, la autoridad de protección de datos el código.</p> <p>7. La autoridad de protección de datos llevará un registro de todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.</p>	
<p><b>ARTÍCULO 43. Supervisión de códigos de conducta aprobados.</b></p> <p>1. Podrá supervisar el cumplimiento de un código de conducta, una entidad que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditada para tal fin por la autoridad de protección de datos, sin perjuicio de las</p>	<p><b>ARTÍCULO 43. Supervisión de códigos de conducta aprobados.</b></p> <p>1. Podrá supervisar el cumplimiento de un código de conducta, una entidad que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditada para tal fin por la autoridad de protección de datos, sin perjuicio de</p>	SIN MODIFICACIONES
Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>funciones y facultades de esta.</p> <p>2. La autoridad de protección de datos fijará los criterios de acreditación de las entidades a las que se refiere el presente artículo.</p> <p>3. Sin perjuicio de las funciones y las facultades de la autoridad de protección de datos, en virtud del numeral 1 del presente artículo, la entidad acreditada deberá, con sujeción a las garantías del debido proceso, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y sus razones, a la autoridad de protección de datos.</p> <p>4. La autoridad de protección de datos podrá revocar la acreditación de una entidad de conformidad con el numeral 1, si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicha entidad infringe la presente ley.</p> <p>5. El presente artículo no se aplicará al tratamiento realizado por autoridades y entidades públicas.</p>	<p>las funciones y facultades de esta.</p> <p>2. La autoridad de protección de datos fijará los criterios de acreditación de las entidades a las que se refiere el presente artículo.</p> <p>3. Sin perjuicio de las funciones y las facultades de la autoridad de protección de datos, en virtud del numeral 1 del presente artículo, la entidad acreditada deberá, con sujeción a las garantías del debido proceso, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y sus razones, a la autoridad de protección de datos.</p> <p>4. La autoridad de protección de datos podrá revocar la acreditación de una entidad de conformidad con el numeral 1, si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicha entidad infringe la presente ley.</p> <p>5. El presente artículo no se aplicará al tratamiento realizado por autoridades y entidades públicas.</p>	
<p><b>ARTÍCULO 44. Deberes de las entidades supervisoras de códigos de conducta.</b></p> <p>Las entidades supervisoras de códigos de conducta deberán</p>	<p><b>ARTÍCULO 44. Deberes de las entidades supervisoras de códigos de conducta.</b></p> <p>Las entidades supervisoras de códigos de conducta deberán</p>	SIN MODIFICACIONES
Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>1. Demostrar, a satisfacción de la autoridad de protección de datos, su independencia y pericia en relación con el objeto del código.</p> <p>2. Establecer procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación.</p> <p>3. Establecer procedimientos y estructuras para tratar los reclamos relativos a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, para hacer que estos sean transparentes para los titulares y el público en general.</p> <p>4. Demostrar, a satisfacción de la autoridad de protección de datos, que sus funciones y objetivos no dan lugar a conflicto de intereses.</p>	<p>cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>1. Demostrar, a satisfacción de la autoridad de protección de datos, su independencia y pericia en relación con el objeto del código.</p> <p>2. Establecer procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación.</p> <p>3. Establecer procedimientos y estructuras para tratar los reclamos relativos a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, para hacer que estos sean transparentes para los titulares y el público en general.</p> <p>4. Demostrar, a satisfacción de la autoridad de protección de datos, que sus funciones y objetivos no dan lugar a conflicto de intereses.</p>	
<p><b>ARTÍCULO 45. Certificación.</b></p> <p>1. La Autoridad de protección de datos promoverá, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de</p>	<p><b>ARTÍCULO 45. Certificación.</b></p> <p>1. La Autoridad de protección de datos promoverá, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de</p>	SIN MODIFICACIONES



Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>protección de datos a fin de demostrar el cumplimiento de lo dispuesto en la presente ley, en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas, las pequeñas y medianas empresas.</p> <p>2. Podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados conforme al numeral 5 del presente artículo, con el objetivo de demostrar que los responsables o encargados no sujetos a la presente ley, según lo establecido en el artículo 3, ofrecen garantías adecuadas en el contexto de transferencias internacionales de datos personales a terceros países u organizaciones internacionales, según lo dispuesto en el artículo 49, numeral 2, literal e). Los responsables o encargados mencionados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas aquellas relativas a los derechos de los titulares.</p> <p>3. La certificación será voluntaria y estará disponible a través de un proceso transparente.</p> <p>4. La certificación a la que se refiere el presente artículo, no limitará las obligaciones</p>	<p>protección de datos a fin de demostrar el cumplimiento de lo dispuesto en la presente ley, en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas, las pequeñas y medianas empresas.</p> <p>2. Podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados conforme al numeral 5 del presente artículo, con el objetivo de demostrar que los responsables o encargados no sujetos a la presente ley, según lo establecido en el artículo 3, ofrecen garantías adecuadas en el contexto de transferencias internacionales de datos personales a terceros países u organizaciones internacionales, según lo dispuesto en el artículo 49, numeral 2, literal e). Los responsables o encargados mencionados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas aquellas relativas a los derechos de los titulares.</p> <p>3. La certificación será voluntaria y estará disponible a través de un proceso transparente.</p> <p>4. La certificación a la que se refiere el presente artículo,</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>del responsable o encargado del tratamiento en cuanto al cumplimiento de la presente ley y se entenderá sin perjuicio de las funciones y las facultades de la autoridad de protección de datos.</p> <p>5. La certificación en virtud del presente artículo será expedida por las entidades de certificación o por la autoridad de protección de datos, sobre la base de los criterios aprobados por ésta.</p> <p>6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación, darán a la entidad de certificación o en su caso a la autoridad de protección de datos, toda la información y acceso a sus actividades de tratamiento que requieran para llevar a cabo el procedimiento de certificación.</p> <p>7. La certificación se expedirá a un responsable o encargado del tratamiento por un periodo máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por las entidades de certificación, o en su caso por la autoridad de protección de datos, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la misma.</p>	<p>no limitará las obligaciones del responsable o encargado del tratamiento en cuanto al cumplimiento de la presente ley y se entenderá sin perjuicio de las funciones y las facultades de la autoridad de protección de datos.</p> <p>5. La certificación en virtud del presente artículo será expedida por las entidades de certificación o por la autoridad de protección de datos, sobre la base de los criterios aprobados por ésta.</p> <p>6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación, darán a la entidad de certificación o en su caso a la autoridad de protección de datos, toda la información y acceso a sus actividades de tratamiento que requieran para llevar a cabo el procedimiento de certificación.</p> <p>7. La certificación se expedirá a un responsable o encargado del tratamiento por un periodo máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por las entidades de certificación, o en su caso por la autoridad de protección de datos, cuando no se cumplan o se hayan dejado de cumplir</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>8. La autoridad de protección de datos llevará en un registro todos los mecanismos de certificación, sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.</p> <p><i>Parágrafo primero:</i> Serán entidades certificadoras aquellas que hayan sido acreditadas por un organismo del subsistema nacional de calidad, el cual tenga la pericia necesaria para evaluar si los aspirantes a entidades certificadoras cuentan con un nivel adecuado de competencia en materia de protección de datos.</p> <p><i>Parágrafo segundo:</i> La autoridad de protección de datos hará públicos los requisitos y los criterios a los que se refiere el numeral 5 del presente artículo, en una forma fácilmente accesible.</p>	<p>los requisitos para la misma.</p> <p>8. La autoridad de protección de datos llevará en un registro todos los mecanismos de certificación, sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.</p> <p><i>Parágrafo primero:</i> Serán entidades certificadoras aquellas que hayan sido acreditadas por un organismo del subsistema nacional de calidad, el cual tenga la pericia necesaria para evaluar si los aspirantes a entidades certificadoras cuentan con un nivel adecuado de competencia en materia de protección de datos.</p> <p><i>Parágrafo segundo:</i> La autoridad de protección de datos hará públicos los requisitos y los criterios a los que se refiere el numeral 5 del presente artículo, en una forma fácilmente accesible.</p>	
<p><b>ARTÍCULO 46. Deberes de las entidades certificadoras.</b></p> <p>Las entidades certificadoras deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>1. Demostrar ante la autoridad de protección de datos y/o los sujetos interesados en la certificación que se encuentran acreditadas por un organismo del</p>	<p><b>ARTÍCULO 46. Deberes de las entidades certificadoras.</b></p> <p>Las entidades certificadoras deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>1. Demostrar ante la autoridad de protección de datos y/o los sujetos interesados en la certificación que se encuentran acreditadas por un organismo del</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>subsistema nacional de calidad.</p> <p>2. Respetar y cumplir los criterios de certificación aprobados por la autoridad de protección de datos.</p> <p>3. Establecer procedimientos para la expedición, revisión periódica y retirada de certificaciones, sellos y marcas de protección de datos en los términos descritos en el numeral 7 del artículo 45.</p> <p>4. Establecer procedimientos y estructuras para tratar los reclamos relativos al retiro de la certificación por el incumplimiento de los requisitos por parte de un responsable o encargado del tratamiento.</p> <p>5. Informar a la autoridad de protección de datos sobre las razones para la retirada de una certificación a un responsable o encargado del tratamiento.</p>	<p>subsistema nacional de calidad.</p> <p>2. Respetar y cumplir los criterios de certificación aprobados por la autoridad de protección de datos.</p> <p>3. Establecer procedimientos para la expedición, revisión periódica y retirada de certificaciones, sellos y marcas de protección de datos en los términos descritos en el numeral 7 del artículo 45.</p> <p>4. Establecer procedimientos y estructuras para tratar los reclamos relativos al retiro de la certificación por el incumplimiento de los requisitos por parte de un responsable o encargado del tratamiento.</p> <p>5. Informar a la autoridad de protección de datos sobre las razones para la retirada de una certificación a un responsable o encargado del tratamiento.</p>	
<p><b>ARTÍCULO 47. Regla general de las transferencias.</b></p> <p>Solo se realizarán transferencias de datos personales si, a reserva de las demás disposiciones de la presente ley, el responsable o el encargado del tratamiento cumplen las condiciones establecidas en el presente título, incluidas las relativas a las transferencias ulteriores de datos personales. Todas las disposiciones del presente título se aplicarán, a fin de asegurar un nivel adecuado en materia de protección de datos personales.</p> <p><i>Parágrafo:</i> Se considera transferencia la salida de datos fuera del territorio nacional, bien sea por cesión o comunicación de datos, o por un tratamiento de</p>	<p><b>ARTÍCULO 47. Regla general de las transferencias.</b></p> <p>Solo se realizarán transferencias de datos personales si, a reserva de las demás disposiciones de la presente ley, el responsable o el encargado del tratamiento cumplen las condiciones establecidas en el presente título, incluidas las relativas a las transferencias ulteriores de datos personales. Todas las disposiciones del presente título se aplicarán, a fin de asegurar un nivel adecuado en materia de protección de datos personales.</p> <p><i>Parágrafo:</i> Se considera transferencia la salida de datos fuera del territorio nacional, bien sea por <del>cesión o comunicación</del> de datos, o por un tratamiento de</p>	Se realizan ajustes atendiendo a las recomendaciones dadas por la Cámara Colombia de Informática y Telecomunicaciones - CCIT-, expresando que: "con el fin de garantizar la seguridad jurídica y dotar al proyecto de ley de total claridad y cohesión en el texto" se procede a realizar la precisión sobre el uso de la "cesión de datos" y su definición.

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
datos personales por parte del encargado del tratamiento.	datos personales por parte del encargado del tratamiento.				
<b>ARTÍCULO 48. Transferencias basadas en un nivel adecuado de protección.</b> 1. Se podrán realizar transferencias de datos personales a países u organismos internacionales que proporcionen niveles adecuados de protección de datos. 2. Se entiende que un tercer país, un territorio, uno o varios sectores específicos del tercer país, o una organización internacional ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Autoridad de Protección de Datos sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a los sujetos obligados. Para emitir una decisión de adecuación, la Autoridad de Protección de Datos deberá tener en cuenta los siguientes elementos: a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales; b) La legislación vigente, tanto general como sectorial, incluidas las limitaciones y garantías para el acceso de las autoridades públicas a los datos personales;	<b>ARTÍCULO 48. Transferencias basadas en un nivel adecuado de protección.</b> 1. Se podrán realizar transferencias de datos personales a países u organismos internacionales que proporcionen niveles adecuados de protección de datos. 2. Se entiende que un tercer país, un territorio, uno o varios sectores específicos del tercer país, o una organización internacional ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Autoridad de Protección de Datos sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a los sujetos obligados. Para emitir una decisión de adecuación, la Autoridad de Protección de Datos deberá tener en cuenta los siguientes elementos: a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales; b) La legislación vigente, tanto general como sectorial, incluidas las limitaciones y garantías para el acceso de las autoridades	SIN MODIFICACIONES	c) La existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales; d) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país u organización que reciba la información, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a las personas Titulares de los datos en el ejercicio de sus derechos, y de cooperar con la Autoridad de Protección de Datos. 3. La declaración de nivel adecuado establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. Cuando la información disponible, muestre que un tercer país, un territorio o un sector específico de ese	públicas a los datos personales; c) La existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales; d) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país u organización que reciba la información, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a las personas Titulares de los datos en el ejercicio de sus derechos, y de cooperar con la Autoridad de Protección de Datos. 3. La declaración de nivel adecuado establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. Cuando la información disponible, muestre que un tercer país, un	
tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado de conformidad con lo dispuesto por el presente artículo, la Autoridad de Protección de Datos, podrá derogar, modificar o suspender, en la medida necesaria y sin efecto retroactivo, la decisión adecuación.  <i>Parágrafo primero:</i> La autoridad de protección de datos habilitará canales de contacto para que el tercer país u organización internacional, pueda subsanar la situación que dé lugar a la decisión adoptada, de conformidad con el numeral 3.	territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado de conformidad con lo dispuesto por el presente artículo, la Autoridad de Protección de Datos, podrá derogar, modificar o suspender, en la medida necesaria y sin efecto retroactivo, la decisión adecuación.  <i>Parágrafo primero:</i> La autoridad de protección de datos habilitará canales de contacto para que el tercer país u organización internacional, pueda subsanar la situación que dé lugar a la decisión adoptada, de conformidad con el numeral 3.		exigible, bilateral o multilateral, entre Colombia y otros países u organizaciones internacionales, que habilite las transferencias desde entidades u organismos públicos establecidas en Colombia hacia entidades u organismos públicos establecidas en otros países. b) Normas corporativas vinculantes de conformidad con el artículo 50 de la presente ley. c) Cláusulas contractuales modelo. La autoridad de protección de datos, establecerá los criterios bajo los cuales se deben elaborar las cláusulas. d) Un código de conducta aprobado con arreglo a la presente ley, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país, de aplicar garantías adecuadas, incluidas las relativas a los	vinculante y exigible, bilateral o multilateral, entre Colombia y otros países u organizaciones internacionales, que habilite las transferencias desde entidades u organismos públicos establecidas en Colombia hacia entidades u organismos públicos establecidas en otros países. b) Normas corporativas vinculantes de conformidad con el artículo 50 de la presente ley. c) Cláusulas contractuales modelo. La autoridad de protección de datos, establecerá los criterios bajo los cuales se deben elaborar las cláusulas. d) Un código de conducta aprobado con arreglo a la presente ley, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país, de aplicar garantías adecuadas,	
<b>ARTÍCULO 49. Transferencias mediante garantías adecuadas.</b> 1. A falta de declaración de nivel adecuado de protección, en los términos del artículo 48, el responsable o el encargado del tratamiento sólo podrá transferir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los titulares cuenten con derechos exigibles y acciones legales efectivas. 2. Las garantías adecuadas con arreglo al numeral 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de la autoridad de protección de datos, por: a) Un instrumento jurídicamente vinculante y	<b>ARTÍCULO 49. Transferencias mediante garantías adecuadas.</b> 1. A falta de declaración de nivel adecuado de protección, en los términos del artículo 48, el responsable o el encargado del tratamiento sólo podrá <del>transferir</del> <b>transferir</b> datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los titulares cuenten con derechos exigibles y acciones legales efectivas. 2. Las garantías adecuadas con arreglo al numeral 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de la autoridad de protección de datos, por: a) Un instrumento jurídicamente	Se realizan modificaciones de redacción.			



Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes.</p> <p>l) La formación en protección de datos pertinente, para el personal que tenga acceso permanente o habitual a datos personales.</p> <p>3. La autoridad de protección de datos podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y la autoridad de control en relación con las normas corporativas vinculantes según lo dispuesto en el presente artículo.</p> <p><i>Parágrafo primero.</i> Las Normas Corporativas Vinculantes sólo podrán ser sometidas a la aprobación de la autoridad de protección de datos una vez hayan sido aprobadas por el órgano correspondiente según los estatutos de la sociedad o los acuerdos del grupo empresarial. Las normas que sean formalmente presentadas ante la autoridad de protección de datos sólo estarán vigentes a partir de la fecha en que ésta emita su certificación y a partir de ese momento, se podrán aplicar.</p> <p><i>Parágrafo segundo.</i> En los casos en que las normas no sean aprobadas, los ajustes requeridos por la autoridad de protección de datos,</p>	<p>correspondiente según los estatutos de la sociedad o los acuerdos del grupo empresarial. Las normas que sean formalmente presentadas ante la autoridad de protección de datos sólo estarán vigentes a partir de la fecha en que ésta emita su certificación y a partir de ese momento, se podrán aplicar.</p> <p><i>Parágrafo segundo.</i> En los casos en que las normas no sean aprobadas, los ajustes requeridos por la autoridad de protección de datos, una vez realizados, deben contar con la aprobación del órgano social o contractual correspondiente, antes de ser sometidas, nuevamente, a aprobación.</p>	
<p>una vez realizados, deben contar con la aprobación del órgano social o contractual correspondiente, antes de ser sometidas, nuevamente, a aprobación.</p> <p><b>ARTÍCULO 51. Excepciones para situaciones específicas.</b></p> <p>1. En ausencia de una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, una transferencia o conjunto de transferencias de datos personales a terceros países u organizaciones internacionales sólo podrá realizarse si se cumplen alguna de las siguientes condiciones:</p> <p>a) El titular haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos de dichas transferencias debido a la ausencia de una declaración de nivel adecuado de protección y de garantías adecuadas.</p> <p>b) La transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento o para la ejecución de medidas precontractuales</p>	<p><b>ARTÍCULO 51. Excepciones para situaciones específicas.</b></p> <p>1. En ausencia de una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, una transferencia o conjunto de transferencias de datos personales a terceros países u organizaciones internacionales sólo podrá realizarse si se cumplen alguna de las siguientes condiciones:</p> <p>a) El titular haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos de dichas transferencias debido a la ausencia de una declaración de nivel adecuado de protección y de garantías adecuadas.</p> <p>b) La transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento o para la ejecución de medidas precontractuales</p>	SIN MODIFICACIONES
<p>adoptadas a solicitud del titular.</p> <p>c) La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del titular, entre el responsable del tratamiento y otra persona natural o jurídica.</p> <p>d) La transferencia sea necesaria por razones importantes de interés público.</p> <p>e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones o administrativas.</p> <p>f) La transferencia sea necesaria para proteger los intereses vitales del titular o de otras personas, cuando el titular esté física o jurídicamente incapacitado para dar su consentimiento.</p> <p>g) La transferencia se realice desde un registro público destinado a facilitar información y esté accesible para consulta por el público en general o cualquier persona con un interés legítimo, siempre que se cumplan las condiciones</p>	<p>adoptadas a solicitud del titular.</p> <p>c) La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del titular, entre el responsable del tratamiento y otra persona natural o jurídica.</p> <p>d) La transferencia sea necesaria por razones importantes de interés público.</p> <p>e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones o administrativas.</p> <p>f) La transferencia sea necesaria para proteger los intereses vitales del titular o de otras personas, cuando el titular esté física o jurídicamente incapacitado para dar su consentimiento.</p> <p>g) La transferencia se realice desde un registro público destinado a facilitar información y esté accesible para consulta por el público en general o cualquier persona con un</p>	
<p>establecidas por la ley para dicha consulta en cada caso particular. En tal situación, la transferencia no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro público. Si la finalidad del registro es la consulta por parte de personas con un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.</p> <p>2. Cuando una transferencia no pueda basarse en una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, y no se aplique ninguna de las excepciones para situaciones específicas mencionadas en el numeral primero del presente artículo, sólo podrá llevarse a cabo si se cumplen las siguientes condiciones:</p> <p>a) No es repetitiva.</p> <p>b) Afecta sólo a un número limitado de titulares.</p> <p>c) Es necesaria para fines e intereses legítimos imperiosos perseguidos por el responsable del</p>	<p>interés legítimo, siempre que se cumplan las condiciones establecidas por la ley para dicha consulta en cada caso particular. En tal situación, la transferencia no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro público. Si la finalidad del registro es la consulta por parte de personas con un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.</p> <p>2. Cuando una transferencia no pueda basarse en una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, y no se aplique ninguna de las excepciones para situaciones específicas mencionadas en el numeral primero del presente artículo, sólo podrá llevarse a cabo si se cumplen las siguientes condiciones:</p> <p>a) No es repetitiva.</p> <p>b) Afecta sólo a un número limitado de titulares.</p> <p>c) Es necesaria para fines e intereses legítimos imperiosos perseguidos</p>	





Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>conformidad con el artículo 50.</p> <p>g) Autorizar las cláusulas contractuales de las que trata el artículo 49, numeral 3, literal a).</p> <p>h) Autorizar los acuerdos administrativos entre las entidades u organismos públicos de conformidad con el artículo 49, numeral 3, literal b).</p> <p>i) Impartir instrucciones a los responsables y encargados del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones.</p> <p>j) Llevar a cabo visitas de inspección, de oficio o a solicitud de parte.</p> <p>k) Llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 45 de la presente ley.</p> <p>l) Requerir a los responsables y encargados del tratamiento sobre presuntas infracciones a la presente ley.</p> <p>m) Obtener de los responsables y encargados del tratamiento el acceso a toda la información necesaria para el ejercicio de sus funciones, así como el acceso a todas las instalaciones, incluidos equipos y medios de tratamiento de datos, respetando el debido proceso y la confidencialidad que ello requiere de acuerdo con la normativa vigente.</p> <p>n) Impartir instrucciones a los responsables y encargados</p>	<p>f) Aprobar normas corporativas vinculantes de conformidad con el artículo 50.</p> <p>g) Autorizar las cláusulas contractuales de las que trata el artículo 49, numeral 3, literal a).</p> <p>h) Autorizar los acuerdos administrativos entre las entidades u organismos públicos de conformidad con el artículo 49, numeral 3, literal b).</p> <p>i) Impartir instrucciones a los responsables y encargados del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones.</p> <p>j) Llevar a cabo visitas de inspección, de oficio o a solicitud de parte.</p> <p>k) Llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 45 de la presente ley.</p> <p>l) Requerir a los responsables y encargados del tratamiento sobre presuntas infracciones a la presente ley.</p> <p>m) Obtener de los responsables y encargados del tratamiento el acceso a toda la información necesaria para el ejercicio de sus funciones, así como el acceso a todas las instalaciones, incluidos equipos y medios de tratamiento de datos, respetando el debido proceso y la confidencialidad que ello requiere de acuerdo con la normativa vigente.</p>		<p>del tratamiento cuando las operaciones de tratamiento infrinjan lo dispuesto en la presente ley.</p> <p>o) Imponer multas de carácter personal o institucional a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido lo establecido en la presente ley.</p> <p>p) Imponer una limitación temporal o definitiva del tratamiento, como resultado de una sanción o de una orden administrativa a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido la presente ley.</p> <p>q) Impartir instrucciones a los responsables y encargados del tratamiento que atiendan las solicitudes de ejercicio de los derechos de los titulares en virtud de los artículos 18 al 27 de la presente ley.</p> <p>r) Impartir instrucciones al responsable del tratamiento para que comunique a los titulares, los incidentes de seguridad de los datos personales.</p> <p>s) Impartir instrucciones para garantizar el pleno y efectivo ejercicio de los derechos de rectificación, supresión o limitación del tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan</p>	<p>n) Impartir instrucciones a los responsables y encargados del tratamiento cuando las operaciones de tratamiento infrinjan lo dispuesto en la presente ley.</p> <p>o) Imponer multas de carácter personal o institucional a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido lo establecido en la presente ley.</p> <p>p) Imponer una limitación temporal o definitiva del tratamiento, como resultado de una sanción o de una orden administrativa a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido la presente ley.</p> <p>q) Impartir instrucciones a los responsables y encargados del tratamiento que atiendan las solicitudes de ejercicio de los derechos de los titulares en virtud de los artículos 18 al 27 de la presente ley.</p> <p>r) Impartir instrucciones al responsable del tratamiento para que comunique a los titulares, los incidentes de seguridad de los datos personales.</p> <p>s) Impartir instrucciones para garantizar el pleno y efectivo ejercicio de los derechos de rectificación, supresión o limitación del</p>	
<p>comunicado datos personales.</p> <p>t) Impartir instrucciones al organismo de certificación para que retire o que no emita una certificación con arreglo al artículo 45, si no se cumplen o dejan de cumplirse los requisitos para ello.</p> <p><i>Parágrafo Primero.</i> La Sala Administrativa del Consejo Superior de la Judicatura cumplirá funciones de promoción y difusión de la normativa en protección de datos personales en la Rama Judicial, y la Sala Disciplinaria será la encargada de investigar y sancionar la conducta de los funcionarios judiciales por el incumplimiento de la misma.</p> <p><i>Parágrafo Segundo.</i> El Departamento Administrativo de la Función Pública en articulación con la Autoridad de protección de datos realizará la promoción y difusión de la normativa en protección de datos personales que debe ser cumplida por cada una de las entidades públicas.</p>	<p>tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales.</p> <p>t) Impartir instrucciones al organismo de certificación para que retire o que no emita una certificación con arreglo al artículo 45, si no se cumplen o dejan de cumplirse los requisitos para ello.</p> <p><i>Parágrafo Primero.</i> La Sala Administrativa del Consejo Superior de la Judicatura cumplirá funciones de promoción y difusión de la normativa en protección de datos personales en la Rama Judicial, y la Sala Disciplinaria será la encargada de investigar y sancionar la conducta de los funcionarios judiciales por el incumplimiento de la misma.</p> <p><i>Parágrafo Segundo.</i> El Departamento Administrativo de la Función Pública en articulación con la Autoridad de protección de datos realizará la promoción y difusión de la normativa en protección de datos personales que debe ser cumplida por cada una de las entidades públicas.</p>		<p>como documento que contiene datos de carácter personal, teniendo en cuenta, entre otros, los siguientes criterios:</p> <p>a) Implementarán procedimientos de trazabilidad al interior de la organización, para evitar que se realicen copias no autorizadas de la cédula de ciudadanía entregada por los titulares. El titular podrá hacer uso de sellos, leyendas o firmas que determinen las condiciones de tiempo, modo, lugar y la finalidad con la que entrega la copia de su cédula de ciudadanía.</p> <p>b) Si no existe una base jurídica que legitime el tratamiento de los datos sensibles contenidos en la cédula de ciudadanía, deberá evitarse su captura o implementar técnicas de anonimización sobre los datos sensibles.</p> <p>c) Exclusivamente el personal autorizado podrá tener acceso a los lugares y/o activos de información donde se archiven</p>	<p>como documento que contiene datos de carácter personal, teniendo en cuenta, entre otros, los siguientes criterios:</p> <p>a) Implementarán procedimientos de trazabilidad al interior de la organización, para evitar que se realicen copias no autorizadas de la cédula de ciudadanía entregada por los titulares. El titular podrá hacer uso de sellos, leyendas o firmas que determinen las condiciones de tiempo, modo, lugar y la finalidad con la que entrega la copia de su cédula de ciudadanía.</p> <p>b) Si no existe una base jurídica que legitime el tratamiento de los datos sensibles contenidos en la cédula de ciudadanía, deberá evitarse su captura o implementar técnicas de anonimización sobre los datos sensibles.</p> <p>c) Exclusivamente el personal autorizado podrá tener acceso a los lugares y/o activos de información</p>	
<p><b>ARTÍCULO 55. Tratamiento de los documentos de identificación.</b></p> <p>1. El responsable y encargado del tratamiento implantarán las medidas técnicas y organizativas en atención al riesgo para evitar la circulación no autorizada de reproducciones digitales, copias o fotocopias de la cédula de ciudadanía,</p>	<p><b>ARTÍCULO 55. Tratamiento de los documentos de identificación.</b></p> <p>1. El responsable y encargado del tratamiento implantarán las medidas técnicas y organizativas en atención al riesgo para evitar la circulación no autorizada de reproducciones digitales, copias o fotocopias de la cédula de ciudadanía,</p>	SIN MODIFICACIONES			



Texto Radicado	Texto Propuesto para Primer Debate	Observaciones	Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
información personal más allá de lo estrictamente necesario para el funcionamiento del servicio y deben usarse exclusivamente con fines técnicos.	4. Las tecnologías de rastreo técnicamente necesarias no deben recopilar información personal más allá de lo estrictamente necesario para el funcionamiento del servicio y deben usarse exclusivamente con fines técnicos.		causado los daños y perjuicios. 4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, de conformidad a los numerales 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado. 5. Cuando, de conformidad con el numeral 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el numeral 2. 6. La autoridad de protección de datos será competente para conocer y decidir sobre la acción descrita en el presente artículo por el incumplimiento de las obligaciones de la presente ley, sin perjuicio del	modo alguno responsable del hecho que haya causado los daños y perjuicios. 4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, de conformidad a los numerales 2 y 3, responsables de cualquier daño o perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el numeral 2. 5. Cuando, de conformidad con el numeral 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el numeral 2. 6. La autoridad de protección de datos será competente para conocer y decidir sobre la acción descrita en	
<b>ARTÍCULO 58. Derecho a indemnización y responsabilidad.</b> 1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia del incumplimiento de cualquiera de las obligaciones contenidas en la presente ley, tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos. 2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por la presente ley. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento, cuando no haya cumplido con las obligaciones de la presente ley dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones del responsable. 3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del numeral 2, si demuestra que no es en modo alguno responsable del hecho que haya	<b>ARTÍCULO 58. Derecho a indemnización y responsabilidad.</b> 1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia del incumplimiento de cualquiera de las obligaciones contenidas en la presente ley, tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos. 2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por la presente ley. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento, cuando no haya cumplido con las obligaciones de la presente ley dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones del responsable. 3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del numeral 2, si demuestra que no es en	Se adiciona un párrafo nuevo atendiendo a las recomendaciones dadas por la Fundación Universitaria del Área Andina -AREANDINA- que señala la necesidad de otorgar funciones jurisdiccionales a la SIC para la aplicación de lo dispuesto en la presente norma: "ante la experticia de la entidad sobre el tema y una plataforma tecnológica que pueda soportar todas las actuaciones. Lo que se coadyuva con la capacidad socializadora y de autoridad que conserva la SIC y que se considera ha funcionado de manera apropiadas"			
derecho que tiene el titular de acceder a la administración de justicia.	el presente artículo por el incumplimiento de las obligaciones de la presente ley, sin perjuicio del derecho que tiene el titular de acceder a la administración de justicia.  <b>Parágrafo: Para efecto de la aplicación de lo dispuesto en el presente artículo, se adiciona un literal al artículo 24 de la Ley 1564 de 2012 el cual quedará así:</b>  <b>f. Acciones de indemnización de daños y perjuicios materiales o inmateriales como consecuencia del incumplimiento de cualquiera de las obligaciones del Régimen General de Protección de Datos.</b>		1. La autoridad de protección de datos, garantizará que la imposición de las sanciones con arreglo al presente título por las infracciones a los deberes y obligaciones contemplados en la presente ley, sean en cada caso individual efectivas, proporcionadas y correctivas. En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Administrativo y de lo Contencioso Administrativo. 2. Las sanciones se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 54. Al decidir la imposición de la sanción y su cuantía se graduarán atendiendo los siguientes criterios que resulten aplicables: a) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta el alcance o propósito de la operación de tratamiento de que se trate, así como, el número de titulares afectados y el daño o peligro generado a los intereses jurídicos tutelados en la presente ley. b) El alcance continuado de la	1. La autoridad de protección de datos, garantizará que la imposición de las sanciones con arreglo al presente título por las infracciones a los deberes y obligaciones contemplados en la presente ley, sean en cada caso individual efectivas, proporcionadas y correctivas. En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Administrativo y de lo Contencioso Administrativo. 2. Las sanciones se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 54. Al decidir la imposición de la sanción y su cuantía se graduarán atendiendo los siguientes criterios que resulten aplicables: a) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta el alcance o propósito de la operación de tratamiento de que se trate, así como, el número de titulares afectados y el daño o peligro generado a los intereses jurídicos tutelados en la presente ley.	
<b>ARTÍCULO 59. Sujetos Responsables.</b> Están sujetos al régimen sancionador establecido en la presente ley: 1. Los responsables del tratamiento, así como los corresponsables en la medida que su participación en la operación de tratamiento fuera determinante en la infracción. 2. Los encargados del tratamiento. 3. Las entidades de certificación. 4. Las entidades acreditadas de supervisión de los códigos de conducta.  <i>Parágrafo:</i> No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este título.	<b>ARTÍCULO 59. Sujetos Responsables.</b> Están sujetos al régimen sancionador establecido en la presente ley: 1. Los responsables del tratamiento, así como los corresponsables en la medida que su participación en la operación de tratamiento fuera determinante en la infracción. 2. Los encargados del tratamiento. 3. Las entidades de certificación. 4. Las entidades acreditadas de supervisión de los códigos de conducta.  <i>Parágrafo:</i> No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este título.	SIN MODIFICACIONES			
<b>ARTÍCULO 60. Condiciones generales para la imposición de sanciones.</b>	<b>ARTÍCULO 60. Condiciones generales para la imposición de sanciones.</b>	SIN MODIFICACIONES			

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>infracción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.</p> <p>c) Si existió dolo o negligencia en la comisión de la infracción.</p> <p>d) Los beneficios obtenidos por el infractor o terceros, en virtud de la comisión de la infracción.</p> <p>e) El grado de responsabilidad del infractor, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud del artículo 35.</p> <p>f) La reincidencia en la comisión de la infracción.</p> <p>g) La resistencia, negativa u obstrucción a las labores de inspección o de vigilancia de la Autoridad de protección de datos.</p> <p>h) La afectación a los derechos de los niñas, niños y adolescentes.</p> <p>i) El incumplimiento de las instrucciones impartidas en virtud del artículo 54, cuando hayan sido ordenadas previamente contra el infractor</p>	<p>b) El alcance continuado de la infracción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.</p> <p>c) Si existió dolo o negligencia en la comisión de la infracción.</p> <p>d) Los beneficios obtenidos por el infractor o terceros, en virtud de la comisión de la infracción.</p> <p>e) El grado de responsabilidad del infractor, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud del artículo 35.</p> <p>f) La reincidencia en la comisión de la infracción.</p> <p>g) La resistencia, negativa u obstrucción a las labores de inspección o de vigilancia de la Autoridad de protección de datos.</p> <p>h) La afectación a los derechos de los niñas, niños y adolescentes.</p> <p>i) El incumplimiento de las instrucciones impartidas en virtud del artículo</p>	
<p>en relación con el mismo asunto.</p> <p>j) La renuencia o desacato a cumplir las instrucciones impartidas por la autoridad de protección de datos.</p> <p>k) Si las infracciones fueron realizadas con el propósito de cometer alguna conducta tipificada como delito por la ley.</p> <p>l) Cualquier medida tomada por el infractor para contener y mitigar los daños y perjuicios sufridos por los titulares.</p> <p>m) El grado de cooperación con la autoridad de protección de datos, con el fin de contener y mitigar los posibles efectos adversos de la infracción.</p> <p>n) La posibilidad de que la conducta del titular hubiera podido inducir a la comisión de la infracción.</p> <p>o) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.</p> <p>p) La forma en que la autoridad de</p>	<p>54, cuando hayan sido ordenadas previamente contra el infractor en relación con el mismo asunto.</p> <p>j) La renuencia o desacato a cumplir las instrucciones impartidas por la autoridad de protección de datos.</p> <p>k) Si las infracciones fueron realizadas con el propósito de cometer alguna conducta tipificada como delito por la ley.</p> <p>l) Cualquier medida tomada por el infractor para contener y mitigar los daños y perjuicios sufridos por los titulares.</p> <p>m) El grado de cooperación con la autoridad de protección de datos, con el fin de contener y mitigar los posibles efectos adversos de la infracción.</p> <p>n) La posibilidad de que la conducta del titular hubiera podido inducir a la comisión de la infracción.</p> <p>o) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a</p>	
<p>protección de datos tuvo conocimiento de la infracción, en particular si el infractor notificó la infracción y, en tal caso, en qué medida.</p> <p>q) La adhesión a códigos de conducta en virtud del artículo 42 o a mecanismos de certificación aprobados de conformidad con el artículo 45.</p> <p>r) Disponer, cuando no fuere obligatorio, de un Oficial de protección de datos.</p> <p>s) El reconocimiento o aceptación expresas que haga el infractor sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.</p> <p>t) El sometimiento por parte del infractor, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier titular o interesado.</p> <p>u) Cualquier otro factor agravante o</p>	<p>la entidad absorbente.</p> <p>p) La forma en que la autoridad de protección de datos tuvo conocimiento de la infracción, en particular si el infractor notificó la infracción y, en tal caso, en qué medida.</p> <p>q) La adhesión a códigos de conducta en virtud del artículo 42 o a mecanismos de certificación aprobados de conformidad con el artículo 45.</p> <p>r) Disponer, cuando no fuere obligatorio, de un Oficial de protección de datos.</p> <p>s) El reconocimiento o aceptación expresas que haga el infractor sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.</p> <p>t) El sometimiento por parte del infractor, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias</p>	
<p>atenuante aplicable a las circunstancias del caso.</p> <p>3. Si la autoridad de protección de datos detecta un posible incumplimiento de las disposiciones de la presente ley por parte de una entidad pública, remitirá la actuación a la Procuraduría General de la Nación para que la procuraduría delegada competente realice la investigación correspondiente.</p> <p>4. El ejercicio por la autoridad de protección de datos de sus funciones en virtud del presente artículo estará sujeto a las garantías del debido proceso.</p>	<p>entre aquellos y cualquier titular o interesado.</p> <p>u) Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso.</p> <p>3. Si la autoridad de protección de datos detecta un posible incumplimiento de las disposiciones de la presente ley por parte de una entidad pública, remitirá la actuación a la Procuraduría General de la Nación para que la procuraduría delegada competente realice la investigación correspondiente.</p> <p>4. El ejercicio por la autoridad de protección de datos de sus funciones en virtud del presente artículo estará sujeto a las garantías del debido proceso.</p>	
<p><b>ARTÍCULO 61. Infracciones.</b> Constituyen infracciones los actos y conductas que resulten contrarios a la aplicación de los principios y obligaciones de la presente ley.</p>	<p><b>ARTÍCULO 61. Infracciones.</b> Constituyen infracciones los actos y conductas que resulten contrarios a la aplicación de los principios y obligaciones de la presente ley.</p>	SIN MODIFICACIONES
<p><b>ARTÍCULO 62. Sanciones.</b> La autoridad de protección de datos podrá imponer a los infractores las siguientes sanciones:</p> <p>1. Multas de carácter personal e institucional hasta por el equivalente de cuatro mil (4,000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción; o, hasta el cinco por ciento (5%) de los ingresos operacionales del infractor en el año fiscal inmediatamente anterior al</p>	<p><b>ARTÍCULO 62. Sanciones.</b> La autoridad de protección de datos podrá imponer a los infractores las siguientes sanciones:</p> <p>1. Multas de carácter personal e institucional hasta por el equivalente de cuatro mil (4,000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción; o, hasta el cinco por ciento (5%) de los ingresos operacionales del infractor en el año fiscal</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>de la imposición de la sanción.</p> <p>2. Sanciones operativas y medidas correctivas.</p> <p>a) Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán las medidas correctivas que se deberán adoptar.</p> <p>b) Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la autoridad de protección de datos.</p> <p>c) Cierre inmediato y definitivo de las operaciones relacionadas con el tratamiento ilícito de Datos Sensibles.</p> <p>d) Las medidas correctivas serán establecidas por la autoridad de protección de datos, de acuerdo a las facultades otorgadas por el artículo 54, dependiendo de cada caso individual y serán independientes de</p>	<p>inmediatamente anterior al de la imposición de la sanción.</p> <p>2. Sanciones operativas y medidas correctivas.</p> <p>a) Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán las medidas correctivas que se deberán adoptar.</p> <p>b) Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la autoridad de protección de datos.</p> <p>c) Cierre inmediato y definitivo de las operaciones relacionadas con el tratamiento ilícito de Datos Sensibles.</p> <p>d) Las medidas correctivas serán establecidas por la autoridad de protección de datos, de acuerdo a las facultades otorgadas por el artículo 54, dependiendo de cada caso individual y serán</p>	

