REPÚBLICA DE COLOMBIA

GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

I S S N 0 1 2 3 - 9 0 6 6

AÑO XXXIV - Nº 1501 Bogotá, D. C., viernes, 22 de agosto de 2025 EDICIÓN DE 40 PÁGINAS

DIRECTORES: DIEGO ALEJANDRO GONZÁLEZ GONZÁLEZ
SECRETARIO GENERAL DEL SENADO
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

PROYECTOS DE LEY ESTATUTARIA

PROYECTO DE LEY ESTATUTARIA NÚMERO 214 DE 2025 CÁMARA

por la cual se reforma la Ley 1581 de 2012 y se dictan otras disposiciones generales relativas a la protección de datos personales.

Bogotá, D. C., 12 de agosto de 2025.

Secretario General

JAIME LUIS LACOUTURE PEÑALOZA

Cámara de Representantes

Referencia: Radicación Proyecto de Ley Estatutaria número 214 de 2025 Cámara, *por la cual se reforma la Ley 1581 de 2012 y se dictan otras disposiciones generales relativas a la protección de datos personales.*

Respetado señor Secretario,

En nuestra condición de miembros del Congreso de la República y en uso del derecho consagrado en la Constitución Política de Colombia y en la Ley 5ª de 1992, nos permitimos poner a consideración de la Honorable Cámara de Representantes el siguiente Proyecto de Ley Estatutaria, *por la cual se reforma la Ley 1581 de 2012 y se dictan otras disposiciones generales relativas a la protección de datos personales*", con el fin de iniciar con el trámite correspondiente y cumplir con las exigencias dictadas por la Constitución y la ley.

De las y los Congresistas,

DUVALIER SÁNCHEZ ARANGO Representante a la Cámara por Valle del Cauca - Alianza Verde	**MARÍA FERNANDA CARRASCAL ROJAS** Representante a la Cámara por Bogotá

KAREN ASTRITH MANRIQUE OLARTE Representante a la Cámara CITREP 2 – Arauca	**CRISTÓBAL CAICEDO ANGULO** Representante a la Cámara por el Valle del Cauca
ETNA TÁMARA ARGOTH CALDERÓN Representante a la Cámara por Bogotá Pacto Histórico PDA	**SANDRA RAMIREZ LOBO SILVA** Senadora de la República Partido COMUNES
JUAN CAMILO LONDOÑO BARRERA Representante a la Cámara por Antioquia Partido Alianza Verde	**GABRIEL BECERRA YAÑEZ** Representante a la Cámara por Bogotá Pacto Histórico - Unión Patriótica

SARAY ELENA ROBAYO BECHARA Representante a la Cámara Departamento de Córdoba	**DAVID ALEJANDRO TORO RAMIREZ** Representante a la Cámara por Antioquia Pacto Histórico
MARIA DEL MAR PIZARRO GARCÍA Representante a la Cámara por Bogotá	**JAIME RAÚL SALAMANCA TORRES** Representante a la Cámara por Boyacá Partido Alianza Verde
HERÁCLITO LANDÍNEZ SUÁREZ Representante a la Cámara Pacto Histórico	**JAMES MOSQUERA TORRES** REPRESENTANTE A LA CÁMARA CITREP CHOCÓ -ANTIOQUIA
ANIBAL GUSTAVO HOYOS FRANCO Representante a la Cámara por Risaralda Partido Liberal	**ALIRIO URIBE MUÑOZ** Representante a la Cámara

PROYECTO DE LEY ESTATUTARIA NÚMERO 214 DE 2025 CÁMARA

por la cual se reforma la Ley 1581 de 2012 y se dictan otras disposiciones generales relativas a la protección de datos personales.

El Congreso de la República

DECRETA:

Artículo 1°. ***Objeto***. La presente ley tiene por objeto modificar y adicionar la Ley Estatutaria 1581 de 2012, con el fin de fortalecer el derecho a la protección de los datos personales, garantizar su efectivo ejercicio y adecuar el régimen jurídico vigente a los avances tecnológicos, económicos y sociales que inciden en el tratamiento de la información personal.

Artículo 2°. Modifíquese el artículo 2° de la Ley 1581 de 2012, el cual quedará así:

Artículo 2°. ***Ámbito de aplicación.*** Las disposiciones y principios consagrados en la presente ley serán aplicables:

1. A todo tratamiento de datos personales efectuado por una persona natural o jurídica, de naturaleza pública o privada, u otros organismos, sin importar el medio utilizado, el país de residencia o domicilio del Responsable o Encargado del tratamiento, ni el lugar donde se encuentren ubicados los datos, siempre que concurra alguna de las siguientes circunstancias:

a) El Tratamiento se lleve a cabo en el territorio nacional; o

b) Las actividades de Tratamiento estén relacionadas con la oferta de bienes o servicios a Titulares con residencia en Colombia, independientemente de si estos son de carácter oneroso o no; o

c) Las actividades de Tratamiento estén relacionadas con el monitoreo o seguimiento del comportamiento de titulares ubicados en Colombia.

2. Cuando proceda la aplicación de la legislación nacional en virtud del Derecho Internacional Público.

3. A todo Responsable o Encargado, que aun sin estar establecido en Colombia, actúa en virtud de una misión diplomática, embajada u oficina consular.

4. El régimen de protección de Datos Personales que se establece en la presente ley no será aplicable a los siguientes tratamientos:

a) Los realizados en un ámbito exclusivamente personal o doméstico.

b) Los realizados por autoridades y organismos competentes cuya finalidad sea la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) Los realizados por autoridades competentes que tengan como fin la gestión de información de inteligencia y/o contrainteligencia;

d) Los que tengan como finalidad cumplir con la actividad periodística y otros contenido de carácter editorial;

e) Los regulados por la Ley 1266 de 2008, salvo lo dispuesto en materia de transferencias internacionales de datos personales. En lo relativo a principios, derechos y garantías, se deberá procurar una interpretación armónica entre ambas normas.

Parágrafo 1°. Los principios sobre protección de datos serán aplicables a todos los tratamientos de datos personales, incluidos los exceptuados en el numeral 4, de conformidad con los límites dispuestos en la presente ley y, siempre y cuando no contravengan normas especiales o afecten datos amparados por reserva legal. En el evento que la normatividad especial que regule los tratamientos exceptuados prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

Parágrafo 2°. El Gobierno nacional en un término de seis meses a partir de la promulgación de la presente ley, reglamentará el deber que tendrán los Responsables y Encargados del tratamiento de datos personales no domiciliados en el territorio nacional, de designar por escrito un representante legal y/o establecer una sucursal en el país, con el fin de atender sus obligaciones ante la Autoridad de Protección de Datos Personales.

Parágrafo 3°. 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.

Artículo 3°. Modifíquese el artículo 3° de la Ley 1581 de 2012, el cual quedará así:

Artículo 3°. ***Definiciones.*** Para los efectos de la presente ley, se entiende por:

a) Anonimización: Procedimiento técnico que, aplicado a unos datos personales, tiene como resultado irreversible que estos no puedan en adelante vincularse o asociarse a una persona natural determinada o determinable;

b) Autorización: Toda manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica del Titular o su representante, expresada mediante una declaración o una clara acción afirmativa para que se traten sus Datos personales;

c) Base de Datos: Conjunto organizado de Datos Personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado.

d) Cesión de datos: tratamiento de datos que implica su revelación a una persona distinta del titular y/o encargado de tratamiento. Una vez el destinatario se le ceden los datos se convierte en responsable del tratamiento. No se considerarán destinatarios las autoridades que puedan recibir datos personales en el marco de una investigación concreta.

e) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

f) 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, voz, datos dactiloscópicos, entre otros;

g) Datos genéticos: Datos Personales sobre las características hereditarias de una persona natural, obtenida por análisis de ácidos nucleicos u otros análisis científicos, que proporcionan información única sobre la fisiología o la salud de esa persona;

h) 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;

i) 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, pertenencia a organizaciones sociales o 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.

j) 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;

k) Encargado del Tratamiento: Persona natural o jurídica, de naturaleza pública o privada, u otro organismo que, que por sí misma o en asocio con otros, realice el tratamiento de los datos personales por cuenta del Responsable del tratamiento;

l). Incidente de seguridad: Cualquier violación de los códigos de seguridad que resulte en el daño, la destrucción, acceso no autorizado o fraudulento, 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;

m) Responsable del Tratamiento: Persona natural o jurídica, de naturaleza pública o privada, u otro organismo que, por sí mismo o en asocio con otros, determine los fines y medios del Tratamiento;

n) 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;

o) Seudonimización: Tratamiento de Datos Personales de manera tal que ya no se pueda vincularse o asociarse a un Titular determinado o determinable sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los Datos Personales no se atribuyen a una persona natural identificada o identificable;

p) Titular: Persona natural cuyos Datos Personales son objeto de Tratamiento;

q) Transferencia Internacional de Datos Personales: Operación o conjunto de operaciones de Tratamiento de datos personales que implique el flujo de los mismos, ya sea mediante su cesión o acceso por cuenta de terceros, a sujetos o destinatarios ubicados fuera del territorio nacional;

r) Tratamiento: Cualquier operación o conjunto de operaciones sobre Datos Personales o conjuntos de Datos Personales, tales como la recolección, registro, estructuración, conservación, almacenamiento, uso, adaptación, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, circulación, destrucción o supresión;

s) Tratamiento de datos 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.

Artículo 4. Modifíquese el artículo 4° de la Ley 1581 de 2012:

Artículo 4°. ***Principios para el Trealtad.*** El tratamiento de los datos personales debe ser justo y equitativo, respetando los derechos y garantías del titular y evitando prácticas fraudulentas, engañosas, dolosas o que generen un desequilibrio injustificado en perjuicio de este.

a) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al Titular. Los datos deben ser recogidos con finalidades determinadas, explícitas y legítimas y no serán tratados ulteriormente de manera incompatible con dichos fines;

b) Principio de minimización de datos: Solo deberán recolectarse los datos personales que sean adecuados, pertinentes y estrictamente necesarios en relación con las finalidades específicas, explícitas y legítimas para las cuales se realiza el tratamiento.

c) Principio de veracidad o calidad: La información sujeta a Tratamiento debe reflejar la situación actual del titular y ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos personales que sean parciales, incompletos, fraccionados o que puedan inducir a error. Los datos suministrados directamente por el titular se presumirán exactos;

d) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener, en cualquier momento y sin restricciones, información clara y suficiente por parte del Responsable del Tratamiento o del Encargado del Tratamiento acerca del uso, finalidad, alcance y condiciones aplicables a sus datos personales. La información suministrada a los titulares deberá ser concisa, accesible e inteligible, utilizando un lenguaje claro y sencillo;

e) 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;

f) Principio de confidencialidad: Los Responsables y Encargados del Tratamiento, así como todas las personas que intervengan en cualquier fase del mismo, deberán garantizar que los datos personales no sean puestos a disposición ni revelados a personas, entidades o procesos no autorizados. Esta obligación subsiste incluso después de finalizado el tratamiento de los datos.

El principio de confidencialidad se aplicará sin perjuicio del deber de secreto profesional u otras obligaciones de reserva que sean exigibles conforme a la normativa sectorial o especial aplicable.

g) Principio de proporcionalidad: Durante todo el ciclo de vida de los datos personales, el Responsable del Tratamiento deberá velar porque el tratamiento sea: i) idóneo, en cuanto apropiado para alcanzar los fines legítimos perseguidos; ii) necesario, en tanto no existan medidas menos invasivas que permitan alcanzar dichos fines; y iii) proporcional, en cuanto exista un equilibrio razonable entre los beneficios del tratamiento y el impacto que este pueda generar sobre los derechos y garantías fundamentales del Titular.

h. Principio de limitación del plazo de conservación: Los datos personales deberán conservarse únicamente durante el tiempo estrictamente necesario para el cumplimiento de las finalidades que justifican su Tratamiento.

Podrán conservarse por períodos más prolongados cuando se traten exclusivamente en virtud de un deber legal o contractual, o con fines de archivo en interés público, investigación científica, histórica o estadística, conforme con las disposiciones normativas aplicables en la materia. En todo caso, deberán implementarse las medidas técnicas, jurídicas y organizativas apropiadas para salvaguardar los derechos y garantías de los Titulares, de acuerdo con lo previsto en la presente ley.

i) 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 ello. Los Encargados del Tratamiento asistirán al Responsable en el cumplimiento de esta obligación;

j) Principio de responsabilidad demostrada: El Responsable o el Encargado 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 al titular y a la autoridad de protección de datos, cuando corresponda, 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.

k) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

Artículo 5°. Modifíquese el artículo 5° de la Ley 1581 de 2012, el cual quedará así:

Artículo 5°. ***Datos sensibles.*** Para los efectos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo

uso indebido pueda dar lugar a discriminación. Se consideran datos sensibles, entre otros, los que revelen el origen racial o étnico; las opiniones políticas; las convicciones religiosas o filosóficas; la afiliación sindical o la pertenencia a organizaciones sociales o de derechos humanos; los datos relativos a la salud física o mental; los datos genéticos y neurodatos; los datos biométricos destinados a identificar de manera unívoca a una persona natural; así como los datos relativos al sexo, las características biológicas, la identidad o expresión de género y la orientación sexual de una persona natural.

Artículo 6°. ***Tratamiento de datos sensibles.*** Se prohíbe el Tratamiento de datos sensibles, excepto cuando concurra una de las siguientes circunstancias:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, para uno o más fines específicos;

b) El Tratamiento sea necesario para proteger la vida o la salud del Titular o de otra persona natural y el Titular se encuentre física o jurídicamente incapacitado para autorizar dicho Tratamiento. En estos eventos, los representantes legales deberán otorgar su autorización;

c) 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, sindical o de derechos humanos, 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 la autorización de los titulares;

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la anonimización de los datos de los Titulares;

f) Cuando el Tratamiento sea necesario por razones de interés público de conformidad con la Constitución y la ley, que debe ser proporcional al objetivo perseguido, respetando el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del Titular;

g) 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, con arreglo a la normatividad vigente, que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del Titular;

h) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluaciones médicas ocupacionales, diagnóstico médico, prestación de asistencia o tratamiento médico, o para la gestión de los sistemas y servicios de salud, podrá realizarse sobre la base de la normativa aplicable o en virtud de un contrato con un profesional de la salud. En todo caso, dicho tratamiento deberá ser realizado por un profesional sujeto al deber de secreto profesional.

i) Cuando el Tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas nacionales o 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, 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.

Parágrafo. Cuando, en virtud de las causales previstas en el presente artículo, se requiera el tratamiento de datos sensibles referentes al sexo, la identidad o expresión de género y/o la orientación sexual, deberá garantizarse el respeto por todas las categorías identitarias diversas, incluyendo a personas intersexuales y no binarias. En caso de que el titular haya otorgado su autorización para el tratamiento de estos datos y ejerza su derecho a la rectificación o supresión, no podrá exigirse ningún requisito adicional para acreditar dicha información.

Artículo 7°. Modifíquese el artículo 7° de la Ley 1581 de 2012 de la siguiente manera:

Artículo 7°. ***Tratamiento de Datos personales de los niños, niñas y adolescentes.***

En el tratamiento de datos personales de niños, niñas y adolescentes deberá garantizarse en todo momento el respeto al principio del interés superior del menor. Dicho tratamiento deberá realizarse de manera responsable, asegurando que responda a finalidades legítimas, proporcionales y acordes con su desarrollo integral.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno nacional reglamentará la materia.

El Tratamiento de Datos Personales de menores de edad podrá fundarse en su autorización directa únicamente cuando estos tengan catorce (14) años o más, salvo en aquellos casos en que el ordenamiento jurídico exija la asistencia o representación legal para la celebración del acto o negocio jurídico en cuyo contexto se solicita dicha autorización.

En el caso de menores de catorce (14) años, el Tratamiento solo será lícito cuando cuente con el consentimiento expreso de su representante legal, otorgado en los términos y con el alcance que este determine.

Parágrafo 1°. La edad mínima requerida para el consentimiento de los niños, niñas y adolescentes establecida en esta ley, no afectará las disposiciones especiales referentes al establecimiento de edades mínimas para efectos civiles, penales, laborales u otros regímenes jurídicos, respecto de la validez y consecuencias de ciertos actos jurídicos.

Parágrafo 2°. Cuando el Tratamiento de Datos Personales de menores de catorce (14) años se base en la autorización del representante legal, el Responsable del Tratamiento deberá adoptar todas las medidas razonables, teniendo en cuenta la tecnología disponible, para verificar que dicha autorización ha sido efectivamente otorgada o avalada por quien ejerce la representación legal del menor.

Parágrafo 3°. Cuando la representación legal del menor de catorce años es ejercida por más de una persona, se presume que la autorización de uno obedece a la voluntad de todos. En el supuesto que, uno de los representantes no esté de acuerdo, puede revocar la autorización ante el Responsable del Tratamiento, y solo podría concederse nuevamente por el mutuo acuerdo de los representantes, o mediante decisión judicial que declare su representación legal.

Parágrafo 4°. Los Responsables y Encargados del Tratamiento deberán implementar mecanismos adecuados para garantizar el respeto al Principio de Transparencia al momento de solicitar la autorización para el Tratamiento de Datos Personales de los niños, niñas y adolescentes.

Artículo 8°. Modifíquese el artículo 8° de la Ley 1581 de 2012, el cual quedará así:

Artículo 8°. ***Derechos de los titulares***. El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus Datos Personales frente a los Responsables del Tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento o la justificación sobre qué base legitimadora se está empleando para dicho Tratamiento;

c) Ser informado por el Responsable del Tratamiento, previa solicitud, acerca de si sus datos personales están siendo objeto de tratamiento y sobre el uso que se les ha dado;

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;

e) Presentar denuncias, a título personal o de forma anónima, ante la Superintendencia de Industria y Comercio por hechos que puedan constituir un incumplimiento de las disposiciones establecidas en la presente ley, con el fin de proteger el interés colectivo y el derecho fundamental a la protección de datos personales;

f) Solicitar la supresión del dato cuando el tratamiento no respete los principios, derechos y garantías constitucionales o legales; cuando los datos personales hayan dejado de ser necesarios en relación con las finalidades para las que fueron recogidos; cuando el titular revoque la autorización y el tratamiento no se fundamente en otra base de legitimación; cuando la supresión sea necesaria para el cumplimiento de una obligación legal; cuando los datos hayan sido obtenidos de menores de edad en el contexto de la oferta de servicios de la sociedad de la información; o cuando la Autoridad de Protección de Datos Personales haya determinado que el Responsable del Tratamiento ha incurrido en conductas contrarias a la presente ley o a la Constitución;

g) Revocar la autorización en cualquier momento. Será tan fácil revocar la autorización como otorgarla;

h) Acceder en forma gratuita a sus Datos Personales que hayan sido objeto de Tratamiento;

i) El Titular tiene derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa, cuando se basen únicamente en tratamientos automatizados, incluida la elaboración de perfiles. Lo anterior, sin perjuicio de lo establecido en el parágrafo 1 del presente artículo;

j) Cuando se traten Datos Personales mediante medios electrónicos o automatizados, el Titular tiene derecho a obtener una copia de los Datos Personales que hubiere proporcionado al Responsable o que sean objeto de Tratamiento, en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización o transferirlos a otro Responsable. El Titular puede solicitar que sus Datos Personales se transfieran directamente de Responsable a Responsable cuando sea técnicamente posible. Lo anterior, sin perjuicio de lo establecido en el parágrafo 2°;

k) El Titular podrá oponerse, en cualquier momento y por motivos relacionados con su situación particular, al tratamiento de sus datos personales que se fundamente en las bases jurídicas previstas en los literales e) o f) del artículo 9° de la presente ley, incluida la elaboración de perfiles. Cuando el tratamiento tenga por objeto actividades de marketing o publicidad directa, el Titular podrá oponerse en todo momento al tratamiento de sus datos personales, incluida la elaboración de perfiles relacionada con dichas actividades. Lo anterior, se entiende sin perjuicio de lo establecido en el artículo 8A, numeral 3 de la presente ley.

l. Solicitar la limitación del tratamiento cuando la exactitud de los datos personales sea controvertida por el titular, durante el plazo necesario para su verificación; cuando el tratamiento sea ilícito y el titular se oponga a la supresión de los datos; cuando el responsable ya no necesite los datos personales para las finalidades del tratamiento, pero el titular los requiera para la formulación, ejercicio o defensa de reclamaciones administrativas o judiciales; o cuando el titular haya ejercido el derecho de oposición, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular;

m) Obtener una indemnización por los daños causados por el indebido Tratamiento de sus Datos Personales.

Artículo 9°. Adiciónese el artículo 8A a la Ley 1581 de 2012, el cual quedará así:

Artículo 8°A. ***Disposiciones específicas sobre los derechos de los titulares.***

1. Lo dispuesto en artículo 8° literal i) no resultará aplicable cuando el tratamiento automatizado:

a) Sea necesario para la celebración o la ejecución de un contrato entre el Titular y el Responsable del Tratamiento;

b) Esté autorizado por una norma de rango legal o constitucional;

c) Se base en la autorización del Titular.

Cuando sea aplicable la excepción prevista en los incisos a) y c), el Titular tendrá derecho a obtener intervención humana, a recibir una explicación sobre la decisión tomada en los términos de lo establecido en el artículo, y a expresar su punto de vista e impugnar la decisión.

El Responsable del Tratamiento no podrá llevar a cabo tratamientos automatizados de datos personales que produzcan efectos discriminatorios sobre los titulares, en particular cuando se basen en alguna de las categorías de datos sensibles definidas en el artículo 5° de la presente ley, salvo que se apliquen las excepciones previstas en esta ley y se hayan adoptado medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.

2. Lo dispuesto en el artículo 8° literal j) no procederá cuando:

a) Su ejercicio imponga una carga financiera o técnica excesiva o irrazonable sobre el Responsable o Encargado del Tratamiento;

b) Afecte negativamente los derechos y garantías de otras personas naturales;

c) El tratamiento sea necesario para el cumplimiento de una función realizada en interés público, o en el ejercicio de poderes o funciones públicas conferidas al Responsable del tratamiento.

d) Se trate de información inferida, derivada, creada, generada u obtenida por el Responsable del Tratamiento a partir del análisis o tratamiento de los datos personales del titular, sin perjuicio de los demás derechos que le asisten al titular de conformidad a la presente ley.

3. Cuando la oposición ejercida en los términos del artículo 8° literal k) se refiera al tratamiento con fines de marketing o publicidad directa, incluida la elaboración de perfiles relacionados, los datos personales dejarán de ser tratados para tales finalidades. Este derecho deberá ser informado de forma clara y separada desde la primera comunicación con el Titular. En los servicios de la sociedad de la información, el ejercicio de este derecho podrá realizarse mediante medios automatizados que apliquen especificaciones técnicas accesibles.

Artículo 10. Modifíquese el artículo 9° de la Ley 1581 de 2012, el cual quedará así:

Artículo 9°. ***Bases que legitiman el Tratamiento.***

El Tratamiento de Datos Personales será legítimo si se cumple al menos una de las siguientes condiciones:

a) El Titular dio su autorización previa para el Tratamiento de sus Datos Personales para uno o varios fines específicos;

b) El Tratamiento es necesario para la ejecución de un contrato en el que el Titular es parte o para la aplicación, a petición de este, de medidas precontractuales;

c) El Tratamiento es necesario para el cumplimiento de un deber legal aplicable al Responsable del Tratamiento;

d) El Tratamiento es necesario para salvaguardar la vida o la salud del Titular o de otra persona natural;

e) El Tratamiento es necesario para el ejercicio de funciones públicas conferidas al Responsable del Tratamiento por la Constitución o la ley;

f) El Tratamiento es necesario para atender intereses legítimos del Responsable del tratamiento o de un tercero, siempre que dichos intereses no prevalezcan sobre los derechos, garantías e intereses fundamentales del Titular que requieran la protección de sus Datos Personales, considerando las expectativas razonables del Titular en su relación con el Responsable, especialmente cuando se trate de menores de edad.

Parágrafo 1°. Lo dispuesto en el literal f) no será de aplicación al Tratamiento realizado por entidades públicas en el ejercicio de sus funciones.

Parágrafo 2°. Para fundamentar la existencia de un interés legítimo que justifique la necesidad del Tratamiento, el Responsable deberá realizar una ponderación previa, detallada y documentada que evalúe la licitud, necesidad y equilibrio del tratamiento en relación con los derechos y garantías fundamentales del Titular. En estos casos, deberá reforzarse el cumplimiento de todos los principios aplicables, en particular los de lealtad, minimización de datos y proporcionalidad.

Parágrafo 3°. En el marco de una actuación administrativa la Autoridad de Protección de Datos Personales podrá requerir al Responsable del Tratamiento el análisis previo que fundamenta

el Tratamiento de los Datos Personales para la satisfacción de un interés legítimo, y el Responsable del Tratamiento deberá ser capaz de demostrar la existencia del interés legítimo, la necesidad de recolectar o tratar los datos en cada caso, y los criterios de razonabilidad y proporcionalidad considerados para acotar dicho Tratamiento, teniendo para sí la carga de la prueba.

Parágrafo 4°. El Gobierno nacional expedirá la reglamentación correspondiente sobre las condiciones que deberán cumplirse para cada una de las bases que legitiman el Tratamiento de Datos Personales durante los seis (6) meses siguientes a la promulgación de la presente ley.

Parágrafo 5°. 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 de lo dispuesto en los literales c) y e), fijando de manera precisa requisitos específicos de tratamiento y otras medidas de conformidad con la presente ley.

Artículo 11. Subróguese el artículo 10 de la Ley Estatutaria 1581 de 2012, el cual quedará así:

Artículo 10. Condiciones para la autorización. Cuando el Tratamiento se base en la autorización del Titular, el Responsable del Tratamiento deberá estar en capacidad de demostrar que el Titular otorgó su autorización de manera previa, expresa, libre, específica, informada e inequívoca, para una o varias finalidades determinadas, mediante una declaración o una clara acción afirmativa. Cuando el Tratamiento tenga múltiples fines, deberá obtenerse el consentimiento para cada uno de ellos. El silencio, las casillas preseleccionadas o la inacción no constituirán manifestaciones válidas de autorización.

Cuando la autorización del Titular se otorgue en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de autorización deberá presentarse de forma claramente distinguible respecto de los demás contenidos, indicando de manera separada y accesible cada finalidad del Tratamiento, utilizando un lenguaje claro, sencillo y comprensible. No será vinculante ninguna parte de la declaración que constituya infracción de la presente ley.

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.

Parágrafo. Las calidades de la autorización se entenderán de la siguiente manera:

a) Previa. La autorización debe solicitarse antes de la recolección de los Datos personales;

b) Expresa. El Titular debe exteriorizar su voluntad con una clara acción afirmativa;

c) Libre. La autorización debe estar exenta de vicios;

d) Específica. Cuando el Tratamiento tenga varios fines, el Titular debe poder otorgar su autorización para cada uno de ellos;

e) Informada. El Titular debe contar al momento de la solicitud de la autorización con la información establecida en el artículo 12 de esta ley;

f) Inequívoca. No debe existir dudas sobre el alcance de la autorización otorgada por el Titular.

Artículo 12. Modifíquese el artículo 11 de la Ley 1581 de 2012, el cual quedará así:

Artículo 11. ***Transparencia de la información.*** El responsable del tratamiento tomará las medidas pertinentes para facilitar al titular toda la información indicada en el artículo 12, así como cualquier comunicación correspondiente a los ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular de conformidad con la presente ley, en forma concisa, transparente, comprensible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un menor.

La información deberá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso.

La información que deba facilitarse a los titulares en virtud del artículo 12 podrá compartirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, comprensible 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.

Parágrafo 1°. El Gobierno nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal, Esta reglamentación deberá darse a más tardar dentro del año siguiente a la promulgación de la presente ley.

Parágrafo 2°. La Autoridad de protección de datos establecerá las reglas para el uso de íconos normalizados que permitan al responsable o encargado del tratamiento cumplir con el deber de información, comunicar políticas de tratamiento, divulgar medidas de seguridad, notificar derechos de los titulares y otras circunstancias en las que sea necesaria su aplicación.

Artículo 13. Modifíquese el artículo 12 de la Ley 1581 de 2012, el cual quedará así:

Artículo 12. ***Deber de informar al Titular.***

1. El Responsable del Tratamiento deberá informar al Titular, en el momento en que obtenga los datos personales, ya sea directamente o a través de terceros, sobre lo siguiente:

a) Nombre o razón social, dirección física o electrónica y teléfono del Responsable del Tratamiento, y en el supuesto de los Responsables no establecidos en Colombia, los de su Representante en el territorio nacional;

b) Las finalidades del Tratamiento y sus bases legitimadoras;

c) Los derechos que le asisten como Titular de conformidad con el artículo 8 de la presente ley;

d) Los datos de contacto del Oficial de Protección de Datos, área o persona encargada de la protección de Datos Personales;

e) Los destinatarios de los Datos Personales, si los hubiera;

f) En caso de ser procedente, la intención del Responsable del Tratamiento de transferir Datos Personales a un tercer país u organización internacional y la existencia o ausencia de un reconocimiento de adecuación por parte de la Autoridad de Protección de Datos Personales;

g) El plazo durante el cual se conservarán los Datos Personales o, cuando no sea posible, los criterios utilizados para determinar dicho plazo;

h) La existencia de decisiones basadas en tratamientos automatizados, 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;

i) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que el ejercicio de sus derechos no ha sido debidamente tramitado o se haya infringido lo establecido en la presente ley;

2. Si los datos no han sido obtenidos del Titular, el Responsable del Tratamiento debe proveer la información prevista en el presente artículo al momento del primer contacto o dentro de un plazo razonable que no puede exceder de un (1) mes desde su obtención. Además de la información detallada en el numeral 1 del presente artículo, el Responsable del Tratamiento deberá indicarle al Titular cual es la fuente de la que proceden los Datos Personales.

Parágrafo. El responsable del tratamiento deberá estar en capacidad de demostrar el cumplimiento de lo dispuesto en el presente artículo, cuando así lo soliciten el Titular o la autoridad de protección de datos.

Artículo 14. Adiciónese el artículo 13ª a la Ley 1581 de 2012, el cual quedará así:

Artículo 13A. ***Garantías para consultas o reclamos.*** El Responsable del Tratamiento deberá facilitar al Titular mecanismos sencillos, accesibles y ágiles para la presentación de consultas y reclamos, a fin de garantizar el ejercicio efectivo de los derechos reconocidos en la presente ley.

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.

Artículo 15. Modifíquese el artículo 14 de la Ley 1581 de 2012, el cual quedará así:

Artículo 14. ***Consultas***. Los Titulares o sus causahabientes podrán acceder a la información personal del Titular que sea objeto de tratamiento, ya sea por el sector público o privado. El Responsable o Encargado del Tratamiento deberán suministrar a estos toda la información que concierna o que esté vinculada con el Titular.

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Parágrafo. Las disposiciones contenidas en leyes especiales o los reglamentos expedidos por el Gobierno nacional podrán establecer términos inferiores, atendiendo a la naturaleza del dato personal.

Artículo 16. Modifíquese el artículo 15 de la Ley 1581 de 2012, el cual quedará así:

Artículo 15. ***Reclamos*****.** El Titular, o sus causahabientes, podrán presentar un reclamo ante el Responsable del Tratamiento en ejercicio de los derechos previstos en el artículo 8° de la presente ley, o cuando adviertan un presunto incumplimiento de los deberes establecidos en la misma. El reclamo se tramitará conforme a las siguientes reglas:

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Cuando el reclamo recibido sea por el ejercicio del derecho de oposición, el Responsable deberá cesar el tratamiento de los datos personales, salvo que acredite motivos legítimos que prevalezcan sobre los derechos, intereses y garantías del titular, o cuando el tratamiento sea necesario

para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales. Cuando el reclamo sea por el ejercicio del derecho de limitación del tratamiento, el Responsable deberá implementar medidas técnicas y organizativas para garantizar que dichos datos no sean objeto de tratamiento, salvo que dicho tratamiento se realice exclusivamente para su conservación, o cuente con la autorización explícita del Titular, o sea necesario para proteger los derechos e intereses de un tercero. El Responsable del Tratamiento deberá notificar al Titular cuando se levante dicha limitación.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado 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.

Artículo 17. Modifíquese el artículo 17 de la Ley 1581 de 2012, el cual quedará así:

Artículo 17. ***Deberes de los Responsables del Tratamiento*****.** 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:

a) Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales;

b) Contar con una base jurídica que legitime el tratamiento de datos personales, de conformidad con lo establecido en la presente ley, y, cuando la base de legitimación sea la autorización del Titular, conservar prueba de su otorgamiento;

c) Informar debidamente al Titular lo establecido en el artículo 12 de la presente ley y conservar prueba de su cumplimiento;

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su daño, la destrucción, pérdida o alteración accidental o intencional de datos personales, acceso no autorizado o fraudulento. Revisar y actualizar dichas condiciones cuando sea necesario;

e) Garantizar que el personal, con acceso a datos personales reciba formación sobre protección de datos y se comprometa por escrito a mantener la confidencialidad y cumplir con las medidas de seguridad;

f) Actualizar o rectificar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;

g) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente legitimado de conformidad con lo previsto en la presente ley;

h) Elegir un Encargado o Encargados del Tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, asegurando el cumplimiento de las condiciones de seguridad y privacidad de la información del Titular;

i) Formalizar mediante un contrato la prestación de servicios de Tratamiento de datos con el Encargado de conformidad con el artículo 17C;

j) Garantizar el pleno ejercicio de los derechos que le conciernen a los titulares, tramitando las consultas y reclamos formulados en los términos señalados en la presente ley;

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;

l. Cumplir las órdenes, instrucciones y requerimientos que imparta la Autoridad de Protección de Datos Personales;

m) Realizar una evaluación del impacto relativa a la protección de los Datos Personales en los términos establecidos en los artículos 17A y 17B, cuando a ello haya lugar;

n) Garantizar que las transferencias internacionales cumplan las condiciones establecidas en la presente ley;

o) Implementar medidas técnicas y organizativas pertinentes para garantizar y poder demostrar el adecuado cumplimiento de la presente ley y las normas reglamentarias, especialmente los derechos de los Titulares de los datos y la materialización de los principios del Tratamiento de Datos Personales. Para lo cual se tendrá en cuenta, entre otras, las medidas establecidas en el artículo 18A;

p) Aplicar medidas técnicas y organizativas apropiadas tanto con anterioridad como durante el Tratamiento de datos, a fin de cumplir los principios y los derechos de los Titulares de los datos establecidos en la presente Ley. Para lo cual se tendrá en cuenta las medidas establecidas en el artículo 18B;

q) Designar un Oficial de Protección de Datos en los términos establecidos en los artículos 18C y 18D;

r) Informar a la Autoridad de Protección de Datos Personales y al Titular de los Datos Personales cuando se presenten incidentes de seguridad y existan riesgos en la administración de la información de los Titulares. Para lo que se considerarán las medidas establecidas en el artículo 18E.

s) Realizar, al menos cada dos años, una revisión interna o externa de los sistemas de información y los medios para el tratamiento de los datos personales, con el fin de verificar el cumplimiento de la presente ley. Esta revisión deberá adelantarse de forma extraordinaria cuando se introduzcan modificaciones sustanciales en los sistemas que puedan afectar dicho cumplimiento, reiniciando en ese caso el cómputo de los dos años.

Parágrafo. Cuando dos o más responsables determinen conjuntamente los fines y medios del tratamiento, serán considerados corresponsables. Deberán acordar de forma transparente sus respectivas obligaciones, en especial sobre el trámite de consultas y reclamos, y el deber de información. Los aspectos esenciales del acuerdo estarán a disposición del titular, quien podrá ejercer sus derechos frente a cualquiera de los corresponsables.

Artículo 18. Adiciónese el Artículo 17A a la Ley 1581 de 2012, el cual quedará así:

Artículo 17A. ***Evaluación de impacto relativa a la protección de Datos Personales***. Cuando el Responsable prevea realizar un tipo de Tratamiento que, en particular implique el uso de nuevas tecnologías, y por su naturaleza, alcance, contexto o finalidades, pueda entrañar un alto riesgo para los derechos y garantías de los Titulares amparados por la presente ley, deberá llevar a cabo, con carácter previo a su implementación, una evaluación de impacto relativa a la protección de los Datos Personales.

Esta evaluación es obligatoria en los siguientes casos, sin perjuicio de otros que establezca la Autoridad de Protección de Datos Personales:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas naturales que se base en un Tratamiento de datos automatizado y semiautomatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que las afecten significativamente;

b) Tratamiento de datos sensibles a gran escala;

c) Observación sistemática a gran escala de una zona de acceso público.

Parágrafo 1°. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

Parágrafo 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.

Parágrafo 3°. La zona de acceso público a la que se refiere el presente artículo comprende cualquier lugar físico, ya sea de propiedad pública o privada, al que pueda acceder un número indeterminado de personas naturales, independientemente de que existan condiciones específicas para su acceso o restricciones en cuanto a su capacidad.

Artículo 19. Adiciónese el Artículo 17B a la Ley 1581 de 2012, el cual quedará así:

Artículo 17B. ***Contenido de la evaluación de impacto***. La evaluación debe incluir, como mínimo:

a) Una descripción sistemática de las operaciones de Tratamiento de datos previstas y de los fines del Tratamiento, incluyendo, cuando proceda, el interés legítimo perseguido por el Responsable de Tratamiento;

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de Tratamiento de datos con respecto a su finalidad;

c) Una evaluación de los riesgos que podría generar a los derechos de los Titulares de los Datos Personales;

d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los Datos Personales, y para demostrar la conformidad con la presente ley, teniendo en cuenta los derechos e intereses legítimos de los Titulares y de otras personas que pudieran verse potencialmente afectadas.

Parágrafo. Cuando una evaluación de impacto evidencie que el Tratamiento entraña un alto riesgo de afectación a los derechos y garantías de los Titulares, el Responsable del Tratamiento debe informar de esta circunstancia a la Autoridad de Protección de Datos Personales. Por su parte, la Autoridad de Protección de Datos Personales podrá pronunciarse sobre el informe.