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>la imposición de multas.</p>	<p>independientes de la imposición de multas.</p>	
<p><b>ARTÍCULO 63. Condiciones del consentimiento.</b></p> <p>La autorización entregada por los titulares de datos recabados antes de la entrada en vigencia de esta ley seguirá siendo válida por un período de un año contados desde la entrada en vigencia. Durante este plazo, el responsable deberá legitimar el tratamiento de datos de conformidad con el artículo 6.</p> <p><i>Parágrafo.</i> La autorización para el tratamiento de datos personales otorgada con fines de investigación en salud y biomédica recogidos con anterioridad a la entrada en vigencia de esta ley no perderá su legitimidad cuando concurra alguna de las circunstancias siguientes:</p> <p>a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento previo y expreso.</p> <p>b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.</p>	<p><b>ARTÍCULO 63. Condiciones del consentimiento.</b></p> <p>La autorización entregada por los titulares de datos recabados antes de la entrada en vigencia de esta ley seguirá siendo válida por un período de un año contados desde la entrada en vigencia. Durante este plazo, el responsable deberá legitimar el tratamiento de datos de conformidad con el artículo 6.</p> <p><i>Parágrafo.</i> La autorización para el tratamiento de datos personales otorgada con fines de investigación en salud y biomédica recogidos con anterioridad a la entrada en vigencia de esta ley no perderá su legitimidad cuando concurra alguna de las circunstancias siguientes:</p> <p>a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento previo y expreso.</p> <p>b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.</p>	SIN MODIFICACIONES
<p><b>ARTÍCULO 64. Plazos para la implantación de las medidas de seguridad.</b></p> <p>La implantación de las medidas de seguridad previstas en la presente ley deberá producirse con arreglo a las siguientes reglas:</p>	<p><b>ARTÍCULO 64. Plazos para la implantación de las medidas de seguridad.</b></p> <p>La implantación de las medidas de seguridad previstas en la presente ley deberá producirse con arreglo a las siguientes reglas:</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>1. Respecto de los tratamientos que existieran al momento de la entrada en vigencia de la presente ley se llevará a cabo de la siguiente manera:</p> <p>a) En el plazo máximo de dieciocho meses desde su entrada en vigencia, deberán implantarse las medidas de seguridad en los tratamientos automatizados.</p> <p>b) Respecto de los tratamientos no automatizados que existieran al momento de la entrada en vigencia de la presente ley, en el plazo máximo de un año.</p> <p>2. Los tratamientos, tanto automatizados como no automatizados, creadas con posterioridad a la fecha de entrada en vigencia de la presente ley deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en esta ley.</p> <p><i>Parágrafo.</i> A requerimiento de la autoridad de protección de datos, el responsable de Tratamiento deberá demostrar que está llevando a cabo la implementación de las medidas de seguridad en los tratamientos existentes en el momento de la entrada en vigencia de la presente ley.</p>	<p>1. Respecto de los tratamientos que existieran al momento de la presente ley se llevará a cabo de la siguiente manera:</p> <p>a) En el plazo máximo de dieciocho meses desde su entrada en vigencia, deberán implantarse las medidas de seguridad en los tratamientos automatizados.</p> <p>b) Respecto de los tratamientos no automatizados que existieran al momento de la entrada en vigencia de la presente ley, en el plazo máximo de un año.</p> <p>2. Los tratamientos, tanto automatizados como no automatizados, creadas con posterioridad a la fecha de entrada en vigencia de la presente ley deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en esta ley.</p> <p><i>Parágrafo.</i> A requerimiento de la autoridad de protección de datos, el responsable de Tratamiento deberá demostrar que está llevando a cabo la implementación de las medidas de seguridad en los tratamientos existentes en el momento de la entrada en vigencia de la presente ley.</p>	
<p><b>ARTÍCULO 65. Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.</b></p>	<p><b>ARTÍCULO 65. Régimen transitorio de las solicitudes para</b></p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
<p>Las solicitudes para el ejercicio de los derechos que hayan sido efectuadas con anterioridad a la entrada en vigencia de la presente ley, su contestación se regirá por la Ley 1581 de 2012.</p>	<p><b>el ejercicio de los derechos de las personas.</b></p> <p>Las solicitudes para el ejercicio de los derechos que hayan sido efectuadas con anterioridad a la entrada en vigencia de la presente ley, su contestación se regirá por la Ley 1581 de 2012.</p>	
<p><b>ARTÍCULO 66. Contratos de encargados del tratamiento.</b></p> <p>Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley serán válidos. Los responsables y encargados tendrán hasta dieciocho meses para modificar aquellos contratos que no resulten conforme a lo dispuesto en el artículo 32 de la presente ley.</p> <p>Durante dicho plazo cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 32 de la presente ley.</p> <p><i>Parágrafo.</i> Los contratos firmados con posterioridad a la fecha de entrada en vigencia de la presente ley deberán cumplir con los requisitos establecidos en el artículo 32.</p>	<p><b>ARTÍCULO 66. Contratos de encargados del tratamiento.</b></p> <p>Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley serán válidos. Los responsables y encargados tendrán hasta dieciocho meses para modificar aquellos contratos que no resulten conforme a lo dispuesto en el artículo 32 de la presente ley.</p> <p>Durante dicho plazo cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 32 de la presente ley.</p> <p><i>Parágrafo.</i> Los contratos firmados con posterioridad a la fecha de entrada en vigencia de la presente ley deberán cumplir con los requisitos establecidos en el artículo 32.</p>	SIN MODIFICACIONES
<p><b>ARTÍCULO 67. Transferencias Internacionales.</b></p> <p>1. Dentro de los primeros dos años posteriores a la entrada en vigencia de la presente ley, la Autoridad de Protección de Datos deberá revisar lo establecido en la Circular Única de la Superintendencia de Industria y Comercio relativo a las transferencias de datos personales, a la luz de los criterios establecidos en el artículo 48.</p>	<p><b>ARTÍCULO 67. Transferencias Internacionales.</b></p> <p>1. Dentro de los primeros dos años posteriores a la entrada en vigencia de la presente ley, la Autoridad de Protección de Datos deberá revisar lo establecido en la Circular Única de la Superintendencia de Industria y Comercio relativo a las transferencias de datos personales, a la luz de los criterios establecidos en el artículo 48.</p>	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
2. Una vez revisada la Circular Única de la Superintendencia de Industria y Comercio, los reconocimientos a países con nivel adecuado por parte de la autoridad de protección de datos a través su Circular tendrán una validez de hasta 2 años contados a partir de la entrada en vigencia de la presente ley.	2. Una vez revisada la Circular Única de la Superintendencia de Industria y Comercio, los reconocimientos a países con nivel adecuado por parte de la autoridad de protección de datos a través su Circular tendrán una validez de hasta 2 años contados a partir de la entrada en vigencia de la presente ley.	
<b>ARTÍCULO 68. Régimen Sancionatorio.</b> 1. El Régimen Sancionatorio contemplado en el Título VII entrará en aplicación a los 2 años de entrada en vigencia de la presente ley. La autoridad de protección de datos impondrá a los responsables y Encargados del Tratamiento las sanciones descritas en la Ley 1581 de 2012, señalando de forma paralela el equivalente de la infracción y su respectiva sanción en el Régimen Sancionatorio aprobado por la presente ley. 2. De conformidad con las facultades constitucionales que le han sido otorgadas a la Procuraduría General de la Nación, esta deberá asignar en el término de 18 meses con posterioridad a la entrada en vigencia de la presente ley, las funciones y competencias a una procuraduría delegada que será seleccionada o creada atendiendo a los criterios de especialidad por el incumplimiento a las	<b>ARTÍCULO 68. Régimen Sancionatorio.</b> 1. El Régimen Sancionatorio contemplado en el Título VII entrará en aplicación a los 2 años de entrada en vigencia de la presente ley. La autoridad de protección de datos impondrá a los responsables y Encargados del Tratamiento las sanciones descritas en la Ley 1581 de 2012, señalando de forma paralela el equivalente de la infracción y su respectiva sanción en el Régimen Sancionatorio aprobado por la presente ley. 2. De conformidad con las facultades constitucionales que le han sido otorgadas a la Procuraduría General de la Nación, esta deberá asignar en el término de 18 meses con posterioridad a la entrada en vigencia de la presente ley, las funciones y competencias a una procuraduría delegada que será seleccionada o creada atendiendo a los criterios de especialidad por el incumplimiento a las	SIN MODIFICACIONES

Texto Radicado	Texto Propuesto para Primer Debate	Observaciones
disposiciones establecidas en la presente ley.	disposiciones establecidas en la presente ley.	
<b>ARTÍCULO 69. Registro Nacional de Bases de Datos - RNBD.</b> El Directorio Público de Bases de Datos, actualmente gestionado por la autoridad de protección de datos, experimentará una transformación tanto en su denominación como en su estructura, convirtiéndose en el "Registro de las Actividades del Tratamiento", en un plazo máximo de dos años a partir de la entrada en vigencia de la presente ley. El Gobierno Nacional reglamentará las categorías de sujetos obligados, así como los términos y condiciones bajo los cuales deben inscribirse en el Registro señalado.	<b>ARTÍCULO 69. Registro Nacional de Bases de Datos - RNBD.</b> El Directorio Público de Bases de Datos, actualmente gestionado por la autoridad de protección de datos, experimentará una transformación tanto en su denominación como en su estructura, convirtiéndose en el "Registro de las Actividades del Tratamiento", en un plazo máximo de dos años a partir de la entrada en vigencia de la presente ley. El Gobierno Nacional reglamentará las categorías de sujetos obligados, así como los términos y condiciones bajo los cuales deben inscribirse en el Registro señalado.	SIN MODIFICACIONES
<b>ARTÍCULO 70. Entidades Certificadoras</b> Los organismos del subsistema de calidad tendrán un año desde la entrada en vigencia de la presente ley para regular la forma de acreditar las entidades descritas en el artículo 45.	<b>ARTÍCULO 70. Entidades Certificadoras</b> Los organismos del subsistema de calidad tendrán un año desde la entrada en vigencia de la presente ley para regular la forma de acreditar las entidades descritas en el artículo 45.	SIN MODIFICACIONES
<b>ARTÍCULO 71. Vigencia y Derogatorias</b> La presente ley entra en vigencia desde su promulgación y será de aplicación obligatoria un año después, salvaguarda los derechos adquiridos y deroga todas las disposiciones que le sean contrarias. También deroga la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa relacionada que sea contraria a las disposiciones de la presente ley.	<b>ARTÍCULO 71. Vigencia y Derogatorias</b> La presente ley entra en vigencia desde su promulgación y será de aplicación obligatoria un año después, salvaguarda los derechos adquiridos y deroga todas las disposiciones que le sean contrarias. También deroga la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa relacionada que sea contraria a las disposiciones de la presente ley.	SIN MODIFICACIONES

**VII. CONCLUSIONES.**

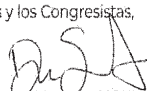
  

La presente iniciativa legislativa establece la actualización del régimen de protección de datos personales y con ello comprende que la tecnología es la base para el desarrollo de los individuos hoy en día. De esta forma, el articulado propuesto comprende que se requiere brindar garantías para la protección de los derechos fundamentales de los individuos como lo es el habeas data y avanzar en la existencia de una normatividad actualizada que garantice la protección de los datos de los ciudadanos y mitigar los riesgos que generan las nuevas tecnologías en materia de privacidad y manejo de la información de los ciudadanos.


**VIII. PROPOSICIÓN FINAL.**

En atención a las consideraciones anteriormente expuestas, se presenta **PONENCIA POSITIVA con modificaciones** y se solicita respetuosamente a los integrantes de la Comisión Primera Constitucional Permanente de la Cámara de Representantes dar primer debate al Proyecto de Ley Estatutaria No. 152 de 2024 Cámara "**Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales**", conforme al texto propuesto.


De las y los Congresistas,




**DUVALIER SANCHEZ ARANGO**  
Representante a la Cámara




**JUAN CARLOS WILLS OSPINA**  
Representante a la Cámara




**GERSEL LUIS PEREZ ALTAMIRANDA**  
Representante a la Cámara




**CARLOS FELIPE QUINTERO OVALLE**  
Representante a la Cámara




**HERNAN DARIO CADAVID MARQUEZ**  
Representante a la Cámara




**ASTRID SANCHEZ MONTES DE OCA**  
Representante a la Cámara




**DIÓGENES QUINTERO AMAYA**  
Representante a la Cámara



**JORGE ALEJANDRO OCAMPO GIRALDO**  
Representante a la Cámara



**LUIS ALBERTO ALBAN URBANO**  
Representante a la Cámara



**MARELEN CASTILLO TORRES**  
Representante a la Cámara



<p><b>IX. TEXTO PROPUESTO PARA PRIMER DEBATE EN LA COMISIÓN PRIMERA CONSTITUCIONAL PERMANENTE DE LA CÁMARA DE REPRESENTANTES</b></p> <p><b>PROYECTO DE LEY ESTATUTARIA 152 DE 2024 CÁMARA</b></p> <p><b>“POR LA CUAL SE DICTAN DISPOSICIONES PARA EL RÉGIMEN GENERAL DE PROTECCIÓN DE DATOS PERSONALES”</b></p> <p><b>EL CONGRESO DE COLOMBIA,</b></p> <p><b>DECRETA:</b></p> <p><b>TÍTULO I</b></p> <p><b>DISPOSICIONES GENERALES</b></p> <p><b>CAPÍTULO I</b></p> <p><b>OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES</b></p> <p><b>ARTÍCULO 1. Objeto.</b></p> <p>La presente ley establece las normas relativas a la protección de las personas naturales en <b>materia de</b> la protección y tratamiento de sus datos personales <b>y su</b> libre circulación.</p> <p>De igual manera, la presente ley protege los derechos y garantías fundamentales de las personas naturales y, en particular, su derecho fundamental a la protección de los datos personales, en los términos descritos en el artículo 15 de la Constitución Política.</p> <p><b>ARTÍCULO 2. Ámbito de la aplicación material.</b></p> <ol style="list-style-type: none"> <li>La presente ley se aplica al tratamiento de los datos personales.</li> <li>El régimen de protección de datos personales establecido en la presente ley no será de aplicación:             <ol style="list-style-type: none"> <li>A los tratamientos efectuados por una persona natural en un ámbito exclusivamente personal o doméstico.</li> <li>A los tratamientos realizados por parte de las autoridades</li> </ol> </li> </ol>	<p>competentes con fines de prevención, investigación, detección, o procesamiento judicial de actos delictivos incluido el lavado de activos y el financiamiento del terrorismo, la ejecución de sanciones penales, así como la de protección frente a amenazas a la seguridad y defensa nacional y su prevención.</p> <ol style="list-style-type: none"> <li>A los tratamientos que tengan como finalidad cumplir con la actividad periodística y otros contenidos editoriales.</li> <li>A los tratamientos que tengan como fin y contengan información de inteligencia y contrainteligencia.</li> <li>A los tratamientos realizados en virtud de la Ley 1266 de 2008</li> </ol> <p><i>Parágrafo primero.</i> Cuando se traten datos de personas fallecidas, los causahabientes, que acrediten tal calidad, podrán dirigirse al responsable o encargado del tratamiento con el objeto de solicitar el acceso a los datos personales de la persona fallecida y, en su caso, su rectificación o supresión.</p> <p><i>Parágrafo segundo.</i> El Gobierno Nacional, reglamentará el tratamiento de datos personales para fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos, la financiación del terrorismo y la ejecución de sanciones penales.</p> <p><i>Parágrafo tercero.</i> Los principios sobre protección de datos serán aplicables a todos los tratamientos de datos personales, incluidos los exceptuados en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal.</p> <p>En el evento que la normatividad especial regule los tratamientos de datos personales exceptuados <b>se deben establecer</b> principios que tengan en consideración la naturaleza especial de los datos <b>y los cuales serán aplicables</b> de manera concurrente a los previstos en la presente ley.</p> <p><b>ARTÍCULO 3. Ámbito territorial.</b></p> <ol style="list-style-type: none"> <li>La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de los responsables o del encargado con domicilio y/o residencia en territorio nacional, independientemente de que el tratamiento tenga lugar o no en Colombia.</li> </ol>
<ol style="list-style-type: none"> <li>La presente ley se aplica al tratamiento de datos personales de titulares que residan en territorio nacional por parte de un responsable o encargado no establecido en Colombia, cuando las actividades de tratamiento estén relacionadas con:             <ol style="list-style-type: none"> <li>La oferta de bienes o servicios a dichos titulares con residencia en Colombia.</li> <li>El control del comportamiento, en la medida en que este tenga lugar en Colombia.</li> </ol> </li> <li>Por un responsable o encargado que no esté establecido en Colombia, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud del derecho internacional público.</li> </ol> <p><b>ARTÍCULO 4. Definiciones.</b> A efectos de la presente ley se entenderá por:</p> <ol style="list-style-type: none"> <li>«Anonimización»: procedimiento técnico que modifica de manera irreversible los datos personales con el fin que no pueda atribuirse a un titular;</li> <li>«Autoridad de Protección de Datos»: entidad pública que tiene como objetivo principal inspeccionar, vigilar y controlar la aplicación del Régimen General de Protección de Datos establecido en esta ley y las demás disposiciones que la desarrollen, modifiquen, adicione o complementen, garantizando la protección de los derechos de los titulares y el efectivo cumplimiento de los deberes de quienes intervengan en el tratamiento de los datos personales.</li> <li>«Base de datos»: todo conjunto de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado.</li> <li>«Bloqueo de datos»: medidas técnicas y organizativas adoptadas por parte del responsable o encargado del tratamiento, que permitan la identificación y reserva de los datos para impedir y/o evitar su tratamiento.</li> <li>«<b>Cesión</b> de datos»: tratamiento de datos que implica su revelación a una persona distinta del titular y/o encargado de tratamiento.</li> <li>«Consentimiento del titular»: Toda manifestación de la voluntad expresa, libre, inequívoca, informada y específica por la que el titular acepta de forma previa, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen.</li> <li>«Corresponsabilidad»: Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento.</li> </ol>	<ol style="list-style-type: none"> <li>«Datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural, que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.</li> <li>«Datos genéticos»: datos personales relativos a la información sobre las características hereditarias de una persona natural, obtenidas por análisis de ácidos nucleicos u otros análisis científicos de una muestra biológica, que proporcionen una información única sobre la fisiología o la salud de esa persona.</li> <li>«Datos personales»: toda información sobre una persona natural identificada o identificable (el titular) se considerará persona natural 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.</li> <li>«Datos relativos a la salud»: datos que revelan aspectos relativos al estado de bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades de una persona natural. Estos datos incluyen, aunque no limitado a, la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud; la información recolectada por dispositivos tecnológicos que busquen hacer mediciones sobre la condición física de su usuario, entre otros.</li> <li>«Datos sensibles»: son los que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características biológicas, identidad o expresión de género y orientación sexual de una persona natural.</li> <li>«Destinatario o tercero»: persona natural o jurídica, pública o privada, a la que se comuniquen datos personales, distinta del titular, responsable de tratamiento y encargado. Una vez el destinatario se le ceden los datos se convierte en responsable. No se considerarán destinatarios a las autoridades públicas que puedan recibir datos personales en el marco</li> </ol>