Artículo 20. Adiciónese el Artículo 17C a la Ley 1581 de 2012, el cual quedará así:

Artículo 17C. ***Contrato de Encargado del tratamiento***. El Tratamiento deberá regirse por un contrato u otro acto jurídico, que deberá constar por escrito, inclusive en formato electrónico, conforme a las normas civiles o mercantiles que vincule al Encargado respecto del Responsable, y que establezca, al menos, el objeto, la duración, la naturaleza, la finalidad del Tratamiento, el tipo de Titulares, las categorías de Datos Personales, así como las obligaciones y derechos del Responsable. Dicho contrato deberá estipular, en particular, que el Encargado:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias internacionales de datos personales, salvo que esté obligado a ello en virtud de un mandato legal que se aplique al Encargado o por razones de interés público.

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.

c) Tomará todas las medidas de seguridad necesarias de conformidad a la presente ley.

d) 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.

e) Asistirá al Responsable, teniendo en cuenta la naturaleza del Tratamiento, mediante la adopción de medidas técnicas y organizativas apropiadas, en la atención de las consultas y reclamos presentados por los Titulares. Cuando así se pacte, podrá asumir directamente, por cuenta del Responsable y dentro de los plazos establecidos en la presente ley, la gestión de dichas solicitudes.

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.

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.

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.

Parágrafo 1°. 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.

Parágrafo 2°. 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 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.

Parágrafo 3°. El responsable del tratamiento podrá exigir a los encargados que presten servicios tecnológicos, aplicaciones o infraestructura tecnológica, cuando la relación se establezca mediante condiciones generales de contratación, que acrediten el cumplimiento de la presente ley. En caso de que el proveedor ignore los requerimientos del responsable o incumpla con sus obligaciones legales, este podrá poner los hechos en conocimiento de la autoridad de protección de datos. Lo anterior no exime al responsable de la obligación de seleccionar un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.

Artículo 21. Modifíquese el artículo 18 de la Ley 1581 de 2012, el cual quedará así:

Artículo 18. ***Deberes de los Encargados del Tratamiento.*** 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:

a) Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales;

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su daño, la destrucción, pérdida o alteración accidental o intencional de datos personales, acceso no autorizado o fraudulento. Revisar y actualizar dichas condiciones cuando sea necesario;

c) 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;

d) Utilizar los datos personales objeto de tratamiento, solo para la finalidad del encargo. En ningún caso podrá utilizar los datos para fines propios;

e) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

f) Colaborar con el Responsable del Tratamiento y proporcionarle, en tiempo oportuno, toda la información y asistencia necesaria para atender las consultas y reclamos formulados por los Titulares, conforme a los términos establecidos en la presente ley;

g) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley;

h) Abstenerse de realizar un Tratamiento sobre información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Autoridad de Protección de Datos Personales;

i) 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 de Protección de Datos Personales, la documentación que demuestre el cumplimiento de estas obligaciones;

j) Cumplir las órdenes, instrucciones y requerimientos que imparta la Autoridad de Protección de Datos Personales;

k) Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando sea el caso;

l) Implementar medidas técnicas y organizativas pertinentes para garantizar y poder demostrar el adecuado cumplimiento de la presente ley y las normas reglamentarias, especialmente los derechos de las personas Titulares de los datos y la materialización de los principios del Tratamiento de Datos Personales. Para lo cual se tendrá en cuenta las medidas establecidas en el artículo 18A;

m) Designar un Oficial de Protección de Datos en los términos establecidos en los artículos 18C y 18D;

n) El encargado informará al responsable del tratamiento, en tiempo oportuno, 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;

o) Formalizar mediante un contrato la prestación de servicios de Tratamiento de datos con el Responsable;

p) No subcontratar ninguna de las prestaciones que formen parte del encargo, salvo que cuente con autorización expresa del responsable.

q) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento;

r) Devolver, una vez cumplida la prestación contractual, al Responsable del Tratamiento los Datos Personales tratados, salvo que medie autorización expresa del Responsable de Tratamiento cuando razonablemente se pueda presumir la posibilidad de ulteriores encargos, en cuyo caso solo podrán conservarse por un máximo de dos (2) años;

s) Facilitarle al Responsable del Tratamiento y a la Autoridad de Protección de Datos Personales realizar inspecciones o auditorías para verificar el cumplimiento de la ley y de lo pactado en el contrato.

Artículo 22. Adiciónese el artículo 18A a la Ley 1581 de 2012, el cual quedará así:

Artículo 18A. ***Medidas para el cumplimiento de la Responsabilidad Demostrada.*** Teniendo en cuenta el estado de la tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de probabilidad y gravedad, variables para los derechos y garantías de los titulares, las medidas adoptadas para el cumplimiento de las disposiciones de la presente ley deben ser útiles, oportunas, pertinentes, efectivas y proporcionales a dichas condiciones del tratamiento de datos personales. Deben contemplar, como mínimo:

a) La adopción de procesos internos para llevar adelante de manera efectiva las medidas de responsabilidad;

b) La implementación de procedimientos para atender el ejercicio de los derechos por parte de los Titulares de los datos;

c) La realización de supervisiones o auditorías, internas o externas, para controlar el cumplimiento de las medidas adoptadas;

d) Implementación de procedimientos de evaluación de impacto conforme a lo establecido en la presente ley;

e) La implantación de medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado al riesgo. Cuando sea pertinente, dichas medidas incluirán, entre otras, la seudonimización y el cifrado de datos personales, mecanismos que aseguren la resiliencia de los sistemas y medios de tratamiento, la capacidad de restaurar la disponibilidad y el acceso a los datos personales en caso de incidente, así como procesos para evaluar la eficacia de las medidas implementadas;

f) La adopción de mecanismos de autorregulación como la adhesión a códigos de conducta o un mecanismo de certificación verificado por la Autoridad de Protección de Datos.

Parágrafo. El Gobierno nacional reglamentará lo concerniente a los códigos de conducta y mecanismos de certificación, dentro de los seis (6) meses siguientes a la promulgación de esta ley.

Artículo 23. Adiciónese el Artículo 18B a la Ley 1581 de 2012, el cual quedará así:

Artículo 18B. Protección de datos desde el diseño y por defecto. Los Responsables del Tratamiento deberán aplicar medidas técnicas y organizativas apropiadas, tanto al momento de determinar los medios como durante el Tratamiento de datos personales, con el fin de garantizar la aplicación efectiva de los principios y el respeto de los derechos de los Titulares consagrados en la presente ley.

Dichas medidas deberán adoptarse teniendo en cuenta el estado de la tecnología, los costos de implementación, así como la naturaleza, el ámbito, el contexto y los fines del Tratamiento, y los riesgos de diversa probabilidad y gravedad que dicho Tratamiento pueda suponer para los derechos de los Titulares.

Asimismo, deberán implementarse medidas técnicas y organizativas apropiadas que garanticen, por defecto, la protección de los datos personales en la toma de decisiones relativas a valores de configuración u opciones de tratamiento predeterminadas en los sistemas o medios utilizados, de modo que únicamente se lleve a cabo el tratamiento estrictamente necesario para cada uno de los fines específicos del mismo. Esta obligación se refiere a la cantidad de datos recabados, la extensión del tratamiento, el plazo de conservación y el grado de accesibilidad a los datos.

En particular, dichas medidas deberán asegurar que, por defecto, los datos personales solo sean accesibles al personal autorizado, salvo que el contexto del tratamiento exija lo contrario.

Artículo 24. Adiciónese el Artículo 18C a la Ley 1581 de 2012, el cual quedará así:

Artículo 18C. ***Oficial de Protección de Datos.*** Los Responsables y Encargados del Tratamiento deben designar un Oficial de Protección de Datos Personales, cuyas funciones se establecen en el artículo 18D de la presente ley, en cualquiera de los siguientes casos:

a) Cuando el Tratamiento lo lleve a cabo una autoridad u organismo público;

b) Se realice Tratamiento de datos sensibles como parte de la actividad principal del Responsable o Encargado del Tratamiento;

c) Se realice Tratamiento de datos a gran escala.

Cuando se trate de una autoridad u organismo público con dependencias adscritas, se puede designar un único Oficial de Protección de Datos Personales, teniendo en consideración su tamaño, estructura organizativa y presupuesto.

Un Grupo Empresarial puede nombrar un único Oficial de Protección de Datos Personales siempre que esté en contacto permanente con cada una de las empresas que lo componen.

La designación del Oficial de Protección de Datos Personales debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones. Además, la Autoridad de protección de datos podrá verificar su capacidad para desempeñar las funciones indicadas en esta ley.

Las funciones del Oficial de Protección de Datos Personales pueden ser desempeñadas por un empleado del Responsable o Encargado del Tratamiento o en el marco de un contrato de prestación de servicios.

Los Responsables y Encargados del Tratamiento estarán obligados a apoyar al Oficial de Protección de Datos Personales en el ejercicio de sus funciones, proporcionándole los recursos necesarios para su adecuado desempeño, así como para el mantenimiento y actualización de sus conocimientos especializados.

Los Responsables y Encargados del Tratamiento garantizarán que el Oficial de Protección de Datos Personales pueda llevar a cabo sus funciones de manera autónoma y libre de interferencias externas. El Oficial de Protección de Datos Personales no será destituido ni sancionado por desempeñar adecuadamente sus funciones. Solo responderá ante el más alto nivel jerárquico de la organización.

Parágrafo 1°. Cuando los Responsables y Encargados del Tratamiento no se encuentren obligados a la designación de un Oficial de Protección de Datos Personales de acuerdo con lo previsto en este artículo, pero decidan designarlo de manera voluntaria, el Oficial de Protección de Datos designado tendrá las funciones previstas en el artículo 18D de la presente ley.

Parágrafo 2°. Cuando los Responsables y Encargados del Tratamiento no se encuentren obligados a la designación de un Oficial de Protección de Datos Personales de acuerdo con lo previsto en este artículo, la Autoridad de Protección de Datos Personales una vez surtida la actuación administrativa correspondiente podrá ordenar su designación y este tendrá las funciones previstas en el artículo 18D de la presente ley.

Parágrafo 3°. 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. 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.

Artículo 25. Adiciónese el Artículo 18D a la Ley 1581 de 2012, el cual quedará así:

Artículo 18D. ***Funciones del Oficial de Protección de Datos Personales***. El Oficial de Protección de Datos Personales tiene las siguientes funciones, sin perjuicio de otras que se le asignen:

a) Informar y asesorar a los Responsables y Encargados del Tratamiento, así como a sus empleados, de las obligaciones a su cargo;

b) Promover y participar en el diseño y aplicación de la Política de Tratamiento de Información del Responsable y/o Encargado;

c) Supervisar el cumplimiento de la presente ley y de la Política de Tratamiento de Información del Responsable y/o Encargado;

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;

e) Asignar responsabilidades, concientizar, formar al personal y realizar las auditorías correspondientes;

f) Ofrecer el asesoramiento que se le solicite para hacer una evaluación de impacto relativa a la protección de datos y supervisar posteriormente su aplicación;

g) Cooperar y actuar como contacto ante las autoridades para cualquier consulta sobre el Tratamiento de datos efectuado por el Responsable o Encargado de Tratamiento;

h) Mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones;

i) 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.

Artículo 26. Adiciónese el Artículo 18E a la Ley 1581 de 2012, el cual quedará así:

Artículo 18E. ***Notificación de incidentes de seguridad***. En caso de que ocurra un incidente de seguridad de los Datos Personales, los Responsables del Tratamiento deben notificarlo a la Autoridad de Protección de Datos Personales dentro de las setenta y dos (72) horas de haber tenido conocimiento de aquel.

Si no hay medios materiales para notificar en el plazo previsto, deberá solicitar ante la Autoridad de Protección de Datos Personales la extensión del plazo, justificando objetivamente dicha necesidad.

La notificación debe contener, al menos, la siguiente información:

a) La naturaleza del incidente;

b) Los Titulares y Datos Personales que pueden estimarse afectados;

c) Describir las posibles consecuencias del incidente de seguridad de los datos personales;

d) Las acciones correctivas adoptadas, y si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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, los Responsables del Tratamiento deben comunicar al Titular de los datos sobre el incidente de seguridad ocurrido, en un lenguaje claro y sencillo, debiendo incluir en la comunicación, además de lo establecido en los literales a), b), c) y d), los medios a disposición del Titular para obtener más información al respecto, incluido el nombre y datos de contacto del Oficial de Protección de Datos Personales o cualquier otra persona o área designada como contacto.

Si la comunicación a los titulares supone un esfuerzo desproporcionado, dicha comunicación puede realizarse mediante comunicación pública o una medida de difusión semejante, si es igualmente efectiva para informar al Titular sobre el incidente.

Parágrafo 1°. Los Responsables del Tratamiento deben documentar todo incidente de seguridad que ponga en alto riesgo los derechos de los Titulares de los datos, ocurrido en cualquier fase del Tratamiento de datos e identificar, de manera enunciativa, pero no limitativa, la fecha en que ocurrió, el motivo del incidente, los hechos relacionados con este y sus efectos, y las medidas correctivas implementadas de forma inmediata y definitiva. En caso de que no sea posible enviar toda la información detallada al mismo tiempo, los Responsables del Tratamiento deberán enviarla a medida que sea posible y sin dilación alguna que le sea imputable.

Parágrafo 2°. El encargado del tratamiento notificará, en tiempo oportuno, al responsable del tratamiento, los incidentes de seguridad de los datos personales de los que tenga conocimiento.

Artículo 27. Modifíquese el Artículo 19 de la Ley 1581 de 2012, el cual quedará así:

Artículo 19. ***Autoridad de Protección de Datos Personales***. La Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales, será la Autoridad de Protección de Datos Personales, y ejercerá de manera imparcial, autónoma e independiente la vigilancia para garantizar que en el Tratamiento de Datos Personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Parágrafo. La vigilancia del Tratamiento de los Datos Personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

Artículo 28. Adiciónese el Artículo 19A a la Ley 1581 de 2012, el cual quedará así:

Artículo 19A. ***Dirección de la Autoridad de Protección de Datos.*** La Autoridad de Protección de Datos Personales estará a cargo de un Delegado para la Protección de Datos Personales que será nombrado por el Superintendente de Industria y Comercio para un periodo fijo de cinco (5) años, previa convocatoria pública, efectuada a través del portal de internet de la Superintendencia, a quienes cumplan con los requisitos y condiciones para ocupar el respectivo cargo. El Gobierno nacional reglamentará lo relacionado con el procedimiento aplicable para su nombramiento.

Artículo 29. Modifíquese el artículo 21 de la Ley 1581 de 2012, el cual quedará así:

Artículo 21. ***Competencias y funciones.*** La Autoridad de Protección de Datos Personales ejercerá las siguientes funciones:

a) Velar por el cumplimiento de la legislación en materia de protección de Datos Personales;

b) Adelantar las investigaciones a que haya lugar, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo cualquiera de los derechos y deberes consagrados en la presente ley;

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva, o cuando se trate de los ejercicios de los derechos de oposición o limitación del tratamiento;

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de Datos Personales e implementar campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;

e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;

f) Ordenar a cargo del Responsable o Encargado del Tratamiento la realización de auditorías externas de sistemas para verificar el cumplimiento de las disposiciones de la presente ley;

g) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones;

h) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos, incluyendo decisiones de adecuación; aprobación de cláusulas contractuales modelo; adopción de mecanismos de certificación y, cuando ello resulte necesario, sobre normas corporativas vinculantes y contratos celebrados para el flujo internacional de datos;

i) Desarrollar y promover mecanismos de autorregulación orientados a la elaboración de códigos de conducta y esquemas de certificación que contribuyan a la adecuada aplicación de la presente ley;

j) Administrar el Registro de las Actividades del Tratamiento y emitir las órdenes y los actos necesarios para su administración y funcionamiento;

k) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional;

l) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de Datos Personales;

m) Promover acciones de cooperación y armonización normativa con autoridades de protección de Datos Personales de otros países, organismos u organizaciones internacionales, y Estados subnacionales; y celebrar convenios de cooperación con organizaciones públicas o privadas, nacionales o extranjeras, en el ámbito de su competencia, para el cumplimiento de sus funciones;

n) Promover e implementar mecanismos alternativos de solución de controversias en materia de Tratamiento de Datos Personales para que los Titulares y los Responsables o Encargados voluntariamente lleguen a acuerdos para garantizar el debido Tratamiento de los Datos Personales;

o) Podrá pronunciarse sobre las evaluaciones de impacto que le sean comunicadas por los Responsables del Tratamiento que identifiquen un alto riesgo de afectación a los derechos de los Titulares;

p) Ordenar la designación de un Oficial de Protección de Datos Personales a los Responsables y Encargados del Tratamiento, una vez surtida la actuación administrativa correspondiente;

q) Emitir órdenes administrativas de obligatorio cumplimiento para garantizar el debido Tratamiento de los Datos Personales y los derechos de los Titulares de los Datos Personales;

r) Requerir a los responsables y encargados del tratamiento sobre presuntas infracciones a la presente ley;

s) Imponer multas de carácter personal o institucional cuando las operaciones de tratamiento hayan infringido lo establecido en la presente ley;

t) Las demás que le sean asignadas por la ley.

Parágrafo 1°. 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 2°. 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.

Artículo 30. Modifíquese el artículo 23 de la Ley 1581 de 2012, el cual quedará así:

Artículo 30. ***Sanciones.*** La Autoridad de Protección de Datos Personales podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) 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. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) Cierre 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 Personales;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

Parágrafo. Las sanciones indicadas en el presente artículo solo aplican para las personas de naturaleza privada. En el evento en el cual la Autoridad de Protección de Datos Personales advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Artículo 31. Modifíquese el artículo 24 de la Ley 1581 de 2012, el cual quedará así:

Artículo 24. ***Criterios para graduar las sanciones***. Las sanciones por infracciones a las que se refieren el artículo anterior se graduarán atendiendo los siguientes criterios, en cuanto 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 beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

c) Si existió dolo o negligencia en la comisión de la infracción;

d) La reincidencia en la comisión de la infracción;

e) Afectación a los derechos de niñas, niños y adolescentes;

f) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;

g) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;

h) 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;

i) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar;

j) Cualquier medida tomada por el infractor para contener y mitigar los daños y perjuicios sufridos por los titulares;

k) Disponer, cuando no fuere obligatorio, de un Oficial de protección de datos;

l) La implementación efectiva de medidas de responsabilidad demostrada.

Artículo 32. Modifíquese el artículo 25 de la Ley 1581 de 2012, el cual quedará así:

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:

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.

b) Los fines del tratamiento.

c) Una descripción de los tipos de titulares y de las categorías de datos personales.

d) Los destinatarios a quienes se cedieron o cederán los datos personales, incluidos los destinatarios en otros países u organizaciones internacionales.

e) Los encargados que intervienen en el tratamiento.

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 26B de la presente esta ley relativa a la documentación de garantías adecuadas.

g) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

h) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 18A de esta ley o la remisión al documento que las contenga.

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.

2. Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

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.

b) Las categorías de tratamientos efectuados por cuenta de cada responsable.

c) Los subencargados autorizados por el responsable, que intervienen en el tratamiento.

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.

e) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 18A de esta ley o la remisión al documento que las contenga.

3. Los registros a los que se refieren los numerales 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de protección de datos, cuando lo requiera.

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.