<p>de una investigación concreta de conformidad con el artículo 2, numeral 2, literal b) y d) de la presente ley.</p> <p>14. «Elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales con el fin de evaluar determinados aspectos de una persona natural. En particular, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, movimientos, entre otros, de dicha persona natural.</p> <p>15. «Encargado del tratamiento» o «Encargado»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.</p> <p>16. «Incidente de seguridad»: cualquier violación de los códigos de seguridad que resulte en el daño, la destrucción, pérdida o alteración accidental o intencional de datos personales, que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado, y que impacte en la confidencialidad, integridad y/o disponibilidad de dichos datos.</p> <p>17. «Limitación del tratamiento»: aplicación de medidas por parte del responsable de manera que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse.</p> <p>18. «Neurodato»: para los efectos de la presente ley, se refiere al conjunto de información obtenida a partir de la actividad cerebral y el sistema nervioso, así como la información inferida de estos datos, de una persona natural identificada o identificable.</p> <p>19. «Representante»: persona natural o jurídica designada por escrito por parte del responsable o el encargado del tratamiento, de conformidad con esta ley, para que los represente en lo que respecta a sus obligaciones en virtud de la presente ley.</p> <p>20. «Responsable del tratamiento» o «responsable»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros determine los fines y medios del tratamiento.</p> <p>21. «Servicio de la sociedad de la información»: <u>Se entenderá como cualquier servicio que, a solicitud de un usuario, sea prestado mediante el uso de equipos electrónicos o tecnologías de la información y las comunicaciones, permitiendo la creación, distribución y manipulación de la información, sin requerir la presencia simultánea de las partes involucradas. Estos servicios pueden incluir, entre otros, el comercio electrónico, plataformas de redes sociales,</u></p>	<p><b>aplicaciones móviles y servicios de almacenamiento en la nube.</b></p> <p>22. «Seudonimización»: tratamiento de datos personales que ya no puedan atribuirse a un titular sin utilizar información adicional. Dicha información debe figurar por separado, estar sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.</p> <p>23. «Titular»: persona natural cuyos datos personales son objeto de Tratamiento.</p> <p>24. «Transferencia internacional de datos personales»: tratamiento que supone un flujo de datos, en el que un responsable y/o encargado del tratamiento ubicado en el territorio nacional, envía y/o habilita accesos a datos personales a destinatarios y/o encargados que se encuentran en el territorio nacional.</p> <p>25. «Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como pueden ser, la recogida, registro, organización, estructuración, conservación, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.</p> <p>26. «Tratamiento a gran escala»: es aquel que afecta a una gran cantidad de datos que se refieren a un elevado número de titulares y que entraña un alto riesgo. Su valoración dependerá de la proporción de la población correspondiente, el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento, el alcance geográfico y la duración o permanencia del tratamiento.</p> <p style="text-align: center;"><b>CAPÍTULO II</b></p> <p style="text-align: center;"><b>PRINCIPIOS Y CONDICIONES RELATIVAS A LA PROTECCIÓN DE DATOS</b></p> <p><b>ARTÍCULO 5. Principios relativos al tratamiento.</b></p> <p>1. El tratamiento de datos personales debe darse en virtud de los siguientes principios:</p> <p style="margin-left: 40px;">a) «Principio de Legalidad»: el tratamiento de los datos personales debe sujetarse a lo establecido en la ley y en las demás</p>
<p>disposiciones que la desarrollen.</p> <p>b) «Principio de lealtad»: las finalidades con la que se recolectan datos personales encontrarán sus límites en la presente ley y no podrán obtenerse por vías fraudulentas, engañosas, ni por acciones que puedan calificarse como dolosas.</p> <p>c) «Principio de transparencia»: exige que la Información facilitada a los titulares sea concisa, accesible e inteligible, utilizando un lenguaje claro y sencillo.</p> <p>d) «Principio de limitación de la finalidad»: los datos <b>personales</b> deben ser <b>recolectados únicamente para fines específicos</b>, explícitos y legítimos. <b>No podrán ser tratados posteriormente para otros fines que no se ajusten a los objetivos originales. Sin embargo, el uso posterior</b> de los datos <b>para</b> fines de archivo en interés público, investigación científica, histórica o estadística se considerará <b>adecuado y permitido, incluso si no coincide exactamente con el propósito inicial.</b></p> <p>e) «Principio de minimización de datos»: sólo se deben recabar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.</p> <p>f) «Principio de exactitud»: los datos de carácter personal deberán ser exactos de tal forma que respondan con veracidad a la situación actual del titular. Si fuera necesario, actualizados; se adoptarán todas las medidas razonables para rectificar o suprimir, sin demora injustificada, los factores que introducen las inexactitudes en los datos personales con respecto a los fines para los que se tratan. Los datos facilitados directamente por el titular se considerarán exactos.</p> <p>g) «Principio de limitación del plazo de conservación»: los datos deben ser mantenidos de forma que se permita la identificación de los titulares durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se trate exclusivamente en cumplimiento de un deber legal o contractual, atendiendo a las disposiciones aplicables a los aspectos administrativos, contables, fiscales, jurídicos, con fines de archivo en interés público, investigación científica, histórica o estadística, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la</p>	<p>presente ley a fin de proteger los derechos y garantías de los titulares.</p> <p>h) «Principio de integridad»: consiste en implantar las medidas de seguridad técnicas y organizativas que garantice que el dato no sea alterado de manera no autorizada. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.</p> <p>i) «Principio de confidencialidad»: los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase del tratamiento, tendrán el deber de garantizar que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. El responsable y/o encargado del tratamiento están obligados a garantizar la reserva de la información, inclusive después de finalizado el tratamiento.</p> <p>El principio señalado será complementario de los deberes de secreto profesional de conformidad con su normativa aplicable.</p> <p>j) «Principio de seguridad»: los sujetos que participen en cualquier etapa del tratamiento deberán realizar análisis de riesgos, orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten, con el fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.</p> <p>k) «Principio de proporcionalidad»: durante el ciclo de vida de los datos, el responsable velará porque el tratamiento sea idóneo respecto a los fines; necesario en cuanto no existan otras medidas para conseguir el fin perseguido; y equilibrado respecto al beneficio que dicho tratamiento proporciona y su impacto sobre los derechos y garantías fundamentales de los titulares.</p> <p>l) «Principio de explicabilidad»: los responsables del tratamiento deben ser capaces de explicar de manera clara y comprensible a los titulares cómo se están utilizando sus datos personales y cómo se toman las decisiones en función de ellos. Los encargados del tratamiento asistirán al responsable en el</p>

<p>cumplimiento de esta obligación.</p> <p>m) «Principio de responsabilidad demostrada» «accountability»: El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en la presente ley, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de protección de datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.</p> <p><b>ARTÍCULO 6. Bases que legitiman el tratamiento.</b></p> <p>1. El tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones:</p> <ol style="list-style-type: none"> <li>El titular dio su consentimiento previo para el tratamiento de sus datos personales para uno o varios fines específicos.</li> <li>El tratamiento es necesario para la ejecución de un contrato en el que el titular es parte o para la aplicación de medidas precontractuales solicitadas por el titular.</li> <li>El tratamiento es necesario para el cumplimiento de un deber legal aplicable al responsable del tratamiento.</li> <li>El tratamiento es necesario en casos de urgencia médica o sanitaria del titular o de otra persona natural.</li> <li>El tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución y la ley.</li> <li>El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan sobre los intereses, derechos y garantías fundamentales del titular que requieran la protección de datos personales. Es fundamental que exista una relación relevante entre el titular y el responsable, en particular cuando el titular sea un menor de</li> </ol>	<p>edad. Se debe realizar un examen de ponderación que garantice que el tratamiento sea lícito, necesario y equilibrado en relación con los derechos del titular.</p> <p>Lo dispuesto en este literal no será aplicable al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.</p> <p>2. Cuando la base jurídica que legitima el tratamiento sea el cumplimiento de un deber legal o el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas la finalidad de este debe estar fundamentada en normativa con rango de ley vigente.</p> <p><i>Parágrafo primero:</i> La normativa vigente a la que se refiere el numeral 2 del presente artículo podrá contener disposiciones específicas para adaptar la aplicación de la presente ley, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los titulares afectados; las entidades a las que se pueden ceder datos personales y los fines de tal cesión; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo. La normativa vigente cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.</p> <p><i>Parágrafo segundo:</i> Las normativas expedidas con posterioridad a la presente ley podrán introducir disposiciones que cumplan con los criterios establecidos en el presente Régimen General de Protección de Datos con respecto al tratamiento, en cumplimiento del numeral 1, literal c) y e), fijando de manera precisa requisitos específicos de tratamiento y otras medidas de conformidad con la presente ley.</p> <p><b>ARTÍCULO 7. Tratamientos con finalidades diferentes a las iniciales.</b></p> <p>Cuando se quiera tratar los datos personales para una finalidad diferente a la que fueron recogidos, y ese nuevo tratamiento no esté basado en el consentimiento del titular o en una norma específica que sea necesaria y proporcional en una sociedad democrática, el responsable del tratamiento deberá considerar si el nuevo tratamiento es compatible con la finalidad original. Para ello, tomará en cuenta lo siguiente:</p> <ol style="list-style-type: none"> <li>La relación entre la finalidad original y la nueva finalidad de</li> </ol>
<p>tratamiento de los datos personales.</p> <ol style="list-style-type: none"> <li>El contexto en que se recogieron los datos personales, especialmente la relación entre los titulares y el responsable del tratamiento.</li> <li>La naturaleza de los datos personales, especialmente si son datos sensibles o relacionados con antecedentes penales, anotaciones judiciales o contravencionales.</li> <li>Las posibles consecuencias para los titulares por el nuevo tratamiento de sus datos.</li> <li>La existencia de garantías adecuadas, como el cifrado o la seudonimización de los datos.</li> </ol> <p><b>ARTÍCULO 8. Condiciones para el consentimiento.</b></p> <ol style="list-style-type: none"> <li>Cuando el tratamiento se base en el consentimiento del titular, el responsable deberá ser capaz de demostrar que aquel otorgó el consentimiento de forma previa el tratamiento de sus datos personales.</li> <li>Corresponderá al responsable del tratamiento, demostrar la existencia del consentimiento del titular por cualquier medio de prueba admisible en derecho.</li> <li>Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, debiendo constar cada finalidad de forma separada, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente ley.</li> <li>El responsable establecerá mecanismos o procedimientos que permitan al titular manifestar su consentimiento mediante un acto afirmativo que refleje una manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. El silencio, las casillas <b>no</b> marcadas o la inacción no deben constituir consentimiento.</li> <li>Si el responsable del tratamiento solicita el consentimiento del titular durante la ejecución de un contrato y este no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al titular que manifieste expresamente su negativa al tratamiento.</li> <li>El titular tendrá derecho a revocar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará la legalidad del</li> </ol>	<p>tratamiento basada en el consentimiento previo a la revocatoria. Será tan fácil revocar el consentimiento como darlo.</p> <p><b>ARTÍCULO 9. Consentimiento de niños, niñas y adolescentes.</b></p> <ol style="list-style-type: none"> <li>El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de dieciséis años. Se exceptúan los supuestos en que la ley exija la asistencia del representante legal para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.</li> <li>El tratamiento de los datos de los menores de dieciséis años, fundado en el consentimiento, sólo será lícito si consta el consentimiento del representante legal, con el alcance que determine el mismo.</li> <li>En relación con la oferta directa a menores de edad de servicios de la sociedad de la información, le serán aplicables las reglas establecidas en el numeral 1 y 2 del presente artículo teniendo en cuenta la tecnología disponible. Cuando concurra la situación descrita en el numeral 2, el responsable del tratamiento adoptará todas las medidas razonables con los recursos que dispone, para verificar que el consentimiento fue dado o autorizado por el representante legal del menor.</li> <li>El numeral 1 no afectará las disposiciones especiales referentes al establecimiento de edades mínimas para efectos civiles y penales, respecto de la validez y consecuencias de ciertos actos jurídicos.</li> <li>El tratamiento de datos personales de menores de edad siempre debe responder al interés superior del menor y asegurar el respeto de sus derechos fundamentales.</li> </ol> <p><i>Parágrafo:</i> En caso de lo dispuesto en el numeral 2, cuando la representación legal del menor de dieciséis años es ejercida por más de una persona, se presume que el consentimiento de uno obedece a la voluntad de todos. En el supuesto de que, uno de los representantes no esté de acuerdo, puede revocar el consentimiento ante el responsable del tratamiento, y sólo podría concederse nuevamente por el mutuo acuerdo de los representantes, o mediante decisión judicial que declare su representación legal.</p> <p><b>ARTÍCULO 10. Tratamiento de datos sensibles.</b></p> <ol style="list-style-type: none"> <li>Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o</li> </ol>

<p>filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características biológicas, identidad o expresión de género y orientación sexual de una persona natural.</p> <p>2. El numeral 1 no será de aplicación cuando concurra alguna de las siguientes excepciones:</p> <ol style="list-style-type: none"> <li>a) Cuando el titular dio su consentimiento previo y expreso para el tratamiento de dichos datos personales para uno o más fines específicos, excepto cuando la ley impida al titular levantar la prohibición mencionada en el numeral 1.</li> <li>b) Cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral o de la seguridad social, en la medida en que así lo autorice la ley o una convención colectiva de trabajo con arreglo a la normatividad vigente, que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del titular.</li> <li>c) Cuando el tratamiento sea necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto que el titular se encuentre incapacitado física o jurídicamente para autorizar dicho tratamiento.</li> <li>d) Cuando el tratamiento sea realizado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otra organización sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los titulares.</li> <li>e) Cuando el tratamiento se refiera a datos personales que el titular de forma libre y voluntaria decida hacer públicos. No debe ser una divulgación de datos accidental, inadvertida o involuntaria.</li> <li>f) Cuando el tratamiento sea necesario para la formulación, el</li> </ol>	<p>ejercicio o la defensa de reclamaciones y/o procedimientos administrativos y/o judiciales, así como procedimientos extrajudiciales o cuando sea un órgano judicial que actúe en ejercicio de su función.</p> <ol style="list-style-type: none"> <li>g) Cuando el tratamiento sea necesario por razones de interés público, para la prestación de servicios públicos o por parte de entidades que ejerzan funciones públicas, sobre la base de la normativa que los faculta para ejercer dichas funciones; el tratamiento debe ser proporcional al objetivo perseguido, respetando el derecho a la protección de datos, estableciendo medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del titular.</li> <li>h) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluaciones médicas ocupacionales del trabajador, diagnóstico médico, prestación de asistencia o tratamiento médico, gestión de los sistemas y prestación de servicios de salud, sobre la base de la normativa o en virtud de un contrato con un profesional de la salud, sin perjuicio de las condiciones y garantías contempladas en el numeral 3 del presente artículo.</li> <li>i) Cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transnacionales graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de la norma, que establezca medidas adecuadas y específicas para proteger los derechos y garantías del titular, en particular el secreto profesional. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y garantías de las personas naturales.</li> <li>j) El tratamiento es necesario con fines de archivo en interés público, investigación científica, histórica o estadística; este debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos, establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.</li> </ol> <p>3. Los datos personales a los que se refiere el numeral 1 podrán tratarse a los fines citados en el numeral 2, literal h), cuando su tratamiento sea</p>
<p>realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto profesional de acuerdo con el artículo 74 de La Constitución Política de Colombia.</p> <p><i>Parágrafo:</i> Cuando por alguna de las causales a las que se refiere el numeral segundo se deban tratar datos sensibles referentes al sexo, identidad o expresión de género y orientación sexual, deberán hacer uso de todas las categorías identitarias diversas, como personas intersexuales y no binarias. En el supuesto de que el titular del dato haya dado su consentimiento para el tratamiento de los datos aquí referidos y ejercite los derechos de rectificación y supresión, no se le exigirán requisitos adicionales para comprobar esta información.</p> <p><b>ARTÍCULO 11. Tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.</b></p> <p>El tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales, así como las medidas de seguridad conexas, además de cumplir con las obligaciones establecidas en la presente ley, sólo podrá realizarse bajo la supervisión de las entidades competentes, quienes deberán garantizar la protección adecuada de los derechos y garantías de los titulares.</p> <p><b>ARTÍCULO 12. Tratamiento de datos relativos a sanciones administrativas y/o disciplinarias.</b></p> <ol style="list-style-type: none"> <li>1. El tratamiento de datos relativo a sanciones administrativas y/o disciplinarias, incluido el mantenimiento de registros relacionados con las mismas, exigirá:             <ol style="list-style-type: none"> <li>a) Que los responsables de dichos tratamientos sean los organismos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.</li> <li>b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.</li> </ol> </li> <li>2. Cuando no se cumpla alguna de las condiciones previstas en el numeral anterior, los tratamientos de datos referidos a infracciones, sanciones</li> </ol>	<p>administrativas y/o disciplinarias, habrán de contar con el consentimiento del titular o estar autorizados por una norma, en la que se regularán, en su caso, garantías adicionales para los derechos de los titulares.</p> <p>3. Fuera de los supuestos señalados en los numerales anteriores, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias sólo serán posibles cuando sean llevados a cabo por abogados y/o agentes oficiosos y que tengan por objeto recoger la información facilitada por sus representados para el ejercicio de sus funciones.</p> <p><i>Parágrafo:</i> Lo descrito en el presente artículo se aplicará igualmente a las sanciones disciplinarias de los servidores públicos.</p> <p style="text-align: center;"><b>TÍTULO II</b></p> <p style="text-align: center;"><b>DEBER DE INFORMACIÓN Y DERECHOS DE LOS TITULARES</b></p> <p style="text-align: center;"><b>CAPÍTULO I</b></p> <p style="text-align: center;"><b>TRANSPARENCIA E INFORMACIÓN</b></p> <p><b>ARTÍCULO 13. Transparencia e información al titular.</b></p> <ol style="list-style-type: none"> <li>1. El responsable del tratamiento tomará las medidas pertinentes para facilitar al titular toda la información indicada en los artículos 14 y 15, así como cualquier comunicación correspondiente a los ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un menor. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. A petición del titular, la información podrá facilitarse verbalmente siempre que se acredite la identidad del mismo por medios adecuados.</li> <li>2. El responsable del tratamiento facilitará al titular mecanismos sencillos y ágiles para el ejercicio de sus derechos en virtud de la presente ley. En caso de que el responsable no esté en condiciones de identificar al titular, no se aplicarán los artículos relativos al ejercicio de derechos de los</li> </ol>



<p>artículos 18 al 23, salvo que el titular facilite información adicional que permita su identificación.</p> <p>3. El responsable del tratamiento facilitará al titular información relativa a sus actuaciones sobre la base de una solicitud de ejercicio de derechos, dentro de los 15 días hábiles contados a partir del día siguiente a la fecha de su recibo.</p> <p>Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al titular los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.</p> <p>Cuando el titular presente la solicitud por medios electrónicos, la información se facilitará por dichos medios cuando sea posible, a menos que el titular solicite que se facilite de otro modo que no represente una carga desproporcionada para el responsable.</p> <p>4. El responsable del tratamiento tiene la obligación de contestar las solicitudes de ejercicio de derechos de forma completa y de fondo. En todas las contestaciones de ejercicio de derechos, se deberá informar la posibilidad de presentar una queja ante la autoridad de protección de datos.</p> <p><b><u>La potestad de presentar queja ante la autoridad debe estar sujeta al agotamiento previo de reclamación directa ante el responsable de los datos con el fin de obtener una solución eficiente de la solicitud.</u></b></p> <p>5. La información facilitada en virtud de los artículos 14 y 15, así como cualquier comunicación correspondiente a los ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, serán a título gratuito.</p> <p>Para tal efecto, se podrá considerar reiterativo el ejercicio del derecho de acceso en más de una ocasión en menos de un mes, a menos que exista causa legítima para ello. El responsable deberá demostrar a la autoridad de protección de datos, cuando ésta así lo requiera, que la conducta del titular es carente de fundamento legal, temeraria y/o reiterativa.</p>	<p>6. Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad del titular que radicó una solicitud de ejercicio de derechos, podrá requerir a éste información adicional necesaria para confirmar su identidad.</p> <p>7. La información que deba facilitarse a los titulares en virtud de los artículos 14 y 15 podrá compartirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. Los responsables tendrán en cuenta a los titulares con discapacidades.</p> <p>8. La Autoridad de protección de datos establecerá las reglas, símbolos e imágenes mediante las cuales el responsable del tratamiento o el encargado podrán dar cumplimiento al deber de información, comunicación de políticas de tratamiento de la información, divulgación de información sobre seguridad de datos, notificación de derechos de los titulares de datos, así como otras circunstancias en las que sea necesario su aplicación.</p> <p><b>ARTÍCULO 14. Información que deberá facilitarse cuando los datos personales se obtengan del titular.</b></p> <p>1. Cuando se obtienen de un titular datos personales relativos a este, el responsable del tratamiento, en el momento en que estos se obtienen, le facilitará la información <b>requerida, específica y separada que se describe</b> a continuación:</p> <ul style="list-style-type: none"> <li>a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.</li> <li>b) Los datos de contacto del oficial de protección de datos o área encargada de la protección de datos personales.</li> <li>c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.</li> <li>d) Los destinatarios de los datos personales, si los hubiera.</li> <li>e) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización</li> </ul>
<p>internacional y la existencia o ausencia de una declaración de nivel adecuado de protección de la autoridad de protección de datos. En los casos de las transferencias indicadas en los artículos 49 o 51, la información referente a las garantías adecuadas o apropiadas, y los medios para obtener una copia de estas o al hecho de que se hayan prestado.</p> <ul style="list-style-type: none"> <li>f) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.</li> <li>g) La descripción y ejercicio de los derechos que le asisten al titular.</li> <li>h) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación.</li> <li>i) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.</li> <li>j) Cuando la <b>cesión</b> de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles consecuencias de no facilitar tales datos.</li> <li>k) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.</li> </ul> <p>2. Cuando el responsable proyecte uno o varios tratamientos de datos personales con finalidades diferentes a las iniciales, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 1 del presente artículo.</p> <p>3. Las disposiciones de los numerales 1 y 2 no serán aplicables en la medida en que el titular ya disponga de la información y exista prueba de ello.</p> <p><b>ARTÍCULO 15. Información que deberá facilitarse cuando los datos</b></p>	<p><b>personales no se hayan obtenido del titular.</b></p> <p>1. Cuando los datos personales no se hayan obtenido del titular, el responsable del tratamiento le facilitará a este la siguiente información:</p> <ul style="list-style-type: none"> <li>a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.</li> <li>b) Los datos de contacto del <b>oficial</b> de protección de datos o área encargada de datos personales.</li> <li>c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.</li> <li>d) Las categorías de datos personales de que se trate.</li> <li>e) Los destinatarios de los datos personales, si aplica.</li> <li>f) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel de adecuado de protección de la autoridad de protección de datos, o, en el caso de las transferencias indicadas en la presente ley referente a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.</li> <li>g) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.</li> <li>h) La descripción y ejercicio de los derechos que le asisten al titular.</li> <li>i) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación.</li> <li>j) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.</li> <li>k) Cuando la <b>cesión</b> de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles consecuencias de <b>no</b> facilitar tales datos.</li> </ul>