Parágrafo. A partir de la entrada en vigencia de la presente ley, toda referencia al Registro Nacional de Bases de Datos se entenderá realizada al Registro Nacional de las Actividades de Tratamiento.

Artículo 33. Subróguese el artículo 26 de la Ley Estatutaria 1581 de 2012, el cual quedará así:

Artículo 26. ***Decisión de Adecuación.*** Se podrán realizar transferencias de Datos Personales a países u organismos internacionales que proporcionen niveles adecuados de protección de datos.

Se entiende que un país o un organismo internacional ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Autoridad de Protección de Datos Personales sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Para emitir una decisión de adecuación, la Autoridad de Protección de Datos Personales 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;

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 Personales.

Parágrafo 1°. Sin perjuicio de los compromisos internacionales vigentes para Colombia, 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 Personales, podrá derogar, modificar o suspender, en la medida necesaria y sin efecto retroactivo, la decisión de adecuación.

Parágrafo 2°. En los primeros dos años posteriores a la entrada en vigencia de esta ley, la Autoridad de Protección de Datos Personales deberá revisar lo establecido en la Circular Única de la Superintendencia de Industria y Comercio relativo a las transferencias de Datos Personales, según los criterios establecidos en el artículo.

Parágrafo 3°. 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 Parágrafo 1°.

Artículo 34. Adiciónese el Artículo 26A a la Ley 1581 de 2012, el cual quedará así:

Artículo 26A. ***Garantías adecuadas.*** En ausencia de una decisión de adecuación de conformidad con el artículo 26 de la presente ley, se podrán realizar transferencias internacionales cuando los Responsables del Tratamiento involucrados en la transferencia brinden garantías adecuadas al Tratamiento de los Datos Personales, en cumplimiento de las condiciones mínimas y suficientes establecidas en la presente ley.

Los siguientes se consideran como garantías adecuadas:

I. Un instrumento jurídicamente vinculante y exigible, bilateral o multilateral, entre Colombia y organismos u organizaciones internacionales, y Estados subnacionales, que habilite las transferencias desde entidades privadas y/o públicas establecidas en Colombia hacia entidades privadas y/o públicas establecidas en otros países;

II. Acuerdos o convenios entre particulares que expresamente reconozcan los principios, derechos y obligaciones establecidos en la presente ley, los que pueden adoptar las siguientes formas:

a) Cláusulas contractuales modelo que hayan sido previamente aprobadas por la Autoridad de Protección de Datos Personales;

b) Normas corporativas vinculantes que hayan sido aprobadas por la Autoridad de Protección de Datos Personales y que se apliquen a todos los miembros de un Grupo Empresarial en los términos establecidos en su regulación;

c) Mecanismos de certificación en materia de protección de datos aprobados por la Autoridad de Protección de Datos Personales.

En los casos de transferencias regidas por el presente artículo, el acuerdo o mecanismo que instrumente la transferencia, debe reconocer que la parte importadora se encuentra sujeta a la jurisdicción de la Autoridad de Protección de Datos Personales y de los tribunales competentes de la República de Colombia, de manera que los Titulares de los datos cuenten con acciones legales efectivas para proteger sus derechos.

Artículo 35. Adiciónese el artículo 26B a la Ley 1581 de 2012, el cual quedará así:

Artículo 26B. ***Transferencias sin decisión de adecuación***. En ausencia de una decisión de adecuación, o de garantías adecuadas, se podrá realizar una transferencia específica y que no sea habitual cuando se trate de alguno de los siguientes casos:

a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;

b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;

d) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;

e) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Parágrafo. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Autoridad de Protección de Datos Personales, proferir la declaración de conformidad relativa a la transferencia internacional de Datos Personales. Para el efecto, la autoridad queda facultada para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Artículo 36. Adiciónese el Artículo 26C a la Ley 1581 de 2012, de la siguiente manera:

Artículo 26C. Las disposiciones contenidas en el Título VIII de la presente ley serán aplicables a todas las bases de datos y/o tratamientos, incluidas aquellas de la Ley 1266 de 2008.

Artículo 37. ***Régimen de transición.*** La presente ley entrará en vigencia un (1) año después de su promulgación. Durante dicho período, las personas obligadas a su cumplimiento deberán realizar las adecuaciones necesarias para garantizar el correcto ejercicio de sus actividades conforme a lo dispuesto en esta ley.

Parágrafo. 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 38. ***Vigencias y derogaciones***. La presente ley entrará en vigencia conforme a lo establecido en el régimen de transición y una vez sea publicada en el ***Diario Oficial***. Deroga todas las disposiciones que le sean contrarias.

De las y los Congresistas,

DUVALIER SÁNCHEZ ARANGO Representante a la Cámara por Valle del Cauca - Alianza Verde	MARÍA FERNANDA CARRASCAL ROJAS Representante a la Cámara por Bogotá
SARAY ELENA ROBAYO BECHARA Representante a la Cámara Departamento de Córdoba	DAVID ALEJANDRO TORO RAMIREZ Representante a la Cámara por Antioquia Pacto Histórico.
MARIA DEL MAR PIZARRO GARCÍA Representante a la Cámara por Bogotá	JAIME RAÚL SALAMANCA TORRES Representante a la Cámara por Boyacá Partido Alianza Verde
HERÁCLITO LANDÍNEZ SUÁREZ Representante a la Cámara Pacto Histórico	JAMES MOSQUERA TORRES REPRESENTANTE A LA CÁMARA CITREP CHOCO -ANTIOQUIA
ANIBAL GUSTAVO HOYOS FRANCO Representante a la Cámara por Risaralda Partido Liberal	ALIRIO URIBE MUÑOZ Representante a la Cámara
KAREN ASTRITH MANRIQUE OLARTE Representante a la Cámara CITREP 2 – Arauca	CRISTÓBAL CAICEDO ANGULO Representante a la Cámara por el Valle del Cauca

ETNA TÁMARA ARGOTE CALDERÓN Representante a la Cámara por Bogotá Pacto Histórico PDA	SANDRA RAMIREZ LOBO SILVA Senadora de la República Partido COMUNES
JUAN CAMILO LONDOÑO BARRERA Representante a la Cámara por Antioquia Partido Alianza Verde	GABRIEL BECERRA YAÑEZ Representante a la Cámara por Bogotá Pacto Histórico - Unión Patriótica
SANTIAGO OSORIO MARIN Representante a la Cámara Caldas Partido Alianza Verde	ÁLVARO LEONEL RUEDA CABALLERO Representante a la Cámara Departamento de Santander
MODESTO AGUILERA VIDES Representante a l Cámara Departamento del Atlántico Cambio Radical	CRISTIAN DANILO AVENDAÑO FINO Representante a la Cámara Departamento de Santander
JORGE HERNAN BASTIDAS ROSERO Representante a la Cámara por el Cauca Pacto Histórico	GLORIA INÉS FLÓREZ SCHNEIDER Senadora de la República Pacto Histórico-Colombia Humana

EXPOSICIÓN DE MOTIVOS

PROYECTO DE LEY ESTATUTARIA NÚMERO 214 DE 2025 CÁMARA

por la cual se reforma la Ley 1581 de 2012 y se dictan otras disposiciones generales relativas a la protección de datos personales.

La presente exposición de motivos está compuesta por once (11) apartes:

1. Objeto del proyecto de ley.
2. Problema a resolver.
3. Antecedentes.
4. Justificación del proyecto.
5. Marco jurídico.
6. Fundamento normativo
7. Derecho comparado.
8. Conflicto de intereses.
9. Impacto Fiscal.
10. Conclusiones.
11. Referencias.

1. OBJETO DEL PROYECTO DE LEY

El presente proyecto de ley tiene por objeto modificar la Ley Estatutaria 1581 de 2012 con el fin de adecuarla a los desafíos actuales del entorno digital, fortalecer las garantías del derecho fundamental a la protección de datos personales y armonizar su aplicación con estándares internacionales y los

derechos fundamentales consagrados en los artículos 15 y 20 de la Constitución Política. La iniciativa mantiene el fundamento normativo existente y su enfoque garantista, al tiempo que introduce precisiones y mecanismos actualizados que permitan una protección más efectiva de los derechos de las personas naturales frente al tratamiento de sus datos personales y la circulación de los mismos.

2. PROBLEMA A RESOLVER

La ausencia de una normativa que permita la protección de datos de los ciudadanos, así como la pérdida de capacidad de la norma actual para abordar de manera adecuada los riesgos que suponen el uso de nuevas tecnologías en la privacidad de los individuos.

Así mismo, la Superintendencia de Industria y Comercio informó (a través de un derecho de petición) durante los últimos 10 años se han presentado 161.098 quejas por la presunta vulneración al derecho fundamental de *habeas data*. En la tabla 2 que se expone a continuación se detalla el número de quejas por año.

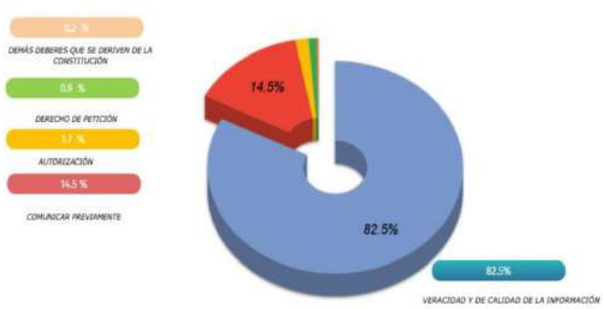
Tabla 2. Quejas presentadas durante (2013-2023 parcial)

Año	**Número de quejas**
2013	3.954
2014	5.634
2015	6.134
2016	6.875
2017	7.317
2018	10.057
2019	15.158
2020	18.920
2021	31.237
2022	37.973
2023	17.839
Total	**161.098**

Fuente: *Superintendencia de Industria y Comercio mediante derecho de petición.*

Los principales motivos por los cuales se han presentado las quejas como fundamento la Ley Estatutaria 1266 de 2008 entre 2010 y 2023, se deben principalmente a:

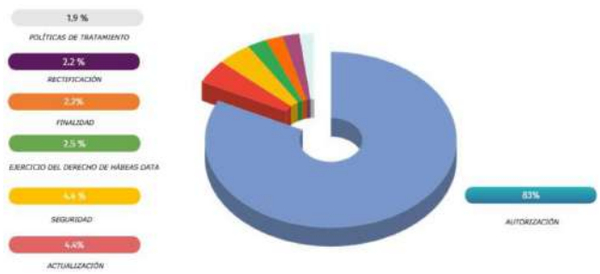
Imagen 1. Número de quejas



Tomado de: *Respuesta DP-Superintendencia de Industria y Comercio.*

De igual manera, los principales motivos por los cuales se han presentado las quejas como fundamento de la Ley Estatutaria 1581 de 2012 entre 2010 y 2023, se deben principalmente a:

Imagen 2. Número de quejas



Tomado de: Respuesta *DP-Superintendencia de Industria y Comercio.*

3. ANTECEDENTES

Es importante señalar que esta iniciativa legislativa ha sido radicada en dos oportunidades: inicialmente en la Legislatura 2023-2024 bajo el número de radicado PLE 156 de 2023 Cámara, y posteriormente en la Legislatura 2024-2025 con el número PLE 152 de 2024 Cámara. Aunque en ambas ocasiones no se logró completar el trámite legislativo, dichos procesos permitieron abrir espacios de diálogo ciudadano que resultaron fundamentales para enriquecer el contenido de la propuesta normativa. A partir de estos ejercicios de participación, se incorporaron múltiples recomendaciones formuladas por la Superintendencia de Industria y Comercio (SIC), así como por entidades públicas, la academia, organizaciones de la sociedad civil y ciudadanos que participaron en la audiencia pública y en mesas de trabajo temáticas.

Con el propósito de fortalecer esta iniciativa, se promovieron diversos espacios de participación ciudadana orientados a ajustar y consensuar el articulado, garantizando su pertinencia frente a las dinámicas de un entorno cada vez más interconectado, donde la información constituye un activo estratégico.

Uno de los mayores espacios de participación, se realizó el día siete (07) de marzo de 2024 por citación de los diez (10) ponentes de la Comisión Primera Constitucional Permanente de la Cámara de Representantes, para escuchar a todos los interesados en la misma.

A la audiencia pública fueron citados el Ministerio de las TIC, las Superintendencia Financiera de Colombia y la de Industria y Comercio; igualmente fueron invitados gremios, organizaciones, cámaras de comercio, universidades, académicos expertos y ciudadanía en general. Es de resaltar que atendiendo a que el objetivo de la presente norma es adecuarnos a los estándares internacionales, contamos con la participación de forma virtual de LEONARDO CERVERA CERVERA NAVAS -Secretario General Supervisor Europeo de Protección de Datos -SEPD- También participan en la audiencia pública integrantes de la academia, gremios y organizaciones de la sociedad civil, entre ellos MERIDIA LEGALTECH, quienes han sido apoyo fundamental en la construcción de la iniciativa legislativa.

Adicionalmente, se realizaron espacios de diálogo con la Superintendencia de Industria y Comercio y la Financiera de Colombia; con la Cámara de Comercio de Bogotá y con gremios y asociaciones para escuchar sus recomendaciones y comentarios sobre la iniciativa legislativa.

4. JUSTIFICACIÓN DE LAS DISPOSICIONES DEL PROYECTO DE LEY

4.1. Necesidad de actualizar la normatividad actual

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 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.

4.1.1. Del Objeto, ámbito de aplicación y definiciones

Si bien los objetivos y principios de la Ley 1581 de 2012 siguen siendo válidos, ello no ha impedido que la protección de datos en Colombia presente una serie de debilidades que han supuesto la necesidad de llevar a cabo una actualización de la legislación en la materia. Esta actualización se enfoca principalmente en regular cómo se deben proteger y tratar los datos personales, así como en promover la libre circulación de esos datos. Asimismo, reconoce la protección de los datos personales como derecho fundamental.

En lo que respecta al ámbito de aplicación este proyecto de ley centra su atención en el titular cuyos datos van a ser tratados, mientras que la normatividad actual coloca el foco en las personas jurídicas que los tratarán. Adicionalmente, se corrige la exclusión de las bases de datos reguladas por leyes específicas (Ley 79 de 1993, derogada por la Ley 2335 de 2023) que se encontraba en la Ley 1581 de 2012. De igual manera, se hace una ampliación del ámbito de aplicación, incluyendo criterio de aplicación territorial. Se establecen reglas claras sobre cómo la ley aplica a las diferentes circunstancias que el establecimiento de los responsables y encargados dentro o fuera del territorio colombiano imponga en torno al tratamiento de los datos personales. Esto permite establecer con mayor precisión los casos en los que la normativa colombiana se aplica. Además, se mantiene la protección de ciertos tratamientos de datos personales que ocurren fuera del territorio nacional, centrando su protección en la titularidad del dato.

En un mundo globalizado donde el flujo transfronterizo de datos es constante, la aplicación extraterritorial de los estándares de protección se vuelve indispensable para garantizar la adecuada protección de los datos personales de los residentes en Colombia. Esto es especialmente relevante dado que muchos tratamientos de datos, impulsados por las nuevas tecnologías, ocurren fuera de las fronteras del país. Por lo tanto, la reestructuración de la materia es una medida urgente y necesaria para asegurar el pleno ejercicio del derecho a la protección de datos. Esta disposición debe, además, leerse en conjunto con los artículos sobre transferencia de datos a terceros países.

Con el transcurso del tiempo, el ámbito de la protección de datos está experimentando un crecimiento significativo, lo cual ha generado un aumento en las dudas y la necesidad de abordar conceptos claves. El avance de la tecnología, el intercambio global de información y el surgimiento de nuevas formas de procesamiento de datos han planteado nuevos desafíos en términos de privacidad y seguridad. Surgen interrogantes sobre la definición y la aplicación de conceptos fundamentales en el ámbito de la protección de datos, que no venían definidos de una forma concreta. Es fundamental abordar estas inquietudes y promover un diálogo continuo para asegurar una protección efectiva y adecuada de los datos personales en un entorno en constante evolución, por lo que el repertorio de definiciones se ha visto incrementado de manera notable.

Finalmente, frente a las definiciones se incluyen nuevos conceptos no presentes en la legislación, como, por ejemplo:

- Anonimización.
- Cesión de datos.
- Datos biométricos.
- Datos genéticos.
- Datos relativos a la salud.
- Elaboración de perfiles.
- Incidente de seguridad.
- Servicio de la sociedad de la información.
- Seudonimización.
- Transferencia internacional de datos personales.
- Tratamiento a gran escala.

4.1.2. **Principios aplicables a la protección de datos**

Sobre los principios y normas relativas a la protección de las personas naturales, en lo que respecta al tratamiento de datos de carácter personal, se dispone el deber de respetar las libertades y derechos fundamentales, en particular, los descritos en los artículos 15 y 20 de la Constitución Política. Por lo tanto, es uno de los fines de la regulación cooperar para lograr la plena realización de un espacio de libertad, seguridad y justicia.

Se pone de manifiesto que el derecho a la información del artículo 20 de la Constitución Política debe ser considerado como un derecho independiente y no simplemente vinculado a la protección de datos. Este derecho se desarrolla de manera completa y, además, en concordancia con el derecho a la protección de datos (Defensoría del pueblo, 2011, como se cita en Corte Constitucional, Sala plena, Sentencia del 6 de octubre de 2011, exp. PE 032).

En ese sentido, se introducen los principios de lealtad, minimización de datos, limitación del plazo de conservación, proporcionalidad, explicabilidad y responsabilidad demostrada. Estos principios adicionales en el artículo 4° buscan fortalecer la protección de datos y promover un tratamiento más responsable y ético, teniendo en cuenta aspectos como la finalidad del tratamiento, la precisión de los datos, la limitación en la recopilación de datos y la proporcionalidad en el uso de los mismos.

Es importante advertir la importancia de reducir la intrusión en la esfera privada de los titulares de datos personales, y lo fundamental que resulta que el tratamiento de dichos datos priorice la limitación de las finalidades para las cuales se recopilan, así como la minimización del volumen de datos recabados. Además, es necesario establecer limitaciones temporales para la conservación de los datos por parte del responsable o encargado del tratamiento, ya que la retención indefinida de los mismos no cumpliría con las premisas del presente proyecto de ley. Todas estas limitaciones son fundamentales y consolidan los principios relacionados con estas prácticas, al mismo tiempo que garantizan una protección adecuada de los datos personales.

La exactitud y actualización de los datos personales son aspectos de vital interés en el tratamiento de la información. Es fundamental que los datos reflejen de manera precisa la situación actual del titular, ya que la toma de decisiones y el logro de los fines del tratamiento dependen en gran medida de la veracidad de la información. La protección de los datos contra alteraciones no autorizadas, divulgaciones indebidas y accesos no autorizados es un aspecto clave en la preservación de la privacidad y la confidencialidad de los individuos. Para garantizar la seguridad de los datos, es necesario implementar medidas técnicas y organizativas adecuadas, adaptadas a los riesgos asociados con cada tipo de tratamiento. Ello se materializa en principios esenciales para establecer un marco sólido para el manejo responsable de los datos personales. El cumplimiento de estos principios promueve la confianza de los titulares de los datos, minimizan los riesgos de error y protege la privacidad frente a posibles incidentes de seguridad. Lo anterior, con fundamento en que el tratamiento de datos personales debe ser equilibrado y justificado, asegurando que las medidas adoptadas sean idóneas, necesarias y proporcionales a los objetivos perseguidos.

Todo lo aquí expuesto debe de ser tenido en cuenta atendiendo a la evolución tecnológica y a la inclusión cada vez más frecuente y necesaria de estas en los tratamientos de datos personales. La inclusión del principio de explicabilidad se justifica por el riesgo que representan los tratamientos automatizados y aquellos que generan efectos jurídicos o significativamente similares para los Titulares, especialmente ante el creciente uso de sistemas de inteligencia artificial. Este principio busca garantizar transparencia y comprensión sobre cómo se utilizan los datos personales y cómo se toman decisiones que pueden afectar derechos fundamentales.

Finalmente, se enfatiza en la responsabilidad del responsable del tratamiento en demostrar el cumplimiento de la normativa. En resumen, el artículo 4° amplía y detalla los principios para el tratamiento de datos personales, incorporando aspectos adicionales que buscan garantizar un tratamiento adecuado y responsable de la información personal, dado que, la evolución tecnológica y la globalización han aumentado la recopilación y el intercambio de datos personales, lo que plantea nuevos desafíos en su protección. Tanto empresas como autoridades utilizan un mayor volumen de datos, mientras que las personas comparten cada vez más información personal. Esto requiere encontrar un equilibrio entre la libre circulación de datos y una alta protección de la privacidad. Por lo tanto, todo lo dispuesto en el proyecto de ley materializa la necesidad de un marco jurídico más sólido y coherente para la protección de datos en Colombia en el que las personas naturales puedan tener el control de sus propios datos personales a la vez se refuerce la seguridad en el tratamiento de estos.

4.1.3. De las bases que legitiman el tratamiento de datos

En el presente proyecto de ley, el consentimiento sigue siendo una base legítima para el tratamiento de datos, pero se acompaña de otras bases que buscan abordar y evitar posibles conflictos en los casos en los que la autorización por sí sola no sea suficiente o apropiada para demostrar la legalidad del tratamiento. De esta manera, se busca establecer un marco normativo más completo que garantice la adecuada protección de los datos personales en diversas situaciones, en tal sentido, se incluyen al contrato, la ley o deber legal, el interés vital del titular, el interés público o el ejercicio de funciones públicas y la satisfacción de interés legítimos. Esto asegura la flexibilidad y protección de los derechos de los titulares de datos en diversas circunstancias.

Es crucial poder demostrar que el consentimiento para el tratamiento de datos personales fue otorgado de manera previa y de forma inequívoca. Esto garantiza la transparencia y la legitimidad del tratamiento de datos. Para validar el consentimiento, es necesario que la manifestación de voluntad sea libre, espontánea, específica, informada y clara. El consentimiento debe abarcar todas las actividades de tratamiento realizadas con los mismos fines y no se puede inferir a través del silencio, casillas marcadas por defecto o la inacción. En los casos en que el consentimiento forme parte de un contrato, pero no sea necesario para el mantenimiento, desarrollo o control de la relación contractual, se permite que la persona se niegue al tratamiento. Este puede ser revocado en cualquier momento, otorgando a los individuos un mayor control sobre sus datos personales.

El tratamiento de los datos de menores de edad ha sido objeto de consideración y ajuste en el presente proyecto de ley por diversas razones. En la Ley 1581 de 2012, la prohibición general del tratamiento de datos de menores limitaba su capacidad de participación en asuntos relacionados con sus propios datos personales, ya que se requería la intervención del representante legal. Esto no siempre reflejaba adecuadamente la madurez y autonomía de algunos menores, impidiendo que ejercitaran su derecho a ser escuchados en relación con el tratamiento de sus datos. La actualización de la ley reconoce la importancia de la participación activa y autónoma de los menores en la protección de sus datos personales. Los menores de catorce años aún requerirán la autorización de su representante legal para el tratamiento de sus datos. Sin embargo, aquellos que superen esa edad podrán otorgar su propio consentimiento.

Esta modificación refleja una mejor adaptación a la realidad tecnológica y a la creciente presencia de los jóvenes en entornos digitales. Es importante garantizar el interés superior del menor y el respeto a sus derechos fundamentales en todo momento, sin importar su edad. De esta manera, se busca equilibrar la protección de los datos personales de los menores con su derecho a participar activamente en decisiones relacionadas con su propia información.

4.1.3.1. Con base en la ejecución de un contrato

En el contexto de la ejecución del contrato, es necesario adaptar la normativa a las particularidades de esta situación mediante la inclusión de disposiciones específicas para el tratamiento de datos. Para garantizar la protección de los derechos de los titulares, solo se recopilarán los datos necesarios para cumplir con el contrato, y para aquellos que no estén directamente relacionados con su ejecución, se requiere de otras bases legitimadoras. Establecer un límite temporal para el tratamiento de los datos es primordial, ajustándose al convenido en el contrato, aunque el responsable podrá conservarlos durante un periodo adicional si existe la posibilidad de responsabilidades derivadas de la relación contractual. Una vez finalizada la relación contractual, los datos deberán ser devueltos al titular como consecuencia del cumplimiento de la finalidad establecida. Esta regulación busca equilibrar la protección de los derechos de los titulares de datos y la necesidad de llevar a cabo la ejecución del contrato de manera eficiente y segura.

4.1.3.2. Con base en un deber legal

El tratamiento de datos basado en el cumplimiento de un deber legal se fundamenta en la necesidad de cumplir con los requisitos y responsabilidades establecidos por la legislación vigente. Esta regulación tiene como objetivo principal salvaguardar los derechos de los titulares de datos, estableciendo limitaciones y requisitos que garanticen su privacidad y seguridad. Al limitar la recopilación de datos únicamente a aquellos que sean necesarios para cumplir con el deber legal, se evita un uso excesivo o innecesario de la información personal. Esto garantiza que los datos sean tratados de manera adecuada y que no se expongan a riesgos innecesarios.

4.1.3.3. Con base en salvaguarda de la vida o la salud

El tratamiento con base en la salvaguarda de la vida o la salud encuentra su fundamento en facilitar atención médica ante cualquier situación que conlleve riesgos para la vida del titular o en momentos en los que este no se encuentra con las facultades necesarias para otorgar el consentimiento. En la regulación actual es considerada como una excepción a la autorización, pero para justificar su aplicación ha sido necesario incorporar en el elenco de bases, legitimadoras pues, la presencia de esta como excepción y no como base legal pone de manifiesto el posible perjuicio al que el titular de datos puede exponerse con consecuencias mayores que el tratamiento de sus datos sin su consentimiento.

De similar forma se actúa en los supuestos en los que, en cumplimiento de una misión realizada en interés público conferida al responsable, se produce un tratamiento de datos personales. El tratamiento debe quedar supeditado a la protección del interés general y el respeto a los derechos fundamentales y, esencialmente al estricto cumplimiento de tales misiones. Todo ello resultará de aplicación con independencia de que el responsable sea un ente de derecho público o privado.

4.1.3.4. Con base en un interés legítimo

Cabe la posibilidad de que intervenga un interés legítimo que no verse sobre el titular o el bienestar colectivo, sino que responda a intereses perseguidos por el responsable o por un tercero. Este tratamiento solo será legítimo, si no prevalecen los intereses o derechos del interesado, teniendo en cuenta sus expectativas razonables basadas en su relación con el responsable. En particular, en ciertas circunstancias, los intereses y derechos fundamentales del interesado pueden prevalecer sobre los intereses del responsable, especialmente cuando el interesado no espera razonablemente un tratamiento ulterior.

En cualquier situación en la que se invoque un interés legítimo como base para el tratamiento de datos personales, es necesario realizar una cuidadosa evaluación. Incluso si un interesado puede razonablemente anticipar, en el momento y contexto de la recopilación de datos, que se realizará dicho tratamiento con ese propósito, se debe llevar a cabo un examen de ponderación para determinar si el tratamiento es lícito. Este examen consta de tres fases esenciales que analizan la finalidad del tratamiento, la necesidad del mismo y el equilibrio entre los intereses en juego. De esta manera, se busca garantizar que cualquier tratamiento basado en un interés legítimo cumpla con los principios de legalidad y proporcionalidad, salvaguardando los derechos y expectativas de privacidad de los interesados.

4.1.4. Otras categorías de manejo de datos

Existen otras categorías de datos a tener en cuenta, como, por ejemplo, los datos personales que poseen una naturaleza especialmente sensible requieren una protección especial debido a su potencial para afectar significativamente los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, datos relativos a la salud o datos relativos a la vida o la orientación sexuales de una persona natural. Es importante matizar que, aunque está prohibido con carácter general, pueden darse circunstancias en las que se exceptúa siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando el titular diese su consentimiento previo y expreso, cuando sea necesario para el cumplimiento de obligaciones y ejercicio de derechos del ámbito laboral, en orden a proteger intereses vitales, cuando el titular decida hacer pública la información, para fines de medicina preventiva o cuando sea necesario para la defensa de reclamaciones, defensa de intereses públicos o fines de archivo público.

Otros datos no presentan la necesidad de identificar al titular. Esto es una manifestación de la minimización de datos por la que se evita la recopilación y procesamiento de información adicional innecesaria para cumplir con los fines previstos. Cuando el responsable no pueda identificar al titular, se exime de ciertos requisitos de la normativa, a menos que el titular proporcione información adicional y desee ejercer sus derechos, momento en el cual se aplicarán los artículos correspondientes para equilibrar la protección de los derechos del titular con la viabilidad práctica de su ejercicio.

4.2. Transparencia e información al titular

De acuerdo con la normativa vigente en Colombia, el responsable del tratamiento de datos personales debe obtener la autorización del titular antes de procesar sus datos. Esta autorización debe ser previa, expresa e informada, y puede ser otorgada por escrito, de forma oral, escrita o a través de conductas inequívocas.

El responsable del tratamiento debe solicitar esta autorización al titular al momento de recolectar los datos, proporcionándole información clara sobre los datos a recolectar y las finalidades específicas del tratamiento.

Existen excepciones en las cuales la autorización del titular no es necesaria, como cuando se trata de información requerida por una entidad pública o administrativa, datos de naturaleza pública, casos de urgencia médica o sanitaria, tratamiento de información autorizado por ley para fines históricos, estadísticos o científicos, y datos relacionados con el Registro Civil de las personas.

El proyecto de ley busca mejorar la normativa actual estableciendo otras bases jurídicas, además del consentimiento, que legitimen el tratamiento de datos, como el contrato, precontrato, interés público, interés legítimo, entre otras. Además, se impone a los responsables del tratamiento la obligación de informar en todo momento a los titulares sobre el tratamiento de sus datos y se establecen mecanismos para facilitar el ejercicio de los derechos de los titulares.

Finalmente, se incluye la posibilidad de utilizar iconos normalizados en combinación con la información facilitada al titular para proporcionar una visión clara y legible del tratamiento de datos previsto, especialmente para alcanzar a los menores y personas con discapacidades. La Superintendencia de Industria y Comercio será responsable de establecer las reglas y pautas para cumplir con este deber de información.

El proyecto de ley tiene como objetivo en este título garantizar que los titulares estén debidamente informados sobre el tratamiento de sus datos personales y que los responsables del tratamiento cumplan con sus obligaciones sin imponer cargas desproporcionadas en la obtención del consentimiento cuando no sea necesario.

4.3. Del ejercicio de los derechos

Según la Superintendencia de Industria y Comercio, los ciudadanos están otorgando cada vez más importancia a su privacidad y a la protección de sus datos personales. En el año 2021, la Superintendencia de Industria y Comercio impuso multas por más de 32 mil millones de pesos debido a quejas por malos tratamientos de datos personales. Según INFOBAE (2022) estas quejas presentadas por los colombianos aumentaron un 74,49% en comparación con el año anterior, lo que sugiere que es probable que también hayan aumentado en el año 2022.

Para INFOBAE (2022) las empresas en Colombia recibieron un total de 28.619 quejas relacionadas con el mal manejo de los datos personales de sus usuarios, lo que equivale a un promedio de 2.384 querellas al mes. Los ciudadanos se quejaron principalmente porque la información almacenada en las bases de datos era falsa, errónea o estaba desactualizada, esto en relación a la Ley 1266 de 2008, conocida como *habeas data*. Además, muchos ciudadanos también se quejaron de violaciones a la Ley Estatutaria 1581 de 2012, la Ley General de Protección de Datos, ya que sus datos fueron recopilados o utilizados sin su permiso.

Es por eso que este Proyecto de Ley brinda los ejercicios de derecho necesarios para garantizar al titular la acción sobre sus datos personales. Comenzando por las disposiciones fundamentales para garantizar el ejercicio efectivo de los derechos de los titulares. Establece mecanismos de accesibilidad, transparencia y flexibilidad en el ejercicio de los derechos, reconociendo la diversidad de situaciones y necesidades de los titulares. Así mismo, asigna responsabilidades claras al responsable del tratamiento, protege los derechos de los menores y asegura la gratuidad de las actuaciones. En conjunto, estas disposiciones fortalecen la protección de datos personales y promueven la confianza en los procesos de tratamiento de información en Colombia.

4.3.1. ***Del derecho de acceso, rectificación y otros***

Las leyes de protección de datos establecen un marco legal claro que regula cómo se deben tratar los datos personales, evitando abusos y prácticas indebidas por parte de las organizaciones y gobiernos. Esto proporciona seguridad jurídica tanto para los individuos como para las entidades que manejan datos personales.

Uno de los derechos consagrados para evitar abusos en el manejo de datos personales es el derecho de acceso. En el proyecto de ley se establece que el titular tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen, así como a solicitar una copia de los datos personales objeto de tratamiento, . Además, se establece que, si el titular solicita la información por medios electrónicos, se facilitará en un formato electrónico de uso común.

El acceso a los datos personales es esencial para que los individuos puedan ejercer otros derechos, como el derecho a la rectificación, el derecho a la supresión y el derecho a la portabilidad de datos. Sin el acceso a sus propios datos, los individuos no podrían verificar su exactitud, corregir errores, eliminar información no deseada o transferir sus datos a otros servicios.

Pese a que la Ley 1581 del 2012 consagra el artículo 4° literal f) el "Principio de acceso y circulación restringida", no define adecuadamente el alcance y los métodos para ejercer el derecho de acceso que le corresponde al titular de los datos.

4.3.1.1. ***Derecho de rectificación***

El derecho de rectificación de datos personales es esencial por diversas razones. En primer lugar, garantiza la exactitud de la información al permitir a los individuos corregir cualquier dato personal inexacto o incompleto que esté siendo procesado. Esto es fundamental para evitar decisiones basadas en datos incorrectos y salvaguardar la precisión de la información. Además, otorga autonomía y control a los individuos sobre su propia información personal, permitiéndoles revisar, actualizar y corregir sus datos según sea necesario. Esto contribuye a su autonomía, les brinda la capacidad de proteger su reputación y privacidad, y asegura que los datos almacenados sean precisos y estén actualizados.

Así mismo, el derecho de rectificación facilita la toma de decisiones informadas al garantizar que los datos sean precisos y actualizados, lo que es especialmente relevante en situaciones como solicitudes de empleo, evaluaciones crediticias o trámites legales. Por último, el cumplimiento del derecho de rectificación cumple con las obligaciones legales y promueve la confianza de los individuos en las organizaciones, fortaleciendo así la protección de datos.

4.3.1.2. ***Derecho de supresión***

El derecho de supresión de datos personales es esencial por diversas razones. En primer lugar, garantiza la privacidad y el control sobre la información personal al permitir que los titulares soliciten la eliminación de sus datos cuando ya no sean necesarios o deseen revocar su consentimiento. Esto brinda a las personas un mayor control sobre su información y les permite decidir qué datos deben ser eliminados y cuándo. Además, el derecho de supresión protege contra el uso indebido de datos al permitir la eliminación de información obtenida ilegalmente o sin consentimiento. Esto asegura que los datos sean tratados de manera legal y ética, promoviendo la confianza en las prácticas de protección de la privacidad.

En segundo lugar, el derecho de supresión resguarda la reputación y la relevancia de la información personal. Permite solicitar la eliminación de datos desactualizados, inexactos o que ya no sean relevantes para el propósito original de su recopilación. Esto es especialmente importante en casos de información difamatoria o perjudicial que ya no tiene relevancia, protegiendo la reputación de las personas. Además, el derecho de supresión cumple con regulaciones normativas y promueve la transparencia, asegurando que las organizaciones cumplan con las leyes de protección de datos y permitiendo que los individuos conozcan y ejerzan su derecho a eliminar sus datos.

El Proyecto de ley busca establecer diversas circunstancias en las que el titular tiene derecho a solicitar la supresión de sus datos personales. Esto incluye situaciones en las que los datos ya no son necesarios para los fines para los que fueron recogidos, cuando el titular retira su consentimiento o se opone al tratamiento, cuando los datos han sido tratados de forma ilícita o cuando exista una obligación legal de supresión. Estas disposiciones brindan a los titulares un mayor control sobre sus datos y la capacidad de decidir sobre su uso y conservación.

La Ley 1581 del 2012 en Colombia reconoce el derecho de los individuos a solicitar la limitación del

tratamiento de sus datos personales como parte de sus derechos de protección de datos. Sin embargo, es cierto que la ley no proporciona una orientación clara y detallada sobre las circunstancias específicas en las que se puede ejercer este derecho, lo que puede generar incertidumbre tanto para los titulares de datos como para las entidades responsables del tratamiento.

Si hacemos un contraste con otras normativas que van a la vanguardia en privacidad y protección de datos como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, este establece disposiciones más precisas y detalladas sobre las condiciones en las que se puede solicitar la limitación del tratamiento de datos. El RGPD enumera claramente las circunstancias en las que los titulares pueden ejercer este derecho, como la impugnación de la exactitud de los datos, la existencia de una base legal para el tratamiento o el ejercicio de derechos legales en un contexto judicial. Además, el RGPD establece los procedimientos y requisitos específicos que deben seguirse para solicitar la limitación del tratamiento de datos.

La falta de una orientación clara en la Ley 1581 del 2012 puede generar incertidumbre y dificultades en la interpretación y aplicación de este derecho en Colombia. Esto puede afectar la capacidad de los titulares de datos para ejercer efectivamente su derecho a la limitación del tratamiento y puede generar desafíos para las entidades responsables del tratamiento al momento de gestionar las solicitudes de los titulares.

4.3.1.3. ***Derecho de limitación del tratamiento***

Esta disposición fortalecería los derechos de los titulares al establecer el derecho a la limitación del tratamiento de datos en diversas situaciones, garantizando un mayor control sobre el uso de su información personal, en aras de que dicha información solo sea utilizada de manera legítima y con su consentimiento. Además, se establecen salvaguardias para proteger los intereses de los titulares y se les brinda información oportuna sobre cualquier cambio en el tratamiento de sus datos. En conjunto, estas disposiciones promoverían la protección de la privacidad y los derechos de los titulares en todos los entornos.