<p>l) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.</p> <p>2. El responsable del tratamiento facilitará al titular la información indicada en el numeral 1:</p> <ol style="list-style-type: none"> <li>Dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se trate dichos datos.</li> <li>Si los datos personales han de utilizarse para comunicación con el titular, a más tardar en el momento de la primera comunicación a dicho titular.</li> <li>Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.</li> </ol> <p>3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 2.</p> <p>4. Las disposiciones de los apartados 1 a 4 no serán aplicables en la medida en que:</p> <ol style="list-style-type: none"> <li>El titular ya disponga de la información.</li> <li>La comunicación de dicha información resulte imposible o suponga una carga desproporcionada, en particular para el tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística, a reserva de las condiciones y garantías indicadas en la presente ley, o en la medida en que la obligación mencionada en el numeral 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos y garantías fundamentales del titular, inclusive haciendo pública la información.</li> <li>La obtención o la <b>cesión</b> esté expresamente establecida por la legislación nacional que se aplique al responsable del</li> </ol>	<p>tratamiento y que establezca medidas adecuadas para proteger los derechos y garantías fundamentales del titular.</p> <p>d) Cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por la legislación nacional.</p> <p><b>ARTÍCULO 16. Aviso de privacidad</b></p> <ol style="list-style-type: none"> <li>Cuando los datos personales sean obtenidos del titular, el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en la presente ley, facilitando al titular la información básica a la que se refiere el numeral siguiente e indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata al resto de la información.</li> <li>La información básica a la que se refiere el numeral anterior deberá contener, al menos:             <ol style="list-style-type: none"> <li>La identidad del responsable del tratamiento y de su representante legal, si aplica.</li> <li>La finalidad del tratamiento.</li> <li>La posibilidad de ejercer los derechos establecidos en los artículos 18 al 27 de la presente ley.</li> </ol> <p>Si los datos obtenidos del titular fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el titular deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre éste o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 25 de la presente ley.</p> </li> <li>Cuando los datos personales no hubieran sido obtenidos del titular, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 de la presente ley facilitando a aquel la información básica señalada en el numeral anterior, indicando una dirección electrónica u otro medio que permita acceder de forma sencilla</li> </ol>
<p>e inmediata a la restante información. En estos supuestos, la información básica incluirá también:</p> <ol style="list-style-type: none"> <li>Las categorías de datos objeto de tratamiento.</li> <li>Las fuentes de las que procedieron los datos.</li> </ol> <p style="text-align: center;"><b>CAPÍTULO II</b></p> <p style="text-align: center;"><b>EJERCICIO DE LOS DERECHOS</b></p> <p><b>ARTÍCULO 17. Disposiciones generales sobre ejercicio de los derechos.</b></p> <ol style="list-style-type: none"> <li>Los derechos reconocidos en la presente ley, podrán ejercerse directamente o con el acompañamiento de los apoyos señalados en la ley 1996 de 2019 y la ley 1306 de 2009 o cualquier norma que la adicione, modifique o sustituya, o por medio de representante legal.</li> <li>El responsable del tratamiento estará obligado a informar al titular sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el titular. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar por otro medio y deberá redirigirse al área encargada de atender de fondo la solicitud presentada por el titular.</li> <li>El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los titulares de sus derechos si así se estableciera en el contrato o acto jurídico que les vincule. En ningún caso ello significa pérdida de la responsabilidad que recae en el responsable del tratamiento.</li> <li>La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulada por el titular recaerá sobre el responsable.</li> <li>Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en la presente ley, se aplicará lo dispuesto en aquellas.</li> </ol>	<ol style="list-style-type: none"> <li>En cualquier caso, los titulares de la patria potestad o representante legal podrán ejercitar en nombre y representación de los menores de edad los derechos de acceso, rectificación, cancelación, oposición o cualquier otro que pudieran corresponderles en el contexto de la presente ley, respetando siempre el interés superior del menor y su derecho a ser escuchado o expresar su opinión en función de su edad y madurez.</li> <li>Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en la presente ley.</li> <li>El ejercicio de uno o varios de los derechos no afectará negativamente al titular para el ejercicio de los demás derechos y garantías contenidos en esta norma siempre que ello fuere posible.</li> </ol> <p><b>ARTÍCULO 18. Derecho de acceso.</b></p> <ol style="list-style-type: none"> <li>El titular tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, el derecho de acceso a tales datos, y entre otra, a la siguiente información:             <ol style="list-style-type: none"> <li>Los fines del tratamiento.</li> <li>Las categorías de datos personales de que se trate.</li> <li>Los destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales.</li> <li>El plazo previsto de conservación de los datos personales o, en su defecto, los criterios utilizados para determinar este plazo.</li> <li>La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al titular, u oponerse a dicho tratamiento.</li> <li>El derecho a presentar una queja ante la autoridad de protección de datos.</li> <li>Cuando los datos personales no se hayan obtenido del titular, cualquier información disponible sobre su origen.</li> <li>La existencia de decisiones automatizadas, incluida la</li> </ol> </li> </ol>



<p>elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.</p> <ol style="list-style-type: none"> <li>2. Cuando se transfieran datos personales a tercer país u organización internacional, el titular tendrá derecho a ser informado de las garantías adecuadas relativas a la transferencia en virtud de la presente ley.</li> <li>3. El responsable del tratamiento facilitará al titular una copia de los datos personales objeto de tratamiento. Cuando el titular presente la solicitud por medios electrónicos, a menos que solicite expresamente otro método de entrega, la información se facilitará en un formato electrónico de uso común. La entrega de la información no afectará negativamente los derechos y garantías de otras personas naturales.</li> </ol> <p><b>ARTÍCULO 19. Derecho de rectificación.</b></p> <ol style="list-style-type: none"> <li>1. El titular tendrá derecho a obtener del responsable del tratamiento, la rectificación en condiciones de equidad de los datos personales inexactos, parciales, incompletos, fraccionados o que induzcan a error que le concierne, teniendo en cuenta los fines del tratamiento.</li> <li>2. En el caso de solicitudes relacionadas con situaciones que tengan consecuencias jurídicas significativas, el responsable del tratamiento podrá requerir pruebas que respalden la inexactitud de los datos, sin que esto suponga una carga desproporcionada para el titular.</li> </ol> <p><b>ARTÍCULO 20. Derecho de supresión.</b></p> <ol style="list-style-type: none"> <li>1. El titular tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le concierne, el cual estará obligado a suprimir los datos personales cuando concurra alguna de las siguientes circunstancias:             <ol style="list-style-type: none"> <li>a) Los datos personales ya no serán necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.</li> <li>b) El titular retire el consentimiento en que se basa el tratamiento de conformidad con la presente ley y este no se fundamente en otra base legitimadora.</li> <li>c) El titular se oponga al tratamiento con arreglo a la presente ley y no prevalezcan otros motivos legítimos.</li> </ol> </li> </ol>	<ol style="list-style-type: none"> <li>d) Los datos personales hayan sido tratados ilícitamente.</li> <li>e) Los datos personales deben suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.</li> <li>f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de edad mencionados en la presente ley.</li> <li>g) La autoridad de protección de datos determine que en el tratamiento ha incurrido en conductas contrarias a la Constitución o la presente ley.</li> </ol> <ol style="list-style-type: none"> <li>2. Cuando haya cedido los datos personales y esté obligado, en virtud de lo dispuesto en el numeral 1, a suprimir dichos datos, el responsable del tratamiento teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los destinatarios o terceros que estén tratando los datos personales de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.</li> <li>3. Los numerales 1 y 2 no se aplicarán cuando el tratamiento sea necesario:             <ol style="list-style-type: none"> <li>a) Para ejercer el derecho a la libertad de expresión e información.</li> <li>b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la ley que se aplique al responsable del tratamiento, o para el cumplimiento de una función realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.</li> <li>c) Por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 10, numeral 2, literales h) e i), y numeral 3 de la presente ley.</li> <li>d) Con fines de archivo en interés público, investigación científica, o estadística, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.</li> <li>e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.</li> <li>f) <b><u>Para la conservación de los datos personales en el desarrollo del derecho a la seguridad social y a la obligación legal de</u></b></li> </ol> </li> </ol>
<p><b><u>conservación que tienen las entidades que hacen parte de este sistema.</u></b></p> <p><b>ARTÍCULO 21. Derecho a la limitación del tratamiento.</b></p> <ol style="list-style-type: none"> <li>1. El titular tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las siguientes condiciones:             <ol style="list-style-type: none"> <li>a) El titular impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.</li> <li>b) El tratamiento sea ilícito y el titular se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.</li> <li>c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de reclamos administrativos o judiciales.</li> <li>d) El titular se haya opuesto al tratamiento en virtud de la presente ley, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular.</li> </ol> </li> <li>2. Cuando el tratamiento de datos personales se haya limitado en virtud del numeral 1, dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del titular; o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales; o con miras a la protección de los derechos de otra persona natural o jurídica o por razones de interés público.</li> <li>3. Todo titular que haya obtenido la limitación del tratamiento con arreglo al numeral 1, será informado por el responsable antes del levantamiento de dicha limitación.</li> </ol> <p><b>ARTÍCULO 22. Obligación de notificar la rectificación o supresión de datos personales o la limitación del tratamiento.</b></p> <p>El responsable del tratamiento notificará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo a esta ley, a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado y</p>	<p>esté en condición de demostrarlo. El responsable informará al titular acerca de dichos destinatarios, si éste así lo solicita.</p> <p><b>ARTÍCULO 23. Derecho a la portabilidad de los datos.</b></p> <ol style="list-style-type: none"> <li>1. El titular tendrá derecho a recibir los datos personales que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común, lectura mecánica e interoperable y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:             <ol style="list-style-type: none"> <li>a) El tratamiento esté basado en el consentimiento o en un contrato con arreglo a esta ley.</li> <li>b) El tratamiento se efectúe por medios automatizados.</li> </ol> </li> <li>2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.</li> <li>3. El ejercicio del derecho mencionado en el numeral 1 del presente artículo se entenderá sin perjuicio de lo dispuesto en esta ley. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una función realizada en interés público, en el ejercicio de poderes o funciones públicas conferidas al responsable del tratamiento.</li> <li>4. El derecho mencionado en el numeral 1 no afectará negativamente los derechos y garantías de otras personas naturales.</li> <li>5. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.</li> </ol> <p><b>ARTÍCULO 24. Derecho de oposición.</b></p>

<p>1. El titular tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de un tratamiento basado en lo dispuesto en esta ley, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las garantías del titular, o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.</p> <p>2. Cuando el tratamiento de datos personales tenga por objeto marketing y publicidad directa, el titular tendrá derecho a oponerse en todo momento al tratamiento de sus datos personales, incluida la elaboración de perfiles en la medida en que esté relacionada con marketing y publicidad. Cuando el titular se oponga al tratamiento con fines de marketing y publicidad directa, los datos personales dejarán de ser tratados para tal fin.</p> <p>3. A más tardar en el momento de la primera comunicación con el titular, el derecho indicado en los numerales 1 y 2 será mencionado explícitamente al titular y será presentado claramente y al margen de cualquier otra información.</p> <p>4. En el contexto de la utilización de servicios de la sociedad de la información, el titular podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.</p> <p>5. Cuando los datos personales se traten con fines de investigación científica, histórica o estadística, el titular tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de sus datos personales, salvo que sea necesario, para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas.</p> <p><b>ARTÍCULO 25. Decisiones individuales automatizadas, incluida la elaboración de perfiles.</b></p> <p>1. Todo titular tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, en los que no medie</p>	<p>intervención humana alguna, incluida la elaboración de perfiles, que le produzca efectos jurídicos o le afecte significativamente de modo similar.</p> <p>2. El numeral 1 no se aplicará, si la decisión:</p> <ul style="list-style-type: none"> <li>a) Es necesaria para la celebración o la ejecución de un contrato entre el titular y un responsable del tratamiento.</li> <li>b) Está autorizada por una ley que se aplique al responsable del tratamiento, siempre que se establezcan medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.</li> <li>c) Se basa en el consentimiento explícito del titular.</li> </ul> <p>3. En los casos a que se refiere el numeral 2, literales a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y garantías fundamentales del titular, como mínimo el derecho a obtener intervención humana por parte del responsable, expresar su punto de vista, recibir una explicación de la decisión e impugnar la decisión.</p> <p>4. Las decisiones a las que se refiere el numeral 2, no se basarán en datos sensibles contemplados en esta ley, salvo que se apliquen las excepciones previstas en la presente ley y se hayan tomado medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.</p> <p><b>ARTÍCULO 26. Derecho a presentar una queja ante la autoridad de protección de datos.</b></p> <p>1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley, tendrá derecho a presentar una queja ante la autoridad de protección de datos.</p> <p>2. El titular o quien represente sus intereses sólo podrá elevar queja ante la autoridad de protección de datos, una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de una solicitud previa, con ejercicio de derechos, ante el responsable o el encargado según sea el caso siempre que, habiendo transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de existir respuesta, esta no satisfaga los intereses del</p>
<p>titular.</p> <p><b>ARTÍCULO 27. Derecho a presentar una denuncia ante la Autoridad de protección de datos.</b></p> <p>1. Quien tenga conocimiento sobre hechos que deriven en el posible incumplimiento de las disposiciones establecidas en esta ley, tendrá derecho a presentar una denuncia ante la autoridad de protección de datos, persiguiendo la protección del interés colectivo y el derecho a la protección de los datos personales.</p> <p>2. La denuncia podrá presentarse a nombre propio o de forma anónima. Si quien presenta la denuncia solicita a la autoridad de protección de datos la reserva de su identidad, ésta deberá adoptar las medidas técnicas necesarias para evitar a terceros conocer los datos personales del denunciante.</p> <p>3. La autoridad de protección de datos tendrá la obligación de examinar integralmente las denuncias presentadas por los ciudadanos. Con base en los hechos presentados, los documentos aportados y las indagaciones preliminares que realice, determinará si existe mérito o no para iniciar una investigación administrativa y, como resultado de ellas, establecerá las medidas que sean necesarias para hacer efectivo el derecho a la protección de los datos personales conforme a lo establecido en la presente ley.</p> <p style="text-align: center;"><b>TITULO III</b></p> <p style="text-align: center;"><b>RESPONSABLE DEL TRATAMIENTO Y ENCARGADO DEL TRATAMIENTO</b></p> <p style="text-align: center;"><b>CAPÍTULO I</b></p> <p style="text-align: center;"><b>OBLIGACIONES GENERALES</b></p> <p><b>ARTÍCULO 28. Deberes del responsable del tratamiento.</b></p> <p>Los responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <p>1. Aplicar los principios contemplados en la presente ley en el tratamiento</p>	<p>de datos personales.</p> <p>2. Establecer una base jurídica que legitime el tratamiento de datos personales de acuerdo con lo establecido en el artículo 6 de la presente ley.</p> <p>3. Implementar medidas de seguridad de conformidad con el artículo 35, a fin de garantizar y demostrar que el tratamiento es conforme con la presente ley. Revisar y actualizar dichas medidas cuando sea necesario.</p> <p>4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley.</p> <p>5. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos a lo que haya tenido acceso y adoptar las demás medidas necesarias para que la información suministrada a este, se mantenga actualizada.</p> <p>6. Garantizar el pleno ejercicio de los derechos que le conciernen a los titulares en los términos previstos en los artículos 18 al 27 de la presente ley y en las demás normas que la modifiquen o adicionen.</p> <p>7. Cumplir con el deber de información contenido en los artículos 14 y 15 de la presente ley</p> <p>8. Notificar a la autoridad de protección de datos, cuando se presenten incidentes de seguridad de conformidad con el artículo 36 de la presente ley.</p> <p>9. Comunicar los incidentes de seguridad, cuando sea el caso, a los titulares afectados de conformidad con el artículo 37 de la presente ley.</p> <p>10. Cumplir las instrucciones y requerimientos que imparta la autoridad de protección de datos.</p> <p>11. Elaborar evaluaciones de impacto sobre la privacidad, cuando sea el caso, en los términos descritos en el artículo 38 de la presente ley.</p> <p>12. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.</p> <p>13. Llevar un registro de las actividades del tratamiento en los términos descritos en el artículo 33 de la presente ley.</p> <p>14. Realizar una revisión interna o externa, a los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, al menos cada dos años, para verificar el cumplimiento de la presente ley.</p> <p>Con carácter extraordinario deberá realizarse dicha revisión siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de la presente ley. Con dicha</p>