En suma, para cerrar este conjunto de derechos derivados del derecho de acceso, en el artículo 31 de este Proyecto de ley se establece la obligación del responsable del tratamiento de notificar a los destinatarios pertinentes cualquier rectificación, supresión o limitación del tratamiento de datos personales. Esta disposición promovería la transparencia, la precisión y la actualización de los datos en manos de terceros. Además, garantizaría el derecho del titular a ser informado acerca de los destinatarios de sus datos personales. En conjunto, estas medidas fortalecerían la protección de los datos personales y empoderarían a los titulares en el manejo de su información.

4.3.2. ***Derecho a la portabilidad de datos***

La Ley 1581 del 2012 no incluye disposiciones específicas sobre el derecho a la portabilidad de datos, que permite a los individuos solicitar que sus datos personales sean transferidos de un responsable del tratamiento a otro.

El derecho a la portabilidad de datos es importante porque empodera a los individuos, facilita la movilidad del usuario, estimula la competencia y la innovación, protege la privacidad y contribuye al cumplimiento normativo. Este derecho promueve una mayor transparencia y control sobre los datos personales, beneficiando tanto a los individuos como a la sociedad en general.

Se debe garantizar el derecho a la portabilidad de los datos personales ya que esto permitiría a los titulares recibir sus datos en un formato compatible y transferirlos a otro responsable de tratamiento de manera eficiente. Además, se establecen salvaguardias para proteger los derechos de terceros y se limita el alcance de este derecho a las bases legales adecuadas. En conjunto, esta disposición fortalecería la autonomía y el control de los titulares sobre sus datos personales, fomentando la competencia y la protección de datos en el país.

4.3.3. ***Derecho de oposición***

En una actualización de la ley de protección de datos de Colombia, también es relevante y necesario incluir la regulación explícita del derecho de oposición. Aunque la Ley 1581 del 2012 no menciona este derecho específicamente, reconocer y regular el derecho de oposición en la nueva ley tendría varias ventajas y beneficios. Algunas razones por las cuales es importante incluir el derecho de oposición en la nueva ley son:

i) ***Fortalecimiento de los derechos de los individuos:*** El derecho de oposición es un derecho relevante en materia de protección de datos y permite a los individuos ejercer un mayor control sobre el tratamiento de sus datos personales. Al incluirlo en la nueva ley, se fortalecerían los derechos de los ciudadanos y se promovería una mayor autonomía y participación en el manejo de su información personal.

ii) ***Alineación con estándares internacionales***: El derecho de oposición está reconocido y regulado en marcos legales internacionales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Al incluir este derecho en la nueva ley de protección de datos de Colombia, se lograría una mayor alineación con estándares internacionales y se promovería la armonización normativa en materia de protección de datos.

iii) Claridad y transparencia: La inclusión del derecho de oposición en la ley brindaría claridad y transparencia tanto a los ciudadanos como a las organizaciones responsables del tratamiento de datos. Establecería las condiciones, procedimientos y requisitos para ejercer este derecho, lo cual evitaría confusiones y promovería una aplicación coherente y uniforme.

Contar con este derecho en este Proyecto de Ley de Protección de Datos de Colombia aseguraría el derecho de oposición de los titulares de datos personales. Esto les permitiría detener o limitar el tratamiento de sus datos en situaciones específicas, como el consentimiento y la publicidad directa. Al informar de manera explícita sobre este derecho, permitir su ejercicio a través de medios automatizados y tener en cuenta el contexto de investigación científica, histórica o estadística, se garantiza un equilibrio adecuado entre la protección de los derechos de los titulares y otros intereses legítimos.

Lamentablemente, la Ley 1581 del 2012 en Colombia no aborda específicamente el tema de las decisiones individuales automatizadas o la elaboración de perfiles en el contexto de la protección de datos personales.

Para darnos una idea de la importancia de estos derechos podemos ir hasta el Reglamento General de Protección de Datos (RGPD) de la Unión Europea que sí aborda detalladamente este tema y establece regulaciones específicas para las decisiones automatizadas y la elaboración de perfiles. Estas regulaciones incluyen el derecho de los interesados a no estar sujetos a decisiones basadas únicamente en el procesamiento automatizado, así como la obligación de proporcionar información clara y transparente sobre la lógica involucrada en el proceso de elaboración de perfiles.

EL GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, establece que:

"No obstante, la elaboración de perfiles y las decisiones automatizadas pueden plantear riesgos importantes para los derechos y libertades de las personas que requieren unas garantías adecuadas.

Estos procesos pueden ser opacos. Puede que las personas no sean conscientes de que se está creando un perfil sobre ellas o que no entiendan lo que implica.

La elaboración de perfiles puede perpetuar los estereotipos existentes y la segregación social. Asimismo, puede encasillar a una persona en una categoría específica y limitarla a las preferencias que se le sugieren. Esto puede socavar su libertad a la hora de elegir, por ejemplo, ciertos productos o servicios como libros, música o noticias. En algunos casos, la elaboración de perfiles puede llevar a predicciones inexactas. En otros, puede llevar a la denegación de servicios y bienes, y a una discriminación injustificada". (Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. (2017). Página 6).

Es por eso que la inclusión de este derecho Proyecto de Ley de Protección de Datos de Colombia garantizaría el derecho de los titulares a no ser sujetos de decisiones individuales automatizadas que les afecten significativamente sin intervención humana. Esta disposición establece excepciones claras, protege los derechos fundamentales de los individuos y prohíbe el uso de datos sensibles en las decisiones automatizadas. Al hacerlo, se promueve la transparencia, la equidad y la protección de los derechos de los titulares en el ámbito del tratamiento automatizado de datos personales.

Además, la inclusión de la elaboración de perfiles en este proyecto es esencial para proteger la privacidad de los individuos, prevenir discriminación y perjuicios, garantizar la transparencia, y fortalecer el control y la autonomía de los titulares sobre el uso de sus datos personales. Estas disposiciones contribuyen a establecer un marco legal sólido que equilibra la innovación tecnológica con la protección de los derechos fundamentales de las personas.

Es fundamental garantizar a los titulares el derecho a presentar una queja ante la Superintendencia de Industria y Comercio, en caso de vulneración de sus derechos de protección de datos.

4.3.4. *Derecho a la queja*

Esta disposición en el presente Proyecto de ley, promueve la protección de los titulares y establece un procedimiento formal para abordar las quejas, asegurando que se examinen de manera integral y se tomen las medidas adecuadas para hacer efectivo el derecho a la protección de los datos personales.

Por último, se incluye el derecho de cualquier persona a presentar una denuncia ante la Autoridad de Control en caso de posibles incumplimientos de la ley de protección de datos. Esta disposición promueve la participación activa de la sociedad en la protección de los datos personales y garantiza que las denuncias sean tratadas de manera integral, fomentando así un entorno de cumplimiento de la legislación de protección de datos.

4.4. Del responsable del tratamiento

4.4.1. *Obligaciones generales*

Con el objetivo de garantizar un nivel coherente de protección de los datos personales y facilitar la libre circulación de estos datos dentro del mercado interior, es necesario que la normativa establezca la seguridad jurídica y la transparencia para los operadores económicos. Para ello, se debe asegurar que los responsables y encargados del tratamiento de datos tengan el mismo nivel de obligaciones y responsabilidades, con el fin de garantizar una supervisión coherente en el tratamiento de datos personales.

En este sentido, el presente proyecto de ley aborda las obligaciones de las figuras del responsable y el encargado del tratamiento. Estas, ya se encuentran contempladas en la Ley 1581 de 2012, concretamente en su artículo 17 se enumeran los deberes relativos a los responsables del tratamiento y en el artículo 18 del mismo cuerpo legal se recogen las obligaciones del encargado del tratamiento. Sin embargo, es necesario reforzarlas y establecer un marco más preciso para proteger de manera rigurosa y efectiva los derechos fundamentales de los ciudadanos.

De este modo, se establecen obligaciones específicas tanto para los responsables del tratamiento como para los encargados, con criterios más precisos para regular la relación entre el responsable y el encargado del tratamiento. Además, se introduce la figura del corresponsable, que es opcional, pero resulta muy útil para lograr un equilibrio de funciones más efectivo. Para demostrar el cumplimiento de sus obligaciones como responsable, este puede optar por adherirse a códigos de conducta o mecanismos de certificación reconocidos. Asimismo, debe garantizar el pleno ejercicio de los derechos de los titulares de los datos que están siendo tratados.

Por ejemplo, se establece que es obligación del responsable del tratamiento suministrar la información pertinente sobre el tratamiento de datos y mantenerla actualizada. Además, debe reconocer y colaborar con la Superintendencia de Industria y Comercio como la autoridad nacional de protección de datos, acatando las instrucciones y requerimientos que esta emita en el ejercicio de sus funciones. Ante la situación de un incidente de seguridad, debe ser quien realice la notificación a la mencionada autoridad de control.

4.5. Seguridad de los datos

En el contexto actual, donde la información personal circula indiscriminadamente en sistemas informáticos interconectados cuya característica principal es su ubicuidad, la seguridad de los datos se convierte en una preocupación fundamental y una medida esencial. Como lo menciona la Guía Para la Gestión de Incidentes de Seguridad de la Superintendencia de Industria y Comercio, *"sin seguridad no hay debido Tratamiento de Datos Personales*".

Esto ya había sido previsto por el legislador de la Ley Estatutaria 1581 de 2012 que contempló la seguridad como un principio fundamental. Con el objetivo de fortalecer su aplicación, la Superintendencia de Industria y Comercio, en su rol de autoridad de control, estableció que la seguridad debe ser abordada como una medida preventiva. Esto implica que tanto los responsables como los encargados del tratamiento de datos están obligados a implementar las acciones necesarias para evitar posibles vulneraciones de la seguridad de la información, salvaguardando así el derecho fundamental a la protección de los datos personales.

4.5.1. *Los problemas de seguridad en el manejo de datos*

El Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales (2021), analizó las medidas de seguridad implantadas para tratar datos personales en 31.169 empresas (entre empresas y entidades públicas) del país. Este estudio refleja que tan solo el 50.7 % de las empresas que hacen parte del estudio, han implementado medidas apropiadas y efectivas para garantizar la seguridad de los datos personales, el 58 % de las organizaciones no han implementado medidas especiales para proteger datos sensibles, y en promedio el nivel de incumplimiento de los *ítems* evaluados por la Superintendencia de Industria y Comercio es de 59.41%. Esto muestra una falta de preparación por parte de los sujetos obligados para garantizar la seguridad de los datos personales, una debilidad de la actual Ley 1581 de 2012 y sus normas reglamentarias para garantizar el cumplimiento de esta obligación y, por ende, una ausencia de capacidades por parte de las organizaciones para la gestión del riesgo en materia de Seguridad.

Esto ha provocado que los ciberdelincuentes observen a Colombia como un país que muestra una menor preparación en ciberseguridad. Colombia recibió 20.000 millones de ciberataques en 2022, lo cual representa un crecimiento del 80 por ciento frente a 2021 tal y como lo reporta Lesmes Díaz, (2023). Este tipo de ataques impacta la reputación de las organizaciones y la de Colombia como un país con niveles de protección adecuados, produce perdidas monetarias y también merma la confianza de los ciudadanos frente a la circulación de sus datos personales.

De acuerdo con Pachón C (2022), Tan solo en el 2021, la Aeronáutica Civil y el DANE fueron protagonistas de ataques a sus sistemas informáticos (Pachón C, 2022). En agosto de 2021, la Aeronáutica Civil sufrió un ciberataque a la seguridad de la entidad con la finalidad de afectar servidores internos que tuvieron un impacto en: los servicios, correo electrónico y, en consecuencia, el sitio web oficial fue suspendido como medida de precaución. En ese mismo año, en el mes de noviembre, el Departamento Administrativo Nacional de Estadística fue víctima de un ataque informático. Los atacantes procedieron a eliminar sistemas de procesamiento estadístico y bases de datos con información de carácter reservado y con "*datos sensibles y confidenciales".*

En un entorno de crecientes amenazas cibernéticas y violaciones de datos personales, es crucial que los responsables y encargados del tratamiento de datos establezcan medidas sólidas de seguridad para proteger la privacidad y la confianza de las personas en el uso de sus datos personales. Según lo establecido por la Corte Constitucional en la Sentencia C-748 de 2011, los *responsables del tratamiento tienen mayores compromisos y obligaciones hacia los titulares de la información*, pues tienen la obligación de garantizar en primer lugar el derecho fundamental a la protección de datos, así como las condiciones de seguridad para evitar cualquier tratamiento ilícito de los datos.

En este sentido, la Seguridad se convierte en una condición *sine qua no* para garantizar la materialización de la protección de los datos personales en diferentes operaciones de tratamiento. Por lo que, no se puede prescindir de la aplicación de este principio al momento de tratar datos personales, sino que debe estar incorporado de manera preventiva.

El presente proyecto de ley busca fortalecer y ampliar el enfoque que trae la normativa vigente en cuanto a seguridad, siendo la Ley 1581 de 2012 una propuesta que no se encuentra al nivel del avance de la tecnología y su potencial para afectar el derecho a la intimidad de los ciudadanos.

En el nuevo cuerpo normativo, los responsables y encargados del tratamiento deben tener en cuenta diferentes factores que están estrechamente relacionados con su tamaño, estructura organizacional, volumen de datos, herramientas y tecnologías implicadas en el tratamiento, tipo de datos y costos aplicados a la operatividad para implementar medidas de seguridad que se ajusten a su realidad y sean el resultado de una evaluación exhaustiva de los riesgos que afronta la organización en el tratamiento de datos personales.

Se propone entonces, unas medidas mínimas de seguridad que ayudan a garantizar de forma efectiva el derecho a la protección de los datos personales de los titulares y el resguardo de su información de accesos y explotación no autorizada por parte de terceros. No pretende esta nueva propuesta legislativa ser una serie de medidas restrictivas que puedan provocar su inaplicación por falta de flexibilidad, sino por el contrario, con los criterios establecidos, busca que sean los responsable y encargados del tratamiento quienes realicen una evaluación de sus operaciones de tratamiento y que esta le permita adecuar al nivel de seguridad que funciona para su organización en particular.

4.5.2. ***Adaptaciones requeridas***

De acuerdo con los establecido en la Guía para la Implementación del Principio de Responsabilidad Demostrada (accountability), las violaciones a los códigos de seguridad de las organizaciones generan un alto riesgo a los titulares de los datos personales y a su vez, causan impactos significativos en la reputación corporativa. No obstante, la Ley 1581 de 2012 y su norma reglamentaria, desarrollan la seguridad como un concepto genérico, que establece lo que se esperaría de cualquier sistema de información, pero no trae consigo estándares mínimos de seguridad que obliguen al responsable y encargado a implantar medidas con un enfoque preventivo.

Por ende, el fortalecimiento de la Seguridad como principio y como deber, implica la adopción de medidas técnicas y organizativas que conjugan la aplicación de la tecnología y buenas prácticas como elementos constitutivos de un sistema de seguridad que garantice la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

Se observa así que, el proyecto de ley introduce el concepto de Resiliencia como característica del desempeño de los servicios de tratamiento de información que puede ayudar a mejorar la seguridad (INSST, 2018). La resiliencia se manifiesta en la capacidad de anticiparse, responder y recuperarse de manera efectiva ante los desafíos y adversidades, permitiendo que el sistema de información se mantenga robusto y operativo en todo momento, sin importar las circunstancias, característica necesaria en tiempos donde los ataques cibernéticos hacen parte del paisaje cotidiano.

En cuanto al sector público, se reconoce la necesidad de integrar la gobernabilidad y la tecnología para mejorar la función pública como soporte del desarrollo social, económico y político de la Nación. El Ministerio de Tecnologías de la Información y otros organismos gubernamentales están trabajando en la materialización de la masificación del Gobierno en línea, a través de la Política de Gobierno Digital, que propende por la transformación digital pública y el fortalecimiento de las relaciones con el ciudadano. La política define cuales deben ser las capacidades que deben desarrollar los sujetos obligados para ejecutar las líneas de acción de dicha Política, siendo uno de los habilitadores la Seguridad y la privacidad de la información.

La Seguridad y Privacidad de la información busca que los sujetos obligados implementen *lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos* (Decreto número 767 de 2022, Artículo 2.2.9.1.2.1. numeral 3.2.). Esto, en reconocimiento de que la ejecución de la Política involucra el tratamiento de los datos de los ciudadanos para hacer posibles la prestación de los servicios ciudadanos digitales y que la arquitectura donde está siendo desarrollada trae consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, esto sin excluir el tratamiento manual o híbrido de datos personales.

Como corolario de lo anterior, el presente proyecto de ley busca que en el continúo desarrollo del modelo de Gobernanza de la Seguridad Digital, los sujetos obligados garanticen la seguridad de los datos personales de los ciudadanos y realicen una adecuada gestión de los riesgos, puesto que la perdida de la confidencialidad, disponibilidad e integridad de la información relacionada con el perfil del ciudadano puede provocar situaciones de discriminación y vulneración de sus derechos y libertades fundamentales.

4.6. Transferencias de datos internacionales

Los flujos transfronterizos de datos personales entre diferentes países desempeñan un papel fundamental en la expansión del comercio y la cooperación internacional. En este sentido, las transferencias internacionales de datos personales son una consecuencia directa de la globalización y los fenómenos de integración económica y social, y el internet, en los que tanto las empresas como las entidades gubernamentales requieren transferir datos personales destinados a diferentes propósitos para el cumplimiento de sus finalidades.

La regulación de las transferencias internacionales de datos personales sufre su más notable modificación en el sentido en el que se enuncian en las respectivas disposiciones normativas. Mientras que en la Ley 1581 de 2012 y el Decreto número 1377 de 2013, se proyectan en una vertiente negativa, mostrándolas como una prohibición sobre la que se aplican excepciones, en este proyecto de ley se ilustran como un principio general en el que, para que concurran, es necesaria que se den ciertas condiciones. La nueva propuesta legislativa, busca procurar los niveles de protección adecuados a través de una serie de obligaciones, medidas y criterios que deben ser acatados por responsables y encargados del tratamiento para no comprometer el nivel de protección garantizado en Colombia, incluso en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional.

Se tiene, entonces como escenario ideal, la transferencia internacional mediante decisión de adecuación, valoración que continúa en cabeza de la Superintendencia de Industria y Comercio y que evalúa aspectos relevantes sobre el tercer país, territorio u organización internacional a la que se le otorga la denominación de "Adecuado". En ausencia de dicha decisión, con el objetivo de impedir que la transferencia internacional de los datos pueda lesionar derechos constitucionales como el derecho a la intimidad, se establece que los responsables y encargados ofrezcan garantías adecuadas, que funcionan tanto para el sector público, en el caso de instrumentos de cooperación jurídicamente vinculantes y exigibles entre autoridades y organismos públicos, como en el sector privado, en cuanto a normas corporativas vinculantes, cláusulas tipo de protección de datos, códigos de conducta y mecanismos de certificación.

Si bien, algunas de las garantías que deben ofrecer los sujetos obligados en el marco de este proyecto de ley, son instrumentos comunes en la práctica empresarial que procura incorporar la protección de los datos en sus operaciones de tratamiento, estos no se encontraban plenamente reconocidos en la legislación vigente, excepto por las normas corporativas vinculantes.

Así mismo, esta nueva propuesta legislativa pretende dilucidar los conceptos de transferencia y transmisión establecidos en los artículos 24 y 25 del Decreto Reglamentario 1377 de 2013. Siendo la transferencia entendida como una "Cesión[1]" en *stricto sensu*, como se conoce a nivel internacional, y la transmisión[2] como el acceso a los datos que tiene el encargado del tratamiento, independientemente de si este se encuentra ubicado o no en territorio nacional.