<p>revisión se reiniciará el cómputo de los dos años señalados en el inciso anterior.</p> <ol style="list-style-type: none"> <li>15. Cooperar con la autoridad de protección de datos cuando lo solicite.</li> <li>16. Elegir un encargado o encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla con los requisitos establecidos en el artículo 32 de la presente ley y garantice la protección de los derechos del titular.</li> <li>17. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.</li> <li>18. Demostrar el cumplimiento del código de conducta al que se haya adherido, de conformidad con el artículo 42 de la presente ley.</li> <li>19. Mantener los compromisos que le ha permitido acceder a un mecanismo de certificación de certificación en los términos descritos en el artículo 45 de la presente ley.</li> </ol> <p><b>ARTÍCULO 29. Deberes del encargado del tratamiento.</b></p> <p>Los encargados del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <ol style="list-style-type: none"> <li>1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.</li> <li>2. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe alguno de los principios contemplados en la presente ley o cualquier otra disposición en materia de protección, informará inmediatamente al responsable.</li> <li>3. Utilizar los datos personales objeto de tratamiento, sólo para la finalidad del encargo. En ningún caso podrá utilizar los datos para fines propios.</li> <li>4. Llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, de conformidad con el artículo 33 de la presente ley.</li> <li>5. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento.</li> <li>6. No subcontratar ninguna de las prestaciones que formen parte del encargo, salvo que cuente con autorización expresa del responsable.</li> <li>7. Mantener el deber de secreto respecto a los datos de carácter personal a</li> </ol>	<p>los que haya tenido acceso en virtud del encargo, incluso después de que finalice el mismo.</p> <ol style="list-style-type: none"> <li>8. Garantizar que el personal, con acceso a datos personales objeto del encargo reciba formación sobre protección de datos y se comprometa por escrito a mantener la confidencialidad y cumplir con las medidas de seguridad. El encargado debe mantener a disposición del responsable y/o la autoridad competente, la documentación que demuestre el cumplimiento de estas obligaciones.</li> <li>9. El encargado informará al responsable del tratamiento, sobre cualquier incidente de seguridad relacionado con los datos personales objeto del tratamiento, proporcionando toda la información pertinente necesaria para documentar y notificar el incidente a la autoridad de protección de datos.</li> <li>10. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.</li> <li>11. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.</li> <li>12. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando sea el caso, de conformidad con el artículo 38 de la presente ley.</li> <li>13. Poner a disposición del responsable o de la Autoridad de Protección de Datos, toda la información necesaria para demostrar el cumplimiento de sus obligaciones.</li> <li>14. Implantar las medidas de seguridad acordadas con el responsable del tratamiento, así como aquellas que correspondan en función del riesgo asociado a la prestación del servicio.</li> <li>15. Eliminar o devolver al responsable del tratamiento los datos personales, así como los soportes en los que estén almacenados, una vez finalizada la prestación del servicio. La devolución debe incluir la eliminación completa de los datos almacenados en los equipos informáticos utilizados por el encargado, a menos que existan excepciones legales y/o contractuales.</li> <li>16. Cooperar con la autoridad de protección de datos cuando lo solicite.</li> </ol> <p><b>ARTÍCULO 30. Protección de datos desde el diseño y por defecto.</b></p> <ol style="list-style-type: none"> <li>1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los</li> </ol>
<p>derechos y garantías de las personas naturales, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos de la presente ley y proteger los derechos de los titulares.</p> <ol style="list-style-type: none"> <li>2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles.</li> </ol> <p>Tendrá acceso únicamente el personal autorizado, salvo que se modifique en razón de las circunstancias del tratamiento.</p> <ol style="list-style-type: none"> <li>3. Para el cumplimiento de lo establecido en los numerales 1 y 2, el responsable del tratamiento tendrá en cuenta:       <ol style="list-style-type: none"> <li>a) La protección de los datos personales de forma proactiva y no reactiva.</li> <li>b) La protección de los datos personales preventiva y no correctiva.</li> <li>c) La privacidad como configuración predeterminada.</li> <li>d) La protección de los datos en el ciclo de vida completo de su tratamiento, es decir, desde la recolección hasta su posible supresión.</li> <li>e) La transparencia en el tratamiento de los datos.</li> <li>f) La prevalencia de la privacidad como interés del titular.</li> </ol> </li> <li>4. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 60, como elemento que acredite el cumplimiento de las obligaciones establecidas en los numerales 1 y 2 del presente artículo.</li> </ol> <p><b>ARTÍCULO 31. Corresponsables del tratamiento.</b></p> <ol style="list-style-type: none"> <li>1. Cuando dos o más responsables determinen conjuntamente los fines y</li> </ol>	<p>los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo, sus respectivas responsabilidades en el cumplimiento de las obligaciones impuestas por la presente ley, en particular, en el ejercicio de los derechos de los titulares y sus obligaciones de suministro de información, a las cuales se refiere la presente ley.</p> <ol style="list-style-type: none"> <li>2. El acuerdo indicado en el numeral 1, reflejará adecuadamente las funciones y relaciones respectivas de los corresponsables en relación con los titulares. Se pondrán a disposición del titular los aspectos esenciales del acuerdo.</li> <li>3. Independientemente de los términos del acuerdo a que se refiere el numeral 1, los titulares podrán ejercer los derechos que les reconoce la presente ley frente a cada uno de los responsables.</li> </ol> <p><b>ARTÍCULO 32. Encargado del tratamiento.</b></p> <ol style="list-style-type: none"> <li>1. El encargado del tratamiento no recurrirá a otro encargado sin la autorización, específica o general, del responsable ya sea por escrito o por mensajes de datos suficientes y verificables.       <p>Cuando la autorización para el subencargo del tratamiento sea general, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.</p> </li> <li>2. El tratamiento debe regirse por un contrato u otro acto jurídico con arreglo a las leyes civiles o mercantiles, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza, la finalidad del tratamiento, el tipo de titulares, categorías de datos personales, las obligaciones y los derechos del responsable. Dicho contrato estipulará, en particular, que el encargado:       <ol style="list-style-type: none"> <li>a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país u organización internacional, salvo que esté obligado a ello en virtud de un mandato legal que se aplique al encargado. En tal caso, el encargado informará al responsable de esa exigencia</li> </ol> </li> </ol>

<p>legal previa al tratamiento, salvo que dicho mandato lo prohíba por razones importantes de interés público.</p> <p>b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza contractual.</p> <p>c) Tomará todas las medidas necesarias de conformidad a la presente ley.</p> <p>d) Respetará las condiciones indicadas en la presente ley para recurrir a un subencargado del tratamiento.</p> <p>e) Asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los titulares o podrá comprometerse a resolver, por cuenta del responsable y dentro de los plazos establecidos en esta ley, las solicitudes de ejercicio de derechos.</p> <p>f) Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en la presente ley, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.</p> <p>g) A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud de una disposición legal o por motivos de responsabilidad derivada de su relación.</p> <p>h) Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.</p> <p>3. El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe la presente ley u otras disposiciones en materia de protección de datos.</p> <p>4. Cuando un encargado del tratamiento recurra a un subencargado para</p>	<p>llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este subencargado, las mismas obligaciones de protección de datos que las estipuladas en el contrato entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones de la presente ley. Si el subencargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo que respecta al cumplimiento de las obligaciones del otro.</p> <p>5. La adhesión del encargado y/o subencargado del tratamiento a un código de conducta aprobado o a un mecanismo de certificación aprobado como lo indica esta ley, podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a las que se refiere el presente artículo.</p> <p>6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato que menciona los numerales 2 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales modelo, las cuales hacen alusión a los numerales 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable, encargado o subencargado de conformidad con esta ley.</p> <p>7. La autoridad de protección de datos podrá fijar cláusulas contractuales modelo, para los contratos a los que hacen mención los numerales 2 y 4 del presente artículo.</p> <p>8. El contrato al cual se refieren los numerales 2 y 4 deberá constar por escrito, inclusive en formato electrónico.</p> <p>9. Sin perjuicio de lo dispuesto en esta ley, si un encargado o subencargado del tratamiento infringe la presente ley, al determinar los fines y medios del tratamiento, será considerado responsable con respecto a dicho tratamiento.</p> <p>10. El responsable del tratamiento podrá exigir a los encargados que sean proveedores de servicios tecnológicos, aplicaciones e infraestructura tecnológica, con los que esté adherido o se vaya a adherir a través de condiciones generales de contratación, que demuestre el cumplimiento de la presente ley. En caso de que el proveedor ignore las solicitudes realizadas por los responsables o incumpla con la presente ley, los responsables podrán denunciar dicha situación ante la autoridad de</p>
<p>protección de datos, de conformidad con lo establecido en el artículo 27 de la presente ley.</p> <p>Lo anterior no exonera al responsable del tratamiento del cumplimiento de las obligaciones establecidas en el artículo 28 de la presente ley.</p> <p><i>Parágrafo primero.</i> Las obligaciones establecidas en esta ley para los encargados del tratamiento serán de aplicación directa para quienes, en atención a lo dispuesto en los numerales 2 y 4 del presente artículo, adquieran la calidad de subencargados.</p> <p><i>Parágrafo segundo.</i> El encargado del tratamiento y cualquier persona que actúe bajo el control del responsable o del encargado y tenga acceso a datos personales, sólo podrán tratar dichos datos siguiendo instrucciones del responsable, a menos que no estén obligados a ello en virtud de una disposición legal.</p> <p><b>ARTÍCULO 33. Registro de las actividades de tratamiento.</b></p> <p>1. Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su control. Dicho registro deberá contener toda la información indicada a continuación:</p> <p>a) El nombre y los datos de contacto del responsable y, cuando sea el caso, del corresponsable, y del oficial de protección de datos o área encargada.</p> <p>b) Los fines del tratamiento.</p> <p>c) Una descripción de los tipos de titulares y de las categorías de datos personales.</p> <p>d) Los destinatarios a quienes se cedieron o cederán los datos personales, incluidos los destinatarios en otros países u organizaciones internacionales.</p> <p>e) Los encargados que intervienen en el tratamiento.</p> <p>f) De ser procedente, las transferencias de datos personales a otro país o una organización internacional, incluida la identificación de dicho país u organización internacional y, en el caso de las transferencias indicadas en el artículo 33 de la presente ley esta ley relativa a la documentación de garantías adecuadas.</p> <p>g) Cuando sea posible, los plazos previstos para la supresión de las</p>	<p>diferentes categorías de datos.</p> <p>h) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la remisión al documento que las contenga.</p> <p>i) Los responsables del tratamiento, deben inscribir sus registros de actividades ante el Registro Nacional de las Actividades, administrado por la autoridad de protección de datos y de libre consulta para los ciudadanos.</p> <p>2. Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:</p> <p>a) El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y del oficial de protección de datos o área encargada.</p> <p>b) Las categorías de tratamientos efectuados por cuenta de cada responsable.</p> <p>c) Los subencargados autorizados por el responsable, que intervienen en el tratamiento.</p> <p>d) De ser procedente, las transferencias de datos personales a otro país u organización internacional, incluida la identificación de dicho país u organización internacional y en el caso de las transferencias indicadas en esta ley, relativo a la documentación de garantías adecuadas.</p> <p>e) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la remisión al documento que las contenga.</p> <p>3. Los registros a los que se refieren los numerales 1 y 2 constarán por escrito, inclusive en formato electrónico.</p> <p>4. El responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de protección de datos, cuando lo requiera.</p> <p>5. Los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas, harán público el registro de sus actividades de tratamiento accesible por medios electrónicos, en el que constará la</p>

información establecida en el presente artículo.

**ARTÍCULO 34. Bloqueo de los datos.**

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.
2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los Jueces y Tribunales, Fiscalía General de la Nación o las Administraciones Públicas competentes, en particular de la autoridad de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo, se procederá a la destrucción de los datos.
3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.
4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información, de manera que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.
5. La autoridad de protección de datos, dentro del ámbito de sus competencias, podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de titulares afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los titulares, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

**CAPÍTULO II**

**SEGURIDAD DE LOS DATOS**

**ARTÍCULO 35. Seguridad del tratamiento.**

1. En caso de incidente de seguridad de los datos personales, el responsable del tratamiento lo notificará a la autoridad de protección de datos de conformidad con esta ley, sin demora injustificada y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicho incidente de seguridad constituya un riesgo para los derechos y las garantías de las personas naturales. Si la notificación a la autoridad de protección de datos no tiene lugar en el plazo de 72 horas, deberá ir acompañada de los motivos que expliquen la dilación.
2. El encargado del tratamiento notificará, sin demora injustificada, al responsable del tratamiento, los incidentes de seguridad de los datos personales de los que tenga conocimiento.
3. La notificación contemplada en el numeral 1 deberá, como mínimo:
  - a) Describir la naturaleza del Incidente de seguridad de los datos personales y, cuando sea posible, el número aproximado, tipo de titulares afectados, las categorías de datos y el número aproximado de registros de datos personales afectados.
  - b) Comunicar el nombre y los datos de contacto del oficial de protección de datos o de otro punto de contacto, en el que pueda obtenerse más información.
  - c) Describir las posibles consecuencias del incidente de seguridad de los datos personales.
  - d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento, para poner remedio al incidente de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
4. Si no fuera posible facilitar la información descrita en el numeral 3 del presente artículo, simultáneamente con la notificación de un incidente de seguridad, y en la medida que esta condición persista, la información se facilitará de manera gradual sin demora injustificada.
5. El responsable del tratamiento documentará cualquier incidente de seguridad de los datos personales, incluidos los hechos relacionados con este, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de protección de datos, verificar el cumplimiento de lo dispuesto en el presente artículo.
6. Los datos personales contenidos en la notificación de un incidente de seguridad y que fueron comunicados a la autoridad de protección de

1. Teniendo en cuenta el estado de la técnica, los costos de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad, variables para los derechos y garantías de los titulares, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
  - a) La seudonimización y el cifrado de datos personales.
  - b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
  - c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
  - d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
2. Al evaluar la adecuación del nivel de seguridad, se tendrá en cuenta los riesgos que presente el tratamiento de datos, en particular, la destrucción, pérdida, alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales.
3. La adhesión a un código de conducta aprobado de conformidad con el artículo 42 o a un mecanismo de certificación aprobado de conformidad con el artículo 45, así como, la adopción de directrices dadas por la autoridad de protección de datos o indicaciones proporcionadas por un oficial de protección de datos podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el numeral 1 del presente artículo.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales, sólo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello por la ley.

**ARTÍCULO 36. Notificación de un Incidente de seguridad de los datos personales a la autoridad de protección de datos.**

datos, proveedores de tecnologías y servicios de seguridad, podrán ser tratados exclusivamente durante el tiempo y alcance necesario para su análisis, detección, protección y respuesta ante el incidente, adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

**ARTÍCULO 37. Comunicación de un Incidente de seguridad de los datos personales al titular.**

1. Cuando sea probable que el incidente de seguridad de los datos personales entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento lo comunicará al titular sin demora injustificada.
2. La comunicación al titular contemplada en el numeral 1 del presente artículo, deberá describir en un lenguaje claro y sencillo la naturaleza del incidente de seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 36, numeral 3, literales b), c) y d).
3. La comunicación al titular a la que se refiere el numeral 1, no será necesaria si se cumple alguna de las siguientes condiciones:
  - a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por el incidente de seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.
  - b) El responsable del tratamiento ha tomado medidas ulteriores que garantizan que ya no exista la probabilidad de que se materialice el alto riesgo para los derechos y garantías del titular.
4. Cuando la comunicación a los titulares suponga un esfuerzo desproporcionado para el responsable del tratamiento, éste podrá optar por una comunicación pública o una medida de difusión semejante, de manera que se informe efectivamente a los titulares.
5. Cuando el responsable no haya comunicado al titular el incidente de seguridad de los datos personales, la autoridad de protección de datos, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo comunique o podrá confirmar que se cumple



<p>alguna de las condiciones mencionadas en el numeral 3.</p> <p style="text-align: center;"><b>CAPÍTULO III</b></p> <p style="text-align: center;"><b>EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS Y CONSULTA PREVIA</b></p> <p><b>ARTÍCULO 38. Evaluación de impacto relativa a la protección de datos y consulta previa.</b></p> <ol style="list-style-type: none"> <li>1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.</li> <li>2. El responsable del tratamiento solicitará asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.</li> <li>3. La evaluación de impacto relativa a la protección de los datos, a los que se refiere el numeral, 1 se requerirá en especial cuando:             <ol style="list-style-type: none"> <li>a) Se realice evaluación sistemática y exhaustiva de aspectos personales de personas naturales, que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que les afecten significativamente de forma similar.</li> <li>b) Tratamiento a gran escala de datos sensibles o de los datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.</li> <li>c) Observación sistemática a gran escala de una zona de acceso público.</li> <li>d) Se efectúen tratamientos sobre neurodatos.</li> </ol> </li> <li>4. La autoridad de protección de datos establecerá y publicará una lista de los tipos de operaciones de tratamiento, que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el</li> </ol>	<p>numeral 1.</p> <ol style="list-style-type: none"> <li>5. La evaluación a la que se refiere el numeral 1 del presente artículo, deberá incluir como mínimo:             <ol style="list-style-type: none"> <li>a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.</li> <li>b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.</li> <li>c) Una evaluación de los riesgos para los derechos y garantías de los titulares a los que se refiere el numeral 1.</li> <li>d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente ley, teniendo en cuenta los derechos y garantías de los titulares y de otras personas afectadas.</li> </ol> </li> <li>6. El cumplimiento de los códigos de conducta aprobados, a los que se refiere el artículo 38, por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.</li> <li>7. Cuando el tratamiento de datos se base en un deber legal o en un interés público y esté regulado por una ley o normativa específica aplicable al responsable del tratamiento, que detalle la operación específica de tratamiento o conjunto de operaciones, y que ya incluya una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general, los numerales 1 a 6 no se aplicarán, a menos que una ley o normativa posterior lo requiera.</li> <li>8. En caso de ser necesario, el responsable examinará si el tratamiento es conforme a la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.</li> <li>9. El responsable del tratamiento consultará previamente a la autoridad de protección de datos antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. Si la autoridad</li> </ol>
<p>de protección de datos considera que el tratamiento previsto supone un alto riesgo, asesorará por escrito al responsable, y en su caso al encargado, sobre las medidas técnicas y organizativas que se deberán adoptar antes del tratamiento de los datos. La autoridad de protección de datos deberá emitir un concepto en el menor tiempo posible.</p> <p><i>Parágrafo:</i> La zona de acceso público a la que se refiere el numeral 3 literal c) del presente artículo, hace referencia a cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas naturales, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad.</p> <p style="text-align: center;"><b>CAPÍTULO IV</b></p> <p style="text-align: center;"><b>OFICIAL DE PROTECCIÓN DE DATOS</b></p> <p><b>ARTÍCULO 39. Designación del Oficial de protección de datos.</b></p> <ol style="list-style-type: none"> <li>1. El responsable y el encargado del tratamiento designarán un oficial de protección de datos siempre que:             <ol style="list-style-type: none"> <li>a) El tratamiento lo lleve a cabo los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas.</li> <li>b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de los titulares a gran escala.</li> <li>c) Las actividades principales del responsable o del encargado, consistan en el tratamiento a gran escala de datos sensibles y de datos relativos a antecedentes penales, anotaciones judiciales o contravencionales, y/o sanciones administrativas.</li> <li>d) La autoridad de protección de datos podrá definir nuevas indicaciones en las que se deba designar un Oficial de protección de datos y estipulará las condiciones y</li> </ol> </li> </ol>	<p>particularidades para dicha designación.</p> <ol style="list-style-type: none"> <li>2. Un grupo empresarial podrá nombrar un único oficial de protección de datos, siempre que sea fácilmente accesible desde cada una de las empresas que pertenecen al grupo.</li> <li>3. Cuando el responsable o el encargado del tratamiento sea una entidad u organismo público, se podrá designar un único oficial de protección de datos para varias de estas entidades u organismos, teniendo en cuenta su estructura administrativa y tamaño.</li> <li>4. En casos distintos de los contemplados en el numeral 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a sectores a los que pertenezcan los responsables o encargados, podrán designar de forma voluntaria un oficial de protección de datos.</li> <li>5. El oficial de protección de datos será designado siempre que cuente con un perfil legal o un perfil interdisciplinario con conocimientos legales y experiencia en protección de datos. Además, se verificará su capacidad para desempeñar las funciones indicadas en esta ley.</li> <li>6. El oficial de protección de datos podrá vincularse con el responsable o el encargado del tratamiento por medio de un contrato de prestación de servicios o un contrato laboral.</li> <li>7. El responsable o el encargado del tratamiento publicará los datos de contacto del oficial de protección de datos y los comunicará a la autoridad de protección de datos en un plazo de quince (15) días hábiles.</li> </ol> <p>Las designaciones, nombramientos y ceses de los oficiales de protección de datos, tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria, también deberán ser notificadas en el mismo término.</p> <ol style="list-style-type: none"> <li>8. La autoridad de protección de datos, mantendrá en el ámbito de sus competencias, una lista actualizada de oficiales de protección de datos que será accesible a través de medios electrónicos.</li> <li>9. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento, podrán establecer la dedicación completa o a tiempo parcial del oficial, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos y garantías de los titulares.</li> </ol> <p><b>ARTÍCULO 40. Posición del oficial de protección de datos.</b></p>