Esta distinción entre transferencia y transmisión dejaba por fuera todas las operaciones de tratamiento que implicaban la exportación de datos fuera del territorio nacional, siendo la única medida de protección en las transferencias internacionales realizadas por encargos el contrato de transmisión de datos personales. No obstante, este acercamiento contemplado en la legislación vigente, se aparta de lo ya teorizado en la comunidad internacional en cuanto a transferencias internacionales de datos, puesto que, no se puede considerar que el acceso a datos de titulares residentes en Colombia por encargados que no se encuentren establecidos en territorio nacional un flujo transfronterizo de datos. Una vez aclarado que pueden coexistir los encargos de tratamiento y las transferencias internacionales, este proyecto de ley, además de garantizar que las remisiones entre responsables y encargados se hagan en virtud de un contrato o instrumento jurídicamente vinculante, también busca blindar el derecho a la protección de los datos de los titulares, si dicho encargo constituye una transferencia internacional.

Las excepciones establecidas por el artículo 26 de la Ley 1581 de 2012 se mantienen, pero siendo estas la última alternativa de los sujetos obligados frente a la ausencia de una declaración de conformidad o garantías adecuadas. Se entiende, entonces que los sujetos obligados asumen el riesgo de realizar las transferencias bajo estas excepciones y que deberán documentar que han realizado las evaluaciones tendientes a demostrar que no se compromete el nivel adecuado de protección durante la transferencia. Cuando estas excepciones tampoco concurran, se permite la transferencia internacional en cumplimiento de los siguientes requisitos: no es repetitiva, afecta a un número limitado de titulares, es necesaria para intereses legítimos imperiosos del responsable del tratamiento, se han evaluado todas las circunstancias y se ofrecen garantías apropiadas para proteger los derechos de los titulares.

En un mundo cada vez más interconectado, donde los datos personales pueden ser transferidos y compartidos a nivel global, resulta fundamental contar con mecanismos que faciliten la aplicación efectiva de la legislación de protección de datos entre países y organizaciones internacionales. Por ello, es esencial que la Superintendencia de Industria y Comercio cooperar internacionalmente para promover y asegurar la protección adecuada de los datos personales, garantizando la seguridad y los derechos fundamentales de los titulares en un entorno globalizado.

---

[1] Superintendencia de Industria y Comercio. guía para la implementación del principio de responsabilidad DEMOSTRADA en las transferencias internacionales de datos personales. (2019). SIC. P. 8. https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales.pdf

[2] Superintendencia de Industria y Comercio. guía para la implementación del principio de responsabilidad DEMOSTRADA en las transferencias internacionales de datos personales. (2019). SIC. P. 8. https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales.pdf

4.7. Indemnización y régimen sancionatorio

Es una deuda del legislador de la Ley 1581 de 2012 con los titulares de los datos personales el ofrecer el derecho a ser indemnizados en caso de que el incumplimiento de las obligaciones en materia de protección de datos y posterior violación a su derecho fundamental por parte de los sujetos obligados hubiere ocasionado daños y perjuicios. Esto se encuentra establecido en el considerando 25 de los Estándares de Protección de Datos Personales elaborado por la Red Iberoamericana de protección de datos, de la que Colombia es Estado miembro.

Asimismo, refleja el Reglamento General de Protección de Datos, referente normativo a nivel internacional en materia de protección de datos, que tanto responsable como encargados del tratamiento deben indemnizar cualquier daño y perjuicio que pueda sufrir una persona natural como consecuencia de un tratamiento en infracción del Reglamento. (Reglamento General de Protección de Datos, 2016, Considerando 146).

En esta nueva propuesta legislativa se introduce la indemnización por daños y perjuicios materiales e inmateriales causados por el incumplimiento de las obligaciones por parte de los sujetos obligados. Esto en respuesta a las consecuencias negativas que el incumplimiento de las obligaciones de los responsable y encargados pueda tener sobre los titulares de los datos personales. En la mayoría de los casos, la denuncia ante la Superintendencia de Industria y Comercio no compensa los perjuicios que pueden llegar a sufrir los ciudadanos por indebido tratamiento de sus datos personales.

De acuerdo con la información de la Dijin, la suplantación de identidad creció 409% en el 2020, debido a la pandemia del Covid-19 (Certicamara/ Dijin, 2020)[3]. Muchas de las víctimas de suplantación manifiestan no haber compartido sus datos personales con extraños, y en muchas ocasiones, solo fue suficiente una copia de su Cédula de Ciudadanía para adquirir un bien o servicio a su nombre. Situaciones que pueden prevenirse si los responsables y encargados del tratamiento implementan medidas técnicas y organizativas de seguridad que permitan incorporar filtros conducentes a establecer la identidad de quien solicita un bien o servicio. Como consecuencia de estas falencias al momento de comprobar la veracidad de los datos, muchos titulares terminan asumiendo obligaciones que no adquirieron, ocasionando perjuicios económicos y daños a su reputación crediticia.

Debe aclararse que con esto no se busca que la Superintendencia de Industria y Comercio analice si se cometió el delito de falsedad personal, puesto que no está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito. Pero sí establecer si existió un tratamiento en incumplimiento de las obligaciones de los sujetos obligados, y decidir sobre el derecho de los titulares a obtener una indemnización si dicho tratamiento provocó daños y perjuicios materiales o inmateriales. No obstante, la mera alegación de que existió un daño y perjuicio no será suficiente para determinar que así haya sido, y en respeto de la garantía constitucional del debido proceso, los sujetos obligados tendrán la oportunidad de demostrar que no fueron responsables en modo alguno del hecho que causó dichos daños y perjuicios.

El legislador de la Ley 1581 de 2012 tenía claro que la protección de los datos personales requería de un régimen sancionatorio expresó, como de una institucionalidad que permita un control y ámbito de garantía efectivo del derecho a la protección de datos personales. Como resultado, en el artículo 22 de la precitada norma quedó establecida la potestad sancionatoria de la Autoridad de Protección de Datos Personales, estableciendo que aquello no reglado, seguiría lo pertinente al procedimiento sancionatorio establecido en el Código Contencioso Administrativo.

En la Sentencia C-748 de 2011 se estableció que:

"*el poder sancionador estatal ha sido definido como un instrumento de autoprotección, en cuanto contribuye a preservar el orden jurídico institucional mediante la asignación de competencias a la administración que la habilitan para imponer a sus propios funcionarios y a los particulares el acatamiento, inclusive por medios punitivos, de una disciplina cuya observancia contribuye a la realización de sus cometidos".*

Esto no es más que la materialización del *ius puniendi*, que debe regirse por los principios de legalidad, tipicidad, debido proceso, proporcionalidad e independencia de la sanción penal. En esta nueva propuesta legislativa no solo es menester incorporar nuevas infracciones con ocasión de las diferentes figuras jurídicas introducidas, sino que también, se establece un Régimen Sancionatorio más claro que permite tipificar mejor las infracciones que puedan llegar a ser cometidas por los actores involucrados en el tratamiento de datos personales.

Con respecto al principio de legalidad, corresponderá al legislador definir la licitud del Régimen una vez se discuta el contenido definitivo del proyecto de ley que debe ser sometido a trámite legislativo; con respecto a la tipicidad, presenta este proyecto de ley una descripción específica, precisa y exhaustiva de las acciones y omisiones que se consideran infracciones en materia de protección de datos, incluso modulando las mismas por nivel de gravedad; en cuanto al debido proceso, si bien, este proyecto de ley continúa con que la actuación administrativa que inicie la investigación se circunscriba a lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, establece sujetos responsables, condiciones generales para la imposición de sanciones, distinción entre los tipos de sanciones

[3] Referenciado en: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651

e incluso un régimen de prescripción y caducidad para las mismas, dando garantías suficientes y la oportunidad a los actores que se encuentren involucrados en un investigación de ejercitar su derecho de defensa; en relación con la aplicación del principio de proporcionalidad, este proyecto de ley propone una modulación de las infracciones, donde la gravedad de las mismas se gradúa en función de su propensión a violar los derechos y garantías fundamentales de los titulares. Como resultado, la sanción impuesta será determinada en consonancia con la magnitud de la infracción cometida.; y, por último, en cuanto a la independencia de la sanción penal, las sanciones descritas en el proyecto de ley pueden ser impuestas sin importar que el hecho que la motiva también pueda constituir una infracción en el régimen penal.

Con la presentación de este nuevo Régimen Sancionatorio, se pretende hacer un esfuerzo por regular de forma sistemática y clara los procedimientos sancionatorios en materia de protección de datos.

4.8. Régimen de transición

El régimen de transición proporcionará certeza y estabilidad a los titulares y responsables del tratamiento en los derechos y deberes que tiene frente a los datos de carácter personal. Permite que los Responsables y Encargados del tratamiento se adapten a las nuevas disposiciones de manera gradual y planificada, evitando confusiones y conflictos legales.

Asimismo, asegura que los derechos y obligaciones adquiridos bajo la legislación anterior no sean afectados de manera injusta por la entrada en vigencia de la nueva ley. Esto evita situaciones en las que los titulares se vean perjudicados debido a cambios repentinos en el marco legal, en particular lo referente al ejercicio de derechos que estén en trámite.

Al incluir un régimen de transición, se brinda a los Responsables y Encargados del Tratamiento un tiempo razonable para cumplir con las nuevas disposiciones. Esto es especialmente relevante en casos en los que se requieren cambios significativos en las prácticas, estructuras organizativas o tecnologías utilizadas.

El régimen de transición en las leyes es fundamental para garantizar la seguridad jurídica, proteger los derechos adquiridos, permitir una adaptación progresiva y considerar situaciones particulares.

4.9. Otras disposiciones.

4.9.1. Autoridades de control

En el proyecto de ley se amplía las funciones de la Autoridad de Protección de Datos Personales fortaleciendo sus poderes. Por último, como órgano correctivo y sancionatorio, debe poder advertir y recomendar a los sujetos obligados cuando sus prácticas operativas en el tratamiento de datos personales no se ajusten a lo establecido en el presente proyecto de ley, así como, recurrir a la imposición de multas y sanciones cuando encuentre que los responsables y/o encargados del tratamiento han incumplido con las obligaciones contenidas en el presente proyecto de ley.

5. MARCO JURÍDICO

5.1. Marco jurídico internacional

a) Derecho a vida privada como base para el derecho a la protección de datos personales

• El artículo 12 de la Declaración Universal de los Derechos Humanos establece que toda persona debe ser protegida ante injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación.

• El artículo 17 el Pacto Internacional de Derechos Civiles y Políticos puntualiza que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

Respecto a este artículo es importante puntualizar que la Observación General 16 del Comité de Derechos Humanos estableció:

"[...] Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y porque nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación [...]".

• El artículo 11 de la Convención Americana de Derechos Humanos dispone que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

b) Declaración de Santa Cruz de la Sierra como fundamento para la reglamentación del derecho a la protección de datos personales en Latinoamérica

En virtud de la cual, veintiún países que se encontraban en la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, entre estos Colombia, manifestaron su preocupación en torno a la protección de derechos personales entendido como un derecho fundamental.

c) Recomendación del Consejo de la OCDE relativo a los lineamientos para la protección al consumidor en el contexto del comercio electrónico

Esta Recomendación aborda tanto la protección al consumidor como el derecho a la protección de datos personales en el ámbito del comercio electrónico. De esta forma establece una serie de lineamientos y principios que los países miembros de la OCDE y otras economías pueden seguir para promover la confianza del consumidor en el comercio electrónico y garantizar la protección de sus datos personales. Algunos de los puntos clave de la Recomendación incluyen:

- Transparencia: Los proveedores de servicios en línea deben proporcionar información clara y comprensible sobre sus prácticas de protección de datos personales, así como sobre los términos y condiciones de las transacciones en línea.

- Consentimiento informado: Los consumidores deben ser informados de manera clara sobre la recopilación, uso y divulgación de sus datos personales, y deben tener la capacidad de dar su consentimiento o rechazarlo de manera libre y voluntaria.

- Seguridad: Los proveedores de servicios en línea deben implementar medidas de seguridad adecuadas para proteger los datos personales de los consumidores contra el acceso no autorizado, la divulgación o el uso indebido.

- Acceso y corrección: Los consumidores deben tener la posibilidad de acceder a sus datos personales y corregir cualquier inexactitud o incompletitud que exista en ellos.

- Cooperación internacional: Se promueve la cooperación y el intercambio de información entre los países para abordar los problemas transfronterizos relacionados con la protección al consumidor y la protección de datos personales en el comercio electrónico.

d) Organización de Estados Americanos: Principios sobre la Privacidad y la Protección de Datos Personales

Fueron adoptados por el Comité Jurídico Interamericano en 2015 para contribuir en la construcción de un marco vigente para la protección del derecho a los datos personales y la autodeterminación en los países de las Américas (OEA,2021). Los principios son los siguientes:

- *"Finalidades Legítimas y Lealtad: Los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios leales y legítimos.*

- *Transparencia y Consentimiento: Antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para las cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el tratamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, inequívoco, libre e informado de la persona a que se refieran.*

- *Pertinencia y Necesidad: Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes, y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior.*

- *Pertinencia y Necesidad: Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes, y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior.*

- *Confidencialidad: Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley.*

- *Seguridad de los Datos: La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aun cuando estos ocurran de manera accidental. Dichas salvaguardias deberían ser objeto de auditoría y actualización permanente.*

- *Exactitud de los Datos: Los datos personales deberían mantenerse exactos, completos y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad.*

- *Acceso, Rectificación, Cancelación, Oposición y Portabilidad: Se debería disponer de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y cancelación de sus datos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a la portabilidad de esos datos personales. Como regla general, el ejercicio de esos derechos debería ser gratuito. En caso de que fuera necesario restringir los alcances de estos derechos, las bases específicas de cualquier restricción deberían especificarse en la legislación nacional y estar en conformidad con los estándares internacionales aplicables.*

- *Datos Personales Sensibles: Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos.*

- *Responsabilidad: Los responsables y encargados del tratamiento de datos deberían adoptar e implementar medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con estos Principios. Dichas medidas deberían ser auditadas y actualizadas periódicamente. El responsable o encargado del tratamiento y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas.*

- *Flujo Transfronterizo de Datos y Responsabilidad: Reconociendo su valor para el desarrollo económico y social, los Estados Miembros deberían cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando estos confieran un nivel adecuado de protección de los datos de conformidad con estos Principios. Asimismo, los Estados Miembros deberían cooperar en la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y ser efectivamente hechos responsables por el cumplimiento de estos Principios.*

- *Excepciones: Cualquier excepción a alguno de estos Principios debería estar prevista de manera expresa y específica en la legislación nacional, ser puesta en conocimiento del público y limitarse únicamente a motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, o el interés público.*

- *Autoridades de Protección de Datos: Los Estados Miembros deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos Principios. Los Estados Miembros deberían promover la cooperación entre tales órganos."*

e) Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos

Como miembro de la Red Iberoamericana de Protección de Datos, Colombia adhiere a los Estándares de Protección de Datos Personales. Para efectos del presente proyecto de ley resulta clave tener en cuenta que el considerando 24 establece que cada Estado Iberoamericano debe contar con una autoridad de control independiente e imparcial en sus potestades que sea ajena a toda influencia externa, con facultades de supervisión e investigación en materia de protección de datos personales.

A su vez, el considerando 25 puntualiza que:

"*Reconociendo que los Estados Iberoamericanos están obligados a adoptar un régimen que garantice a los titulares una serie de mecanismos y procedimientos, para presentar sus reclamaciones ante la autoridad de control cuando consideren vulnerado su derecho a la protección de datos personales, así como para ser indemnizados cuando hubieren sufrido daños y perjuicios como consecuencia de una violación de su derecho…"*

5.2. Marco jurídico nacional

5.2.1. Fundamento Constitucional

El derecho fundamental a la protección de datos se encuentra cimentado en los artículos 15 y 20 de la Constitución Política, en virtud de los cuales se establecen los derechos a la Intimidad Personal y Familiar, y Buen Nombre, además de la Libertad de Expresión e Información.

En particular es importante tener en cuenta que el artículo 15 establece que la recolección, tratamiento y circulación de datos deben respetar la libertad y demás garantías inscritas en la Constitución.

6. FUNDAMENTO NORMATIVO

a) Ley 1581 de 2012:

Como se reiterará a lo largo del presente documento, la Ley 1581 de 2012 constituye el pilar central del régimen de protección de datos personales en Colombia, estableciendo los elementos esenciales para su tratamiento, conforme al estado tecnológico y los estándares internacionales vigentes en el momento de su expedición.

Entre sus disposiciones más relevantes se encuentra la prohibición del tratamiento de datos personales de menores de edad sin la intervención de su representante legal. La ley exige que el responsable del tratamiento obtenga autorización previa, expresa e informada del titular, la cual puede manifestarse por escrito, verbalmente o mediante conductas inequívocas, e impone la obligación de informar claramente sobre los datos recolectados y las finalidades específicas del tratamiento.

Asimismo, prevé excepciones a la exigencia de autorización en casos como solicitudes de entidades públicas, tratamiento de datos de naturaleza pública, situaciones de urgencia médica o sanitaria, finalidades históricas, estadísticas o científicas, y datos relativos al Registro Civil. La norma incorpora el principio de acceso y circulación restringida, limitando el tratamiento únicamente a personas autorizadas por el titular o por la ley.

De igual manera, reconoce el derecho de supresión de los datos, así como la posibilidad de solicitar la limitación del tratamiento. También establece los deberes de los responsables y encargados del tratamiento, consagra la seguridad como principio rector y prohíbe la transferencia internacional de datos hacia países que no cuenten con niveles adecuados de protección, salvo en los casos expresamente permitidos, como el consentimiento expreso del titular, el tratamiento de datos médicos,

transferencias bancarias o bursátiles, cumplimiento de tratados internacionales, ejecución de contratos, o la defensa de derechos en sede judicial.

La ley confiere la función de autoridad de control a la Superintendencia de Industria y Comercio, a través de su Delegatura para la Protección de Datos Personales, y prohíbe el tratamiento de datos sensibles, salvo con fines históricos, estadísticos o científicos, previa disociación de la identidad del titular.

Finalmente, precisa que se entiende por dato personal toda información vinculada o que pueda asociarse a una persona natural determinada o determinable, excluyendo del ámbito de aplicación los datos de contacto de personas jurídicas, y otorga a la autoridad de protección facultades sancionatorias frente al incumplimiento del régimen.

b) Decreto número 1377 de 2013:

El Decreto número 1377 de 2013 reglamenta la Ley 1581 de 2012 y establece disposiciones específicas para su implementación, desarrollando aspectos clave del régimen de protección de datos personales en Colombia. En su artículo 2°, el Decreto señala un tipo de tratamiento excluido del ámbito de aplicación del régimen general: los datos mantenidos en contextos meramente personales o domésticos. Se entiende por estos aquellos vinculados a actividades propias de la vida privada o familiar de las personas naturales.