<p>1. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relacionadas con la protección de datos personales.</p> <p>2. El responsable y el encargado del tratamiento respaldarán al oficial de protección de datos en el desempeño de las funciones estipuladas en la presente ley, facilitando los recursos necesarios para el desempeño de dichas funciones, el acceso a los datos personales y a las operaciones de tratamiento.</p> <p>3. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. El oficial de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.</p> <p>4. Los titulares podrán ponerse en contacto con el oficial de protección de datos, en relación a todas las cuestiones correspondientes al tratamiento de sus datos personales y al ejercicio de sus derechos y garantías al amparo de la presente ley.</p> <p>5. El oficial de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el artículo 74 de la Constitución Política.</p> <p>6. El oficial de protección de datos podrá desempeñar otras funciones y el responsable o encargado del tratamiento garantizará que estas no den lugar a conflicto de intereses.</p> <p>7. El oficial de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la autoridad de protección de datos. El oficial podrá verificar los procedimientos y emitir recomendaciones en el ámbito de sus competencias.</p> <p><b>ARTÍCULO 41. Funciones del oficial de protección de datos.</b></p> <p>1. El oficial de protección de datos tendrá como mínimo las siguientes funciones:</p> <p>a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones que les competen en virtud de la ley y otras</p>	<p>disposiciones referentes a la protección de datos.</p> <p>b) Supervisar el cumplimiento de lo dispuesto en la presente ley.</p> <p>c) Supervisar la implementación y aplicación de un manual interno de políticas y procedimiento en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.</p> <p>d) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto, relativa a la protección de datos y supervisar su aplicación de conformidad con la presente ley.</p> <p>e) Cooperar con la autoridad de protección de datos.</p> <p>f) Actuar como punto de contacto de la autoridad de protección de datos, sobre cuestiones relativas al tratamiento, incluida la consulta previa a la que se refiere el artículo 38, numeral 9, así como solicitar instrucciones, en su caso, sobre cualquier otro asunto.</p> <p>g) Cuando el oficial de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos, lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.</p> <p>2. El oficial de protección de datos, desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.</p> <p style="text-align: center;"><b>CAPÍTULO V</b></p> <p style="text-align: center;"><b>MECANISMOS DE AUTORREGULACIÓN</b></p> <p><b>ARTÍCULO 42. Códigos de conducta.</b></p> <p>1. La Autoridad de protección de datos, promoverá la elaboración de códigos de conducta, destinados a contribuir a la correcta aplicación de la presente ley, teniendo en cuenta las características específicas de las distintas actividades de tratamiento y las necesidades específicas de las microempresas, las pequeñas y medianas empresas.</p> <p>2. Las asociaciones y otras entidades representativas de categorías de responsables o encargados del tratamiento podrán elaborar códigos de</p>
<p>conducta, modificar o ampliar dichos códigos con objeto de especificar la aplicación de la presente ley, en lo que respecta a:</p> <p>a) El tratamiento leal y transparente.</p> <p>b) Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos.</p> <p>c) La recogida de datos personales.</p> <p>d) La seudonimización de datos personales.</p> <p>e) La información proporcionada al público y a los titulares.</p> <p>f) El ejercicio de los derechos de los titulares.</p> <p>g) La información proporcionada a los menores y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o representantes legales del menor.</p> <p>h) Las medidas, procedimientos y las acciones para garantizar la seguridad del tratamiento contenidas en esta ley.</p> <p>i) La notificación de incidentes de seguridad de los datos personales a la autoridad de protección de datos y la comunicación de dichos incidentes a los titulares.</p> <p>j) La transferencia de datos personales a terceros países u organizaciones internacionales.</p> <p>k) Los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos, que permitan resolver las controversias entre los responsables y los titulares relativos al tratamiento, sin perjuicio del derecho presentar una queja ante la autoridad de protección de datos o acudir ante autoridad judicial.</p> <p>3. Los responsables o encargados del tratamiento a los que se aplica la presente ley, así como también, a los que no se aplica, podrán adherirse también a códigos de conducta aprobados de conformidad con el numeral 5 del presente artículo, con el fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales.</p> <p>Los mencionados responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas las relativas a los derechos de los titulares.</p>	<p>4. El código de conducta, contendrá mecanismos que permitan a la entidad supervisora, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados del tratamiento, que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de la autoridad de protección de datos.</p> <p>5. Las asociaciones y otras entidades mencionadas en el numeral 2 del presente artículo, que pretendan elaborar un código de conducta, modificar o ampliar un código existente presentarán el proyecto de código, la modificación o ampliación a la autoridad de protección de datos.</p> <p>La autoridad de protección de datos determinará si el proyecto de código, la modificación o ampliación es conforme con la presente ley y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.</p> <p>6. Si el proyecto de código, la modificación o ampliación es aprobado de conformidad con el numeral 5, la autoridad de protección de datos el código.</p> <p>7. La autoridad de protección de datos llevará un registro de todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.</p> <p><b>ARTÍCULO 43. Supervisión de códigos de conducta aprobados.</b></p> <p>1. Podrá supervisar el cumplimiento de un código de conducta, una entidad que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditada para tal fin por la autoridad de protección de datos, sin perjuicio de las funciones y facultades de esta.</p> <p>2. La autoridad de protección de datos fijará los criterios de acreditación de las entidades a las que se refiere el presente artículo.</p> <p>3. Sin perjuicio de las funciones y las facultades de la autoridad de protección de datos, en virtud del numeral 1 del presente artículo, la entidad acreditada deberá, con sujeción a las garantías del debido proceso, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este.</p> <p>Informará de dichas medidas y sus razones, a la autoridad de protección</p>

<p>de datos.</p> <ol style="list-style-type: none"> <li>La autoridad de protección de datos podrá revocar la acreditación de una entidad de conformidad con el numeral 1, si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicha entidad infringe la presente ley.</li> <li>El presente artículo no se aplicará al tratamiento realizado por autoridades y entidades públicas.</li> </ol> <p><b>ARTÍCULO 44. Deberes de las entidades supervisoras de códigos de conducta.</b></p> <p>Las entidades supervisoras de códigos de conducta deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <ol style="list-style-type: none"> <li>Demostrar, a satisfacción de la autoridad de protección de datos, su independencia y pericia en relación con el objeto del código.</li> <li>Establecer procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación.</li> <li>Establecer procedimientos y estructuras para tratar los reclamos relativos a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, para hacer que estos sean transparentes para los titulares y el público en general.</li> <li>Demostrar, a satisfacción de la autoridad de protección de datos, que sus funciones y objetivos no dan lugar a conflicto de intereses.</li> </ol> <p><b>ARTÍCULO 45. Certificación.</b></p> <ol style="list-style-type: none"> <li>La Autoridad de protección de datos promoverá, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en la presente ley, en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas, las pequeñas y medianas empresas.</li> </ol>	<ol style="list-style-type: none"> <li>Podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados conforme al numeral 5 del presente artículo, con el objetivo de demostrar que los responsables o encargados no sujetos a la presente ley, según lo establecido en el artículo 3, ofrecen garantías adecuadas en el contexto de transferencias internacionales de datos personales a terceros países u organizaciones internacionales, según lo dispuesto en el artículo 49, numeral 2, literal e).</li> </ol> <p>Los responsables o encargados mencionados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas aquellas relativas a los derechos de los titulares.</p> <ol style="list-style-type: none"> <li>La certificación será voluntaria y estará disponible a través de un proceso transparente.</li> <li>La certificación a la que se refiere el presente artículo, no limitará las obligaciones del responsable o encargado del tratamiento en cuanto al cumplimiento de la presente ley y se entenderá sin perjuicio de las funciones y las facultades de la autoridad de protección de datos.</li> <li>La certificación en virtud del presente artículo será expedida por las entidades de certificación o por la autoridad de protección de datos, sobre la base de los criterios aprobados por ésta.</li> <li>Los responsables o encargados que sometan su tratamiento al mecanismo de certificación, darán a la entidad de certificación o en su caso a la autoridad de protección de datos, toda la información y acceso a sus actividades de tratamiento que requieran para llevar a cabo el procedimiento de certificación.</li> <li>La certificación se expedirá a un responsable o encargado del tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes.</li> </ol> <p>La certificación será retirada, cuando proceda, por las entidades de certificación, o en su caso por la autoridad de protección de datos, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la misma.</p> <ol style="list-style-type: none"> <li>La autoridad de protección de datos llevará en un registro todos los mecanismos de certificación, sellos y marcas de protección de datos y los</li> </ol>
<p>pondrá a disposición pública por cualquier medio apropiado.</p> <p><i>Parágrafo primero:</i> Serán entidades certificadoras aquellas que hayan sido acreditadas por un organismo del subsistema nacional de calidad, el cual tenga la pericia necesaria para evaluar si los aspirantes a entidades certificadoras cuentan con un nivel adecuado de competencia en materia de protección de datos.</p> <p><i>Parágrafo segundo:</i> La autoridad de protección de datos hará públicos los requisitos y los criterios a los que se refiere el numeral 5 del presente artículo, en una forma fácilmente accesible.</p> <p><b>ARTÍCULO 46. Deberes de las entidades certificadoras.</b></p> <p>Las entidades certificadoras deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:</p> <ol style="list-style-type: none"> <li>Demostrar ante la autoridad de protección de datos y/o los sujetos interesados en la certificación que se encuentran acreditadas por un organismo del subsistema nacional de calidad.</li> <li>Respetar y cumplir los criterios de certificación aprobados por la autoridad de protección de datos.</li> <li>Establecer procedimientos para la expedición, revisión periódica y retirada de certificaciones, sellos y marcas de protección de datos en los términos descritos en el numeral 7 del artículo 45.</li> <li>Establecer procedimientos y estructuras para tratar los reclamos relativos al retiro de la certificación por el incumplimiento de los requisitos por parte de un responsable o encargado del tratamiento.</li> <li>Informar a la autoridad de protección de datos sobre las razones para la retirada de una certificación a un responsable o encargado del tratamiento.</li> </ol> <p style="text-align: center;"><b>TITULO IV</b></p> <p style="text-align: center;"><b>TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES</b></p> <p><b>ARTÍCULO 47. Regla general de las transferencias.</b></p> <p>Solo se realizarán transferencias de datos personales si, a reserva de las demás disposiciones de la presente ley, el responsable o el encargado del tratamiento</p>	<p>cumplen las condiciones establecidas en el presente título, incluidas las relativas a las transferencias ulteriores de datos personales. Todas las disposiciones del presente título se aplicarán, a fin de asegurar un nivel adecuado en materia de protección de datos personales.</p> <p><i>Parágrafo:</i> Se considera transferencia la salida de datos fuera del territorio nacional, bien sea por cesión de datos, o por un tratamiento de datos personales por parte del encargado del tratamiento.</p> <p><b>ARTÍCULO 48. Transferencias basadas en un nivel adecuado de protección.</b></p> <ol style="list-style-type: none"> <li>Se podrán realizar transferencias de datos personales a países u organismos internacionales que proporcionen niveles adecuados de protección de datos.</li> <li>Se entiende que un tercer país, un territorio, uno o varios sectores específicos del tercer país, o una organización internacional ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Autoridad de Protección de Datos sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a los sujetos obligados. Para emitir una decisión de adecuación, la Autoridad de Protección de Datos deberá tener en cuenta los siguientes elementos:       <ol style="list-style-type: none"> <li>El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales;</li> <li>La legislación vigente, tanto general como sectorial, incluidas las limitaciones y garantías para el acceso de las autoridades públicas a los datos personales;</li> <li>La existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales;</li> <li>La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país u organización que reciba la información, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a las personas Titulares de los datos en el ejercicio de sus derechos, y de cooperar con la Autoridad de Protección de Datos.</li> </ol> </li> </ol>

<p>3. La declaración de nivel adecuado establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. Cuando la información disponible, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado de conformidad con lo dispuesto por el presente artículo, la Autoridad de Protección de Datos, podrá derogar, modificar o suspender, en la medida necesaria y sin efecto retroactivo, la decisión adecuación.</p> <p><i>Parágrafo primero:</i> La autoridad de protección de datos habilitará canales de contacto para que el tercer país u organización internacional, pueda subsanar la situación que dé lugar a la decisión adoptada, de conformidad con el numeral 3.</p> <p><b>ARTÍCULO 49. Transferencias mediante garantías adecuadas.</b></p> <ol style="list-style-type: none"> <li>A falta de declaración de nivel adecuado de protección, en los términos del artículo 48, el responsable o el encargado del tratamiento sólo podrá <b>transferir</b> datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los titulares cuenten con derechos exigibles y acciones legales efectivas.</li> <li>Las garantías adecuadas con arreglo al numeral 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de la autoridad de protección de datos, por:             <ol style="list-style-type: none"> <li>Un instrumento jurídicamente vinculante y exigible, bilateral o multilateral, entre Colombia y otros países u organizaciones internacionales, que habilite las transferencias desde entidades u organismos públicos establecidas en Colombia hacia entidades u organismos públicos establecidas en otros países.</li> <li>Normas corporativas vinculantes de conformidad con el artículo 50 de la presente ley.</li> <li>Cláusulas contractuales modelo. La autoridad de protección de datos, establecerá los criterios bajo los cuales se deben elaborar las cláusulas.</li> </ol> </li> </ol>	<ol style="list-style-type: none"> <li>Un código de conducta aprobado con arreglo a la presente ley, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país, de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares.</li> <li>Un mecanismo de certificación aprobado con arreglo al artículo 45, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares.</li> </ol> <p>3. Siempre que exista declaración de nivel adecuado de protección, expedida por la autoridad de protección de datos, las garantías adecuadas contempladas en el numeral 1 podrán igualmente ser aportadas, en particular, mediante:</p> <ol style="list-style-type: none"> <li>Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional.</li> <li>Disposiciones que se incorporen en acuerdos administrativos entre las entidades u organismos públicos, que incluyan derechos efectivos y exigibles para los titulares.</li> </ol> <p><b>ARTÍCULO 50. Normas corporativas vinculantes.</b></p> <ol style="list-style-type: none"> <li>La autoridad de protección de datos aprobará normas corporativas vinculantes, siempre que estas:             <ol style="list-style-type: none"> <li>Sean jurídicamente vinculantes y se apliquen a todos los miembros que hacen parte del mismo grupo de empresas o de la unión de empresas dedicadas a una actividad económica conjunta.</li> <li>Confieran expresamente a los titulares derechos exigibles previstos en los artículos 18 al 27 de la presente ley.</li> <li>Cumplan los requisitos establecidos en el numeral 2 del presente artículo.</li> </ol> </li> <li>Las normas corporativas vinculantes mencionadas en el numeral 1 especificarán, como mínimo, los siguientes elementos:             <ol style="list-style-type: none"> <li>La estructura y los datos de contacto del grupo empresarial o</li> </ol> </li> </ol>
<p>de la unión de empresas dedicadas a una actividad económica conjunta.</p> <ol style="list-style-type: none"> <li>Las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamiento y sus fines, el tipo de titulares afectados y el nombre de los países en cuestión.</li> <li>Su carácter jurídicamente vinculante, tanto a nivel interno como externo.</li> <li>La aplicación de los principios generales en materia de protección de datos establecidos en la presente ley.</li> <li>Los derechos de los titulares en relación con el tratamiento y los medios para ejercerlos.</li> <li>La forma en que se facilita a los titulares la información, sobre las normas corporativas vinculantes.</li> <li>Las funciones del o los oficiales de protección de datos, designados de conformidad con el artículo 39, de cualquier otra persona o entidad encargada de la supervisión y del cumplimiento de las normas corporativas vinculantes, así como de la supervisión de la formación y de la tramitación de las reclamaciones.</li> <li>Los procedimientos de reclamaciones.</li> <li>Los mecanismos establecidos, para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas con el fin de proteger los derechos del titular.</li> <li>Los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de protección de datos.</li> <li>Los mecanismos para informar a la autoridad de protección de datos de cualquier requisito jurídico de aplicación en un tercer país a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes.</li> <li>La formación en protección de datos pertinente, para el personal que tenga acceso permanente o habitual a datos personales.</li> </ol>	<ol style="list-style-type: none"> <li>La autoridad de protección de datos podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y la autoridad de control en relación con las normas corporativas vinculantes según lo dispuesto en el presente artículo.</li> </ol> <p><i>Parágrafo primero.</i> Las Normas Corporativas Vinculantes sólo podrán ser sometidas a la aprobación de la autoridad de protección de datos una vez hayan sido aprobadas por el órgano correspondiente según los estatutos de la sociedad o los acuerdos del grupo empresarial. Las normas que sean formalmente presentadas ante la autoridad de protección de datos sólo estarán vigentes a partir de la fecha en que ésta emita su certificación y a partir de ese momento, se podrán aplicar.</p> <p><i>Parágrafo segundo.</i> En los casos en que las normas no sean aprobadas, los ajustes requeridos por la autoridad de protección de datos, una vez realizados, deben contar con la aprobación del órgano social o contractual correspondiente, antes de ser sometidas, nuevamente, a aprobación.</p> <p><b>ARTÍCULO 51. Excepciones para situaciones específicas.</b></p> <ol style="list-style-type: none"> <li>En ausencia de una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, una transferencia o conjunto de transferencias de datos personales a terceros países u organizaciones internacionales sólo podrá realizarse si se cumplen alguna de las siguientes condiciones:             <ol style="list-style-type: none"> <li>El titular haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos de dichas transferencias debido a la ausencia de una declaración de nivel adecuado de protección y de garantías adecuadas.</li> <li>La transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.</li> <li>La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del titular, entre el responsable del tratamiento y otra persona natural o jurídica.</li> </ol> </li> </ol>

<p>d) La transferencia sea necesaria por razones importantes de interés público.</p> <p>e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones judiciales o administrativas.</p> <p>f) La transferencia sea necesaria para proteger los intereses vitales del titular o de otras personas, cuando el titular esté física o jurídicamente incapacitado para dar su consentimiento.</p> <p>g) La transferencia se realice desde un registro público destinado a facilitar información y esté accesible para consulta por el público en general o cualquier persona con un interés legítimo, siempre que se cumplan las condiciones establecidas por la ley para dicha consulta en cada caso particular. En tal situación, la transferencia no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro público. Si la finalidad del registro es la consulta por parte de personas con un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.</p> <p>2. Cuando una transferencia no pueda basarse en una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, y no se aplique ninguna de las excepciones para situaciones específicas mencionadas en el numeral primero del presente artículo, sólo podrá llevarse a cabo si se cumplen las siguientes condiciones:</p> <p>a) No es repetitiva.</p> <p>b) Afecta sólo a un número limitado de titulares.</p> <p>c) Es necesaria para fines e intereses legítimos imperiosos perseguidos por el responsable del tratamiento, sobre los cuales no prevalecen los intereses, derechos y garantías del titular. El responsable del tratamiento informará al titular, de la transferencia y de los intereses legítimos imperiosos perseguidos.</p> <p>d) El responsable del tratamiento ha evaluado los riesgos y basándose en esta evaluación ha ofrecido garantías apropiadas con respecto a la protección de datos personales.</p> <p>Adicionalmente, el responsable del tratamiento informará a la autoridad de protección de datos sobre la transferencia y a los</p>	<p>titulares de los intereses legítimos imperiosos perseguidos con dicha transferencia.</p> <p>3. El numeral 1, literales a), b) y c), y el numeral 2 no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus funciones.</p> <p>4. En ausencia de una declaración de nivel adecuado de protección, una normativa con rango de ley, podrá por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional.</p> <p>5. El responsable o el encargado del tratamiento documentará en los registros de las actividades del tratamiento, la evaluación y las garantías apropiadas a las que se refiere el numeral 2 del presente artículo.</p> <p><b>ARTÍCULO 52. Cooperación internacional en el ámbito de la protección de datos personales.</b></p> <p>En relación con terceros países y organizaciones internacionales, la autoridad de protección de datos tomará medidas apropiadas para:</p> <p>a) Crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales.</p> <p>b) Prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y garantías fundamentales.</p> <p>c) Asociar a partes interesadas en la materia, a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales.</p> <p>d) Promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.</p> <p style="text-align: center;"><b>TITULO V</b></p> <p style="text-align: center;"><b>AUTORIDAD DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS</b></p>
<p><b>ARTÍCULO 53. Autoridad de Protección de Datos.</b></p> <p>1. La Superintendencia de Industria y Comercio ejercerá la función de autoridad nacional de protección de datos personales, garantizando el efectivo cumplimiento de los principios, derechos, garantías y los procedimientos establecidos en la presente ley en aras de facilitar la libre circulación de datos.</p> <p>2. Sin perjuicio de lo mencionado, cuando el tratamiento de datos personales dé lugar a un comportamiento delictivo, la Fiscalía General de la Nación será la encargada de la persecución penal de dichas conductas.</p> <p>3. La autoridad de protección de datos, tendrá a su cargo las funciones de inspección, vigilancia y control, las cuales se desarrollarán en cumplimiento de las facultades otorgadas en la presente ley.</p> <p>4. Para el ejercicio de sus funciones, deberán tenerse en cuenta las garantías constitucionales y principios generales que regulan el actuar de la autoridad de protección de datos, garantizando en todo momento el derecho al debido proceso y demás garantías procesales.</p> <p><b>ARTÍCULO 54. Funciones de la Autoridad de Protección de Datos.</b></p> <p>La autoridad de protección de datos, ejercerá las siguientes funciones:</p> <p>a) Responder a las consultas previas realizadas por los responsables del tratamiento de conformidad con lo establecido en el artículo 38.</p> <p>b) Emitir, por iniciativa propia o previa solicitud, instrucciones, guías y demás instrumentos que considere necesarios sobre cualquier asunto relacionado con la protección de los datos personales.</p> <p>c) Emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 44 de la presente ley.</p> <p>d) Aprobar criterios de certificación.</p> <p>e) Aprobar las Cláusulas contractuales modelo contempladas en el artículo 49, numeral 2, literal c).</p> <p>f) Aprobar normas corporativas vinculantes de conformidad con el artículo 50.</p> <p>g) Autorizar las cláusulas contractuales de las que trata el artículo 49, numeral 3, literal a).</p> <p>h) Autorizar los acuerdos administrativos entre las entidades u organismos públicos de conformidad con el artículo 49, numeral 3, literal b).</p>	<p>i) Impartir instrucciones a los responsables y encargados del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones.</p> <p>j) Llevar a cabo visitas de inspección, de oficio o a solicitud de parte.</p> <p>k) Llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 45 de la presente ley.</p> <p>l) Requerir a los responsables y encargados del tratamiento sobre presuntas infracciones a la presente ley.</p> <p>m) Obtener de los responsables y encargados del tratamiento el acceso a toda la información necesaria para el ejercicio de sus funciones, así como el acceso a todas las instalaciones, incluidos equipos y medios de tratamiento de datos, respetando el debido proceso y la confidencialidad que ello requiere de acuerdo con la normativa vigente.</p> <p>n) Impartir instrucciones a los responsables y encargados del tratamiento cuando las operaciones de tratamiento infrinjan lo dispuesto en la presente ley.</p> <p>o) Imponer multas de carácter personal o institucional a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido lo establecido en la presente ley.</p> <p>p) Imponer una limitación temporal o definitiva del tratamiento, como resultado de una sanción o de una orden administrativa a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido la presente ley.</p> <p>q) Impartir instrucciones a los responsables y encargados del tratamiento que atiendan las solicitudes de ejercicio de los derechos de los titulares en virtud de los artículos 18 al 27 de la presente ley.</p> <p>r) Impartir instrucciones al responsable del tratamiento para que comunique a los titulares, los incidentes de seguridad de los datos personales.</p> <p>s) Impartir instrucciones para garantizar el pleno y efectivo ejercicio de los derechos de rectificación, supresión o limitación del tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales.</p> <p>t) Impartir instrucciones al organismo de certificación para que retire o</p>

que no emita una certificación con arreglo al artículo 45, si no se cumplen o dejan de cumplirse los requisitos para ello.