El artículo 3° del Decreto define conceptos fundamentales como la transferencia y la transmisión de datos. La **transferencia** se configura cuando el responsable y/o encargado del tratamiento ubicado en Colombia remite los datos personales a otro responsable, dentro o fuera del país. Por su parte, la transmisión corresponde al tratamiento que implica la comunicación de datos, también dentro o fuera del territorio nacional, para ser procesados por un encargado por cuenta del responsable.

El Capítulo 2 se concentra en el elemento de la autorización, abordando las condiciones y formas en que debe otorgarse en consonancia con los principios rectores del tratamiento de datos personales. En este sentido, el artículo 4° establece cómo debe llevarse a cabo la recolección de los datos, y el artículo 7° regula la obtención de la autorización, admitiendo su automatización siempre que se exprese por escrito, de forma verbal o mediante conductas inequívocas del titular, excluyendo expresamente que esta pueda inferirse por silencio. A su vez, el artículo 9° reconoce el derecho del titular a revocar la autorización y a solicitar la supresión de sus datos, imponiendo al responsable o encargado la obligación de disponer mecanismos gratuitos y accesibles para ello. Una vez presentada la reclamación, la supresión debe efectuarse en un plazo de 15 días hábiles, *so pena* de sanción.

El Capítulo 3 desarrolla las **políticas de tratamiento de la información** como instrumentos rectores para la gestión de datos en las organizaciones. El artículo 16 impone la obligación de conservar el modelo de aviso de privacidad, herramienta clave para informar a los titulares sobre el tratamiento de sus datos. Por su parte, el artículo 19 faculta a la Superintendencia de Industria y Comercio para emitir instrucciones en materia de seguridad de la información, a través de circulares y resoluciones. Adicionalmente, el artículo 23 establece la obligación de designar un responsable de los datos personales al interior de cada organización.

En cuanto a la **transmisión y transferencia internacional de datos**, el Capítulo 4 contempla que, conforme al artículo 24, no será necesario informar al titular ni contar con su autorización cuando exista un contrato entre el responsable y el encargado que sustente la transmisión internacional. El artículo 25 detalla que dicho contrato debe incluir las condiciones particulares y las características esenciales de la relación entre quien es titular de la base de datos y quien la administra.

Finalmente, el Decreto cierra con un capítulo dedicado al principio de **responsabilidad demostrad**a, entendido como el deber empresarial de evidenciar el cumplimiento del régimen de protección de datos. El artículo 26 faculta a la Superintendencia de Industria y Comercio para solicitar a las empresas la descripción de sus procedimientos y las pruebas de las medidas adoptadas para garantizar la seguridad de la información. Por su parte, el artículo 27 establece que la Superintendencia impartirá directrices tomando en cuenta tres parámetros: la existencia de una estructura administrativa proporcional al tamaño de la organización, la adopción de mecanismos internos para implementar las políticas de tratamiento, y la existencia de procesos eficaces para la atención de consultas, peticiones y reclamos de los titulares.

c) Decreto número 767 de 2022:

Para efectos del presente proyecto de ley resulta importante destacar este Decreto en virtud del cual se establecen lineamientos generales de la Política de Gobierno Digital, en particular el numeral 3.2. del artículo 2.2.9.1.2.1. prescribe como elementos de la Política de Gobierno Digital:

"[...] 3.2. Seguridad y Privacidad de la Información: Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos [...]".

6.1. Fundamento jurisprudencial:

A partir de la sentencia de la Corte Constitucional T-414 de 1992 se comenzó a desarrollar el derecho de *habeas data*, definido como una garantía del derecho a la intimidad. De esta forma la protección de los datos se asume desde la esfera de la vida privada y familiar, luego, ni el Estado ni otros particulares pueden intervenir en su órbita (Rojas, 2014).

Por su parte, la sentencia **SU-082 de 1995** puntualizó los elementos que componen el *habeas data*, en los siguientes términos:

"[…] El contenido del habeas data se manifiesta por tres facultades concretas que el citado artículo 15 reconoce a la persona a la cual se refieren los datos recogidos o almacenados:

a*) El derecho a conocer las informaciones que a ella se refieren;*

b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos;

c) El derecho a rectificar las informaciones que no correspondan a la verdad […]".

Posteriormente, a través de la sentencia T-729 de 2002 se precisaron diferencias entre el derecho al *habeas data* y otras garantías como el buen nombre y la intimidad (Rojas, 2014), siendo estas:

"[…] la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; (ii) por la delimitación de los contextos materiales que comprenden sus ámbitos jurídicos de protección; y (iii) por las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información [...]".

A su vez, esta sentencia reconoció en el *habeas data* una acción ciudadana que permite salvaguardar el derecho a la intimidad como garantía de la vida privada y familiar, pasando de ser una garantía de alcance limitado a un derecho más amplio.

Teniendo en cuenta el crecimiento de las amenazas cibernéticas y violaciones de datos personales la Corte Constitucional a través de la sentencia C-748 de 2011 puntualizó que:

"[…] los responsables del tratamiento tienen mayores compromisos y deberes frente al titular del dato, pues son los llamados a garantizar en primer lugar el derecho fundamental al habeas data, así como las condiciones de seguridad para impedir cualquier tratamiento ilícito del dato. La calidad de responsable igualmente impone un haz de responsabilidades, específicamente en lo que se refiere a la seguridad y a la confidencialidad de los datos sujetos a tratamiento […]".

Adicionalmente, en dicha sentencia precisó que las autoridades de control en materia de protección de datos constituyen un mecanismo esencial que asegura la observancia efectiva del derecho fundamental de la protección de los datos personales a través de labores de vigilancia, puntualizando, en relación con el *habeas data* que:

"[…] Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no solo deben depender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones […]".

Respecto a la relación entre la Libertad de Expresión y el *habeas data*, la sentencia **T-277 de 2015** prescribió:

"[…] La libertad de expresión se deriva de que este derecho no solo faculta a las personas para manifestar sus ideas y opiniones, y para transmitir información, sino que también protege que el contenido expresado se difunda y llegue a otros […]".

Finalmente, es importante tener en cuenta la sentencia SU-139 de 2021 en virtud de la cual la Corte reitera el contenido y alcance del derecho al *habeas data*, así:

"[…] El habeas data es un derecho fundamental autónomo, que busca proteger el dato personal, en tanto información que tiene la posibilidad de asociar un determinado contenido a una persona natural en concreto, cuyo ámbito de acción es el proceso en virtud del cual un particular o una entidad adquiere la potestad de captar, administrar y divulgar tales datos. Igualmente, debe destacar que estas dos dimensiones están íntimamente relacionadas con el núcleo esencial del derecho, el cual, a la luz de la Sentencia C-540 de 2012, se compone de los siguientes contenidos mínimos: 1) el derecho de las personas a conocer (acceder) a la información que sobre ellas está recogida en las bases de datos; 2) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; 3) el derecho a actualizar la información; 4) el derecho a que la información contenida en las bases de datos sea corregida; y, 5) el derecho a excluir información de una base de datos (salvo las excepciones previstas en las normas) […]".

7. DERECHO COMPARADO

Unión Europea: Reglamento General de Protección de Datos (RGPD). Como se ha reiterado a lo largo del presente proyecto de ley, las medidas propuestas se encuentran inspiradas, entre otros, en el Reglamento General de Protección de Datos, el cual ha provocado un cambio importante en el abordaje mundial de la protección de datos, impulsando la adopción de marcos normativos sólidos y elevando los estándares de privacidad y seguridad en el procesamiento de datos personales.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea es una normativa que fue adoptada el 27 de abril de 2016 y entró en vigor el 25 de mayo de 2018. El RGPD tiene como objetivo proteger los derechos y libertades fundamentales en lo que respecta al procesamiento de los datos personales.

Establece una serie de principios y obligaciones que deben cumplir las organizaciones que procesan datos personales, así como los derechos que tienen los individuos sobre sus datos. Algunos de los aspectos clave del RGPD son los siguientes:

Consentimiento: Se requiere un consentimiento claro y explícito de los individuos para procesar sus datos personales. El consentimiento debe ser libremente dado, específico, informado e inequívoco.

Derechos de los individuos: El RGPD otorga a los individuos una serie de derechos, como el derecho de acceso, rectificación, supresión, restricción del procesamiento, portabilidad de datos y oposición al procesamiento de sus datos personales.

Responsabilidad y rendición de cuentas: Las organizaciones son responsables de garantizar el cumplimiento del RGPD y deben implementar medidas técnicas y organizativas adecuadas para proteger los datos personales y demostrar su cumplimiento.

Notificación de violaciones de datos: En caso de violación de seguridad que pueda afectar los derechos y libertades de las personas, las organizaciones están obligadas a notificar a la autoridad de protección de datos competente y, en algunos casos, también a los individuos afectados.

Transferencias internacionales: El RGPD establece reglas estrictas para la transferencia de datos personales a países fuera de la Unión Europea, asegurando un nivel adecuado de protección de los datos.

Designación de un Delegado de Protección de Datos (DPD): Algunas organizaciones están obligadas a designar un DPD, una persona encargada de supervisar el cumplimiento del RGPD dentro de la organización.

Ley de Protección de Información Personal y Documentos Electrónicos de Canadá (PIPEDA). Esta ley federal es aplicable a las organizaciones que recopilan, utilizan o revelan datos personales en el ámbito comercial en Canadá. La PIPEDA establece las reglas para el manejo adecuado de los datos personales y los derechos de los individuos en relación con sus datos.

Ley de Protección de Datos Personales de Japón. Regula la recopilación, uso y divulgación de datos personales por parte de las organizaciones en Japón. También establece ciertos derechos de los individuos y requisitos para las transferencias internacionales de datos.

Ley de Protección de Datos Personales de Brasil (LGPD). Esta ley brasileña, Ley número 13.709/2018, inspirada en el RGPD de la Unión Europea, establece las reglas para el tratamiento de los datos personales en Brasil. La LGPD busca proteger los derechos fundamentales de privacidad y establece obligaciones para las organizaciones que procesan datos en Brasil.

Ley Orgánica de Protección de Datos Personales de Ecuador (LOPD). Esta reciente ley ecuatoriana, también inspirada en los principios rectores del RGPD de la Unión Europea, establece las reglas para el tratamiento de los datos personales en Ecuador e introduce por primera vez en el país, una regulación sobre protección de datos. La LOPD busca garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección.

Ley de Protección de Datos Personales en Argentina. La Ley número 25.326 establece las reglas para la protección de datos personales en Argentina. Esta ley establece los principios para el tratamiento de los datos, los derechos de los titulares de los datos y las obligaciones de las organizaciones que procesan datos personales.

Ley de Protección de Datos Personales en Chile. La Ley número 19.628 regula la protección de datos personales en Chile. Esta ley establece los principios y las reglas para el tratamiento de datos, así como los derechos de los titulares de los datos y las obligaciones de las organizaciones.

Ley de Protección de Datos Personales en México. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece las reglas para el tratamiento de datos personales por parte de los particulares en México. Esta ley también establece los derechos de los titulares de los datos y las obligaciones de las organizaciones.

Ley de Protección de Datos Personales en Uruguay. La Ley número 18.331 regula la protección de datos personales en Uruguay. Esta ley establece los principios y las reglas para el tratamiento de los datos, los derechos de los titulares de los datos y las obligaciones de las organizaciones.

Marco de Privacidad de Datos EU-USA (2023). Esta decisión de la Comisión Europea concluye que los Estados Unidos garantizan un nivel de protección adecuado (equiparable al de la Unión Europea) de los datos personales transferidos de la UE a empresas estadounidenses al amparo del nuevo marco.

Ley Federal de Protección de datos (LPD) de Suiza. La Ley de Protección de Datos en Suiza y las disposiciones de aplicación de las nuevas Ordenanzas de Protección de Datos (OPDo) entrarán en vigor el 1º de septiembre de 2023, cuyo como objetivo es ajustar la legislación suiza sobre protección de datos a los avances tecnológicos recientes y a las necesidades de la sociedad actual.

7. CONFLICTOS DE INTERÉS

Dando alcance a lo establecido en el artículo 3° de la Ley 2003 de 2019, *por la cual se modifica parcialmente la Ley 5ª de 1992,* se hacen las siguientes consideraciones a fin de describir la circunstancias o eventos que podrían generar conflicto de interés en la discusión y votación de la presente iniciativa legislativa, de conformidad con el artículo 286 de la Ley 5ª de 1992, modificado por el artículo 1° de la Ley 2003 de 2019, que reza:

"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.

Se entiende como conflicto de interés una situación donde la discusión o votación de un proyecto de ley o acto legislativo o artículo, pueda resultar en un beneficio particular, actual y directo a favor del congresista.

A. Beneficio particular: aquel que otorga un privilegio o genera ganancias o crea indemnizaciones económicas o elimina obligaciones a favor del congresista de las que no gozan el resto de los ciudadanos. Modifique normas que afecten investigaciones penales, disciplinarias, fiscales o administrativas a las que se encuentre formalmente vinculado.

B. *Beneficio actual: aquel que efectivamente se configura en las circunstancias presentes y existentes al momento en el que el congresista participa de la decisión.*

C. Beneficio directo: aquel que se produzca de forma específica respecto del congresista, de su cónyuge, compañero o compañera permanente, o parientes dentro del segundo grado de consanguinidad, segundo de afinidad o primero civil. (...)".

Sobre este asunto la Sala Plena Contenciosa Administrativa del Honorable Consejo de Estado en su sentencia 02830 del 16 de julio de 2019, m. p. Carlos Enrique Moreno Rubio, señaló que:

"*No cualquier interés configura la causal de desinvestidura en comento, pues se sabe que solo lo será aquél del que se pueda predicar que es directo, esto es, que per se el alegado beneficio, provecho o utilidad encuentre su fuente en el asunto que fue conocido por el legislador; particular, que el mismo sea específico o personal, bien para el congresista o quienes se encuentren relacionados con él; y actual o inmediato, que concurra para el momento en que ocurrió la participación o votación del congresista, lo que excluye sucesos contingentes, futuros o imprevisibles. También se tiene noticia que el interés puede ser de cualquier naturaleza, esto es, económico o moral, sin distinción alguna".*

Se estima que la discusión y aprobación del presente Proyecto de ley 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 5ª de 1992 modificado por la Ley 2003 de 2019, no exime al Congresista de identificar causales adicionales en las que pueda estar incurso.

9. 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".

El presente proyecto de ley no ordena a las entidades públicas erogaciones presupuestales. Por lo anterior, la iniciativa no acarrea la necesidad de presentar un análisis de impacto fiscal por parte de los autores.

10. CONCLUSIONES.

En los términos expuestos, se presenta ante el Congreso de la República el Proyecto de Ley Estatutaria, *por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales,* para que sea tramitado, y con el apoyo de las y los Congresistas sea discutido y aprobado.

De las y los Congresistas,

11. REFERENCIAS

Superintendencia Financiera. Respuesta Derecho de Petición UTL Mafe Carrascal. Bogotá, D. C.

Superintendencia de Industria y Comercio. Respuesta Derecho de Petición UTL Mafe Carrascal. Bogotá, D. C.

(Defensoría del pueblo, 2011, como se cita en Corte Constitucional, Sala plena, Sentencia del 6 de octubre de 2011, exp. PE 032)

Política Nacional para la Transformación Digital e Inteligencia Artificial. (2019). CONPES 3975. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf

Español, A. G., Uribe, E. T., Ayerbe, P. G., Mujica, M. P. (2021). Marco Etico para la Inteligencia Artificial. Recuperado de: https://inteligenciaartificial.gov.co/static/img/MARCO_ETICO.pdf

INFOBAE (2022). Se dispararon las quejas por protección de datos: SIC. Recuperado de: https://www.infobae.com/america/colombia/2022/01/29/se-dispararon-las-quejas-por-proteccion-de-datos-sic/

CALDERON, R.A. (2021). ¿Cómo defender nuestra privacidad e identidad cerebral frente a los riesgos de la neurotecnología? Recuperado de: https://cincodias.elpais.com/cincodias/2021/01/27/legal/1611779453_654051.html

RAMIREZ, M, J. (2023). Uso de las redes sociales en Colombia: 90.5% utiliza Facebook. M4RKETING ECOMMERCE CO. Disponible en: https://marketing4ecommerce.co/uso-de-redes-sociales-en-colombia-90-5-utiliza-facebook/

Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. (2017). GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Página 6. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

Salazar Castellanos, D. (25 de enero de 2023). ¿Por qué hay una ola de ciberataques en Colombia y el país está tan vulnerable? Bloomberg Linea. https://www.bloomberglinea.com/2023/01/25/porque-hay-una-ola-de-ciberataques-en-colombia-y-el-pais-aun-es-tan-vulnerable/

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos Personales. (15 de marzo de 2022). Estudio de medidas de seguridad en el tratamiento de datos personales. https://www.sic.gov.co/sites/default/files/files/2022/Estudio%20de%20seguridad%202022%2015III2022.pdf

Lesmes Díaz, L. (10 de abril de 2023). Colombia recibió 20.000 millones de ciberataques en 2022. El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-colombia-datos-sobre-ciberataques-en-el-pais-757651

Pachón, C. (22 de diciembre de 2022). Los Ciberataques más famosos del 2021 en Colombia y el mundo. NSIT – Information technology. https://www.nsit.com.co/los-ciberataques-mas-famosos-del-2021-en-colombia-y-el-mundo/

Superintendencia de Industria y Comercio. (2015). Guía para la Implementación del Principio de Responsabilidad Demostrada (accountability). SIC. https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Instituto Nacional de Seguridad y Salud en el Trabajo (INSST). (2018). Ingeniería de la resiliencia: conceptos básicos del nuevo paradigma en seguridad. INSST. https://www.insst.es/documents/94886/564690/ntp-1.132w.pdf/1791350b-969f-4ded-885a-8eaa46b8e987

Superintendencia de Industria y Comercio. guía para la implementación del principio de responsabilidad DEMOSTRADA en las transferencias internacionales de datos personales. (2019).SIC.P.8.https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales.pdf

Reglamento General de Protección de Datos, 2016, Considerando 146. Obtenido de: https://gdpr-text.com/es/read/recital-146/#:~:text=(146)%20El%20responsable%20o%20el,en%20infracción%20del%20presente%20Reglamento.

Asuntos legales (2020) Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. Obtenido de: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651

Corte Constitucional. (1992). Sentencia T-414 de 1992, Sala Primera de Revisión. M. P. Ciro Angarita Barón. Bogotá.

Corte Constitucional. (1995). Sentencia SU-082 de 1995, Sala Primera de Revisión. M. P. Jorge Arango Mejía. Bogotá.

Corte Constitucional. (2002). Sentencia T-729 de 2002, Sala Séptima de Revisión. m. p. Eduardo Montealegre Lynett. Bogotá.

Corte Constitucional. (2011). Sentencia C-748 de 2011, Sala Plena. M. P. Jorge Ignacio Pretelt Chaljub. Bogotá.

Corte Constitucional. (2015). Sentencia T-277 de 2015, Sala Primera de Revisión. M. P. María Victoria Calle Correa. Bogotá.

Corte Constitucional. (2021). Sentencia SU -139 de 2021, Sala Plena. M. P. Jorge Enrique Ibáñez Najar. Bogotá.

OEA. (2021). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Oas.org. Recuperado el 17 de julio de 2023, de https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Rojas-Bejarano, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.