*Parágrafo Primero.* La Sala Administrativa del Consejo Superior de la Judicatura cumplirá funciones de promoción y difusión de la normativa en protección de datos personales en la Rama Judicial, y la Sala Disciplinaria será la encargada de investigar y sancionar la conducta de los funcionarios judiciales por el incumplimiento de la misma.

*Parágrafo Segundo.* El Departamento Administrativo de la Función Pública en articulación con la Autoridad de protección de datos realizará la promoción y difusión de la normativa en protección de datos personales que debe ser cumplida por cada una de las entidades públicas.

**TÍTULO VI**

**DISPOSICIONES RELATIVAS A SITUACIONES ESPECÍFICAS DE TRATAMIENTO**

**CAPÍTULO I**

**TRATAMIENTOS DE DOCUMENTOS PÚBLICOS**

**ARTÍCULO 55. Tratamiento de los documentos de identificación.**

1. El responsable y encargado del tratamiento implantarán las medidas técnicas y organizativas en atención al riesgo para evitar la circulación no autorizada de reproducciones digitales, copias o fotocopias de la cédula de ciudadanía, como documento que contiene datos de carácter personal, teniendo en cuenta, entre otros, los siguientes criterios:
  - a) Implementarán procedimientos de trazabilidad al interior de la organización, para evitar que se realicen copias no autorizadas de la cédula de ciudadanía entregada por los titulares. El titular podrá hacer uso de sellos, leyendas o firmas que determinen las condiciones de tiempo, modo, lugar y la finalidad con la que entrega la copia de su cédula de ciudadanía.
  - b) Si no existe una base jurídica que legitime el tratamiento de los datos sensibles contenidos en la cédula de ciudadanía, deberá evitarse su captura o implementar técnicas de anonimización sobre los datos sensibles.

- c) Exclusivamente el personal autorizado podrá tener acceso a los lugares y/o activos de información donde se archiven las copias de la cédula de ciudadanía.
  - d) Aquellas copias de cédulas de ciudadanía que se hubiesen recabado exclusivamente para la realización de trabajos temporales deberán cumplir, entre otras, las medidas de seguridad de conformidad con el artículo 35 y ser borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su tratamiento.
  - e) Mientras la cédula de ciudadanía no se encuentre archivada en los dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser tratada por terceros no autorizados.
2. Si para efectos de identificación, el titular no facilitó su cédula de ciudadanía para las operaciones de tratamiento llevadas a cabo por el responsable, en caso de ejercicio de los derechos contemplados en esta ley, utilizará el método de identificación previsto al momento de la recolección de los datos personales del titular, y sólo en caso excepcional y motivado, podrá requerirles para que el titular se identifique.
  3. Cuando sea necesaria la publicación de un acto administrativo que contenga datos personales del titular, incluyendo su cédula de ciudadanía, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de la cédula de ciudadanía, cédula de extranjería, pasaporte o documento equivalente o cualquier otro mecanismo de seudonimización.

*Parágrafo.* Lo contemplado en el presente artículo aplicará en igual medida para cédula de extranjería, pasaporte o documento de identificación equivalente presentado por el titular.

**CAPÍTULO II**

**NEURODATOS**

**ARTÍCULO 56. Tratamiento de neurodatos.**

El responsable, o en su caso el encargado que traten neurodatos, deberán

garantizar la protección de los derechos y garantías fundamentales relacionadas con la protección de los datos personales y la intimidad de las personas, por lo que se establecen las siguientes obligaciones:

1. Se prohíbe la obtención de neurodatos mediante técnicas de manipulación o coerción que comprometa la integridad cerebral o afecte negativamente la salud mental. Todo tratamiento efectuado a neurodatos respetará la dignidad y la integridad física y psíquica de las personas.
2. El deber de información, además de cumplir los requisitos del artículo 14, podrá contener los riesgos y beneficios para el titular.
3. Queda prohibido cualquier tratamiento de neurodatos que pueda ocasionar la pérdida de identidad personal.

**ARTÍCULO 57. Tecnologías de rastreo.**

1. Es necesario obtener el consentimiento del titular para utilizar tecnologías de rastreo. Las opciones de aceptar o rechazar deben presentarse de manera destacada y equitativa, sin que rechazar sea más complicado que aceptar. No se considerará acción afirmativa utilizar los servicios sin manifestar la aceptación o el rechazo de las tecnologías de rastreo.
2. Las tecnologías de rastreo técnicamente necesarias o esenciales, que son indispensables para el funcionamiento adecuado y para proporcionar los servicios solicitados por el titular, están exentas del requisito de obtener el consentimiento.
3. Las tecnologías consideradas técnicamente necesarias cumplen con los siguientes criterios:
  - a) Son temporales y se eliminan al finalizar la sesión. Se utilizan para mantener la sesión del titular, establecer parámetros libremente elegidos por éste y permitir el acceso a ciertas funcionalidades.
  - b) Se utilizan para recordar los artículos agregados al carrito de compras, durante una sesión de compra en línea.
  - c) Se utilizan para mantener la sesión activa y autenticar al titular mientras navega por la plataforma.

- d) Se utilizan para garantizar la seguridad de las interacciones detectando actividades potencialmente maliciosas o no autorizadas.
  - e) No podrán ser usadas para otras finalidades ni para elaborar perfiles de los titulares. En caso de que no cumplan esta función, se deberá informar al usuario y darle la opción de rechazarlas.
4. Las tecnologías de rastreo técnicamente necesarias no deben recopilar información personal más allá de lo estrictamente necesario para el funcionamiento del servicio y deben usarse exclusivamente con fines técnicos.

**TÍTULO VII**

**INDEMNIZACIÓN Y RÉGIMEN SANCIONATORIO**

**CAPÍTULO I**

**DISPOSICIONES GENERALES Y GRADUACIÓN DE LAS SANCIONES**

**ARTÍCULO 58. Derecho a indemnización y responsabilidad.**

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia del incumplimiento de cualquiera de las obligaciones contenidas en la presente ley tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por la presente ley. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento, cuando no haya cumplido con las obligaciones de la presente ley dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones del responsable.
3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del numeral 2, si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.
4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, de conformidad a los numerales 2 y 3, responsables de cualquier daño o perjuicio causado por dicho



<p>tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.</p> <p>5. Cuando, de conformidad con el numeral 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el numeral 2.</p> <p>6. La autoridad de protección de datos será competente para conocer y decidir sobre la acción descrita en el presente artículo por el incumplimiento de las obligaciones de la presente ley, sin perjuicio del derecho que tiene el titular de acceder a la administración de justicia.</p> <p><b>Parágrafo: Para efecto de la aplicación de lo dispuesto en el presente artículo, se adiciona un literal al artículo 24 de la Ley 1564 de 2012 el cual quedará así:</b></p> <p><b>f) Acciones de indemnización de daños y perjuicios materiales o inmateriales como consecuencia del incumplimiento de cualquiera de las obligaciones del Régimen General de Protección de Datos.</b></p> <p><b>ARTÍCULO 59. Sujetos Responsables.</b></p> <p>Están sujetos al régimen sancionador establecido en la presente ley:</p> <ol style="list-style-type: none"> <li>1. Los responsables del tratamiento, así como los corresponsables en la medida que su participación en la operación de tratamiento fuera determinante en la infracción.</li> <li>2. Los encargados del tratamiento.</li> <li>3. Las entidades de certificación.</li> <li>4. Las entidades acreditadas de supervisión de los códigos de conducta.</li> </ol> <p><i>Parágrafo:</i> No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este título.</p> <p><b>ARTÍCULO 60. Condiciones generales para la imposición de sanciones.</b></p> <ol style="list-style-type: none"> <li>1. La autoridad de protección de datos, garantizará que la imposición de las</li> </ol>	<p>sanciones con arreglo al presente título por las infracciones a los deberes y obligaciones contemplados en la presente ley, sean en cada caso individual efectivas, proporcionadas y correctivas. En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Administrativo y de lo Contencioso Administrativo.</p> <p>2. Las sanciones se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 54. Al decidir la imposición de la sanción y su cuantía se graduarán atendiendo los siguientes criterios que resulten aplicables:</p> <ol style="list-style-type: none"> <li>a) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta el alcance o propósito de la operación de tratamiento de que se trate, así como, el número de titulares afectados y el daño o peligro generado a los intereses jurídicos tutelados en la presente ley.</li> <li>b) El alcance continuado de la infracción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.</li> <li>c) Si existió dolo o negligencia en la comisión de la infracción.</li> <li>d) Los beneficios obtenidos por el infractor o terceros, en virtud de la comisión de la infracción.</li> <li>e) El grado de responsabilidad del infractor, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud del artículo 35.</li> <li>f) La reincidencia en la comisión de la infracción.</li> <li>g) La resistencia, negativa u obstrucción a las labores de inspección o de vigilancia de la Autoridad de protección de datos.</li> <li>h) La afectación a los derechos de los niñas, niños y adolescentes.</li> <li>i) El incumplimiento de las instrucciones impartidas en virtud del artículo 54, cuando hayan sido ordenadas previamente contra el infractor en relación con el mismo asunto.</li> <li>j) La renuencia o desacato a cumplir las instrucciones impartidas por la autoridad de protección de datos.</li> <li>k) Si las infracciones fueron realizadas con el propósito de cometer alguna conducta tipificada como delito por la ley.</li> <li>l) Cualquier medida tomada por el infractor para contener y</li> </ol>
<p>mitigar los daños y perjuicios sufridos por los titulares.</p> <ol style="list-style-type: none"> <li>m) El grado de cooperación con la autoridad de protección de datos, con el fin de contener y mitigar los posibles efectos adversos de la infracción.</li> <li>n) La posibilidad de que la conducta del titular hubiera podido inducir a la comisión de la infracción.</li> <li>o) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.</li> <li>p) La forma en que la autoridad de protección de datos tuvo conocimiento de la infracción, en particular si el infractor notificó la infracción y, en tal caso, en qué medida.</li> <li>q) La adhesión a códigos de conducta en virtud del artículo 42 o a mecanismos de certificación aprobados de conformidad con el artículo 45.</li> <li>r) Disponer, cuando no fuere obligatorio, de un Oficial de protección de datos.</li> <li>s) El reconocimiento o aceptación expresas que haga el infractor sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.</li> <li>t) El sometimiento por parte del infractor, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier titular o interesado.</li> <li>u) Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso.</li> </ol> <p>3. Si la autoridad de protección de datos detecta un posible incumplimiento de las disposiciones de la presente ley por parte de una entidad pública, remitirá la actuación a la Procuraduría General de la Nación para que la procuraduría delegada competente realice la investigación correspondiente.</p> <p>4. El ejercicio por la autoridad de protección de datos de sus funciones en virtud del presente artículo estará sujeto a las garantías del debido proceso.</p> <p style="text-align: center;"><b>CAPÍTULO II</b></p> <p style="text-align: center;"><b>DE LAS INFRACCIONES EN MATERIA DE PROTECCIÓN DE DATOS</b></p>	<p><b>ARTÍCULO 61. Infracciones.</b></p> <p>Constituyen infracciones los actos y conductas que resulten contrarios a la aplicación de los principios y obligaciones de la presente ley.</p> <p style="text-align: center;"><b>CAPÍTULO III</b></p> <p style="text-align: center;"><b>DE LA IMPOSICIÓN DE SANCIONES</b></p> <p><b>ARTÍCULO 62. Sanciones.</b></p> <p>La autoridad de protección de datos podrá imponer a los infractores las siguientes sanciones:</p> <ol style="list-style-type: none"> <li>1. Multas de carácter personal e institucional hasta por el equivalente de cuatro mil (4.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción; o, hasta el cinco por ciento (5%) de los ingresos operacionales del infractor en el año fiscal inmediatamente anterior al de la imposición de la sanción.</li> <li>2. Sanciones operativas y medidas correctivas.             <ol style="list-style-type: none"> <li>a) Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán las medidas correctivas que se deberán adoptar.</li> <li>b) Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la autoridad de protección de datos.</li> <li>c) Cierre inmediato y definitivo de las operaciones relacionadas con el tratamiento ilícito de Datos Sensibles.</li> <li>d) Las medidas correctivas serán establecidas por la autoridad de protección de datos, de acuerdo a las facultades otorgadas por el artículo 54, dependiendo de cada caso individual y serán independientes de la imposición de multas.</li> </ol> </li> </ol> <p style="text-align: center;"><b>TÍTULO VIII</b></p> <p style="text-align: center;"><b>RÉGIMEN DE TRANSICIÓN</b></p> <p><b>ARTÍCULO 63. Condiciones del consentimiento.</b></p>



La autorización entregada por los titulares de datos recabados antes de la entrada en vigencia de esta ley seguirá siendo válida por un período de un año contados desde la entrada en vigencia. Durante este plazo, el responsable deberá legitimar el tratamiento de datos de conformidad con el artículo 6.

Parágrafo. La autorización para el tratamiento de datos personales otorgada con fines de investigación en salud y biomédica recogidos con anterioridad a la entrada en vigencia de esta ley no perderá su legitimidad cuando concurra alguna de las circunstancias siguientes:

- a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento previo y expreso.
- b) Que, habiéndolo obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

**ARTÍCULO 64. Plazos para la implantación de las medidas de seguridad.**

La implantación de las medidas de seguridad previstas en la presente ley deberá producirse con arreglo a las siguientes reglas:

1. Respecto de los tratamientos que existieran al momento de la entrada en vigencia de la presente ley se llevará a cabo de la siguiente manera:
  - a) En el plazo máximo de dieciocho meses desde su entrada en vigencia, deberán implantarse las medidas de seguridad en los tratamientos automatizados.
  - b) Respecto de los tratamientos no automatizados que existieran al momento de la entrada en vigencia de la presente ley, en el plazo máximo de un año.
2. Los tratamientos, tanto automatizados como no automatizados, creadas con posterioridad a la fecha de entrada en vigencia de la presente ley deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en esta ley.

Parágrafo. A requerimiento de la autoridad de protección de datos, el responsable de Tratamiento deberá demostrar que está llevando a cabo la implementación de las medidas de seguridad en los tratamientos existentes

en el momento de la entrada en vigencia de la presente ley.

**ARTÍCULO 65. Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.**

Las solicitudes para el ejercicio de los derechos que hayan sido efectuadas con anterioridad a la entrada en vigencia de la presente ley, su contestación se regirá por la Ley 1581 de 2012.

**ARTÍCULO 66. Contratos de encargados del tratamiento.**

Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley serán válidos. Los responsables y encargados tendrán hasta dieciocho meses para modificar aquellos contratos que no resulten conforme a lo dispuesto en el artículo 32 de la presente ley.

Durante dicho plazo cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 32 de la presente ley.

Parágrafo. Los contratos firmados con posterioridad a la fecha de entrada en vigencia de la presente ley deberán cumplir con los requisitos establecidos en el artículo 32.

**ARTÍCULO 67. Transferencias Internacionales.**

1. Dentro de los primeros dos años posteriores a la entrada en vigencia de la presente ley, la Autoridad de Protección de Datos deberá revisar lo establecido en la Circular Única de la Superintendencia de Industria y Comercio relativo a las transferencias de datos personales, a la luz de los criterios establecidos en el artículo 48.
2. Una vez revisada la Circular Única de la Superintendencia de Industria y Comercio, los reconocimientos a países con nivel adecuado por parte de la autoridad de protección de datos a través su Circular tendrán una validez de hasta 2 años contados a partir de la entrada en vigencia de la presente ley.

**ARTÍCULO 68. Régimen Sancionatorio.**

1. El Régimen Sancionatorio contemplado en el Título VII entrará en

aplicación a los 2 años de entrada en vigencia de la presente ley. La autoridad de protección de datos impondrá a los responsables y Encargados del Tratamiento las sanciones descritas en la Ley 1581 de 2012, señalando de forma paralela el equivalente de la infracción y su respectiva sanción en el Régimen Sancionatorio aprobado por la presente ley.

2. De conformidad con las facultades constitucionales que le han sido otorgadas a la Procuraduría General de la Nación, esta deberá asignar en el término de 18 meses con posterioridad a la entrada en vigencia de la presente ley, las funciones y competencias a una procuraduría delegada que será seleccionada o creada atendiendo a los criterios de especialidad por el incumplimiento a las disposiciones establecidas en la presente ley.

**ARTÍCULO 69. Registro Nacional de Bases de Datos - RNBD.**

El Directorio Público de Bases de Datos, actualmente gestionado por la autoridad de protección de datos, experimentará una transformación tanto en su denominación como en su estructura, convirtiéndose en el "Registro de las Actividades del Tratamiento", en un plazo máximo de dos años a partir de la entrada en vigencia de la presente ley.

El Gobierno Nacional reglamentará las categorías de sujetos obligados, así como los términos y condiciones bajo los cuales deben inscribirse en el Registro señalado.

**ARTÍCULO 70. Entidades Certificadoras**

Los organismos del subsistema de calidad tendrán un año desde la entrada en vigencia de la presente ley para regular la forma de acreditar las entidades descritas en el artículo 45.

**ARTÍCULO 71. Vigencia y Derogatorias**

La presente ley entra en vigencia desde su promulgación y será de aplicación obligatoria un año después, salvaguarda los derechos adquiridos y deroga todas las disposiciones que le sean contrarias. También deroga la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa relacionada que sea contraria a las disposiciones de la presente ley.

De las y los Congresistas,

De las y los Congresistas,

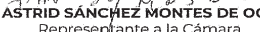
  
**DUVALIER SÁNCHEZ ARANGO**  
Representante a la Cámara


  
**JUAN CARLOS WILLS OSPINA**  
Representante a la Cámara

  
**GERSEL LUIS PÉREZ ALTAMIRANDA**  
Representante a la Cámara

  
**CARLOS FELIPE QUINTERO OVALLE**  
Representante a la Cámara

  
**HERNÁN DARIO CADAVID MARQUEZ**  
Representante a la Cámara

  
**ASTRID SÁNCHEZ MONTES DE OCA**  
Representante a la Cámara

  
**DIÓGENES QUINTERO AMAYA**  
Representante a la Cámara

  
**JORGE ALEJANDRO OCAMPO GIRALDO**  
Representante a la Cámara

  
**LUIS ALBERTO ALBAN URBANO**  
Representante a la Cámara

  
**MARELEN CASTILLO TORRES**  
Representante a la Cámara