REPÚBLICA DE COLOMBIA

GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

ISSN 0123 - 9066

AÑO XXXV - Nº 1217 Bogotá, D. C., martes, 8 de septiembre de 2026 EDICIÓN DE 33 PÁGINAS

DIRECTORES: DIEGO ALEJANDRO GONZÁLEZ GONZÁLEZ
SECRETARIO GENERAL DEL SENADO
www.secretariasenado.gov.co

MIGUEL ÁNGEL SÁNCHEZ VÁSQUEZ
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 282 DE 2026 CÁMARA

por la cual se modifica parcialmente la Ley 1581 de 2012 y se dictan otras disposiciones relativas al derecho fundamental a la protección de datos personales.

Bogotá, D. C., agosto de 2026

Secretario

Secretaría General

Cámara de Representantes

Asunto: Radicación del Proyecto de Ley Estatutaria número 282 de 2026 Cámara, *por la cual se modifica parcialmente la Ley 1581 de 2012 y se dictan otras disposiciones relativas al derecho fundamental a la protección de datos personales.*

Respetado Secretario,

Por medio de la presente y de conformidad con lo establecido en el artículo 154 de la Constitución Política, así como en los artículos 139, 140 y 149 de la Ley 5ª de 1992, me permito someter a consideración del Honorable Congreso de la República el Proyecto de Ley Estatutaria número 282 de 2026 Cámara, *por la cual se modifica parcialmente la Ley 1581 de 2012 y se dictan otras disposiciones relativas al derecho fundamental 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,

MARÍA FERNANDA CARRASCAL ROJAS
Representante a la Cámara por Bogotá

DUVALIER SÁNCHEZ ARANGO
Senador de la República

PROYECTO DE LEY ESTATUTARIA NÚMERO 282 DE 2026 CÁMARA

por la cual se modifica parcialmente la Ley 1581 de 2012 y se dictan otras disposiciones relativas al derecho fundamental a la protección de datos personales.

El Congreso de Colombia

DECRETA:

Artículo 1°. *Objeto.* La presente ley tiene por objeto modificar parcialmente la Ley Estatutaria 1581 de 2012, fortalecer el régimen jurídico relativo al derecho fundamental a la protección de datos personales y actualizar la normatividad vigente.

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

Artículo 2°. *Ámbito de aplicación*. Las disposiciones contenidas en la presente ley serán aplicables a:

1. El tratamiento de datos personales, realizado por cualquier persona natural o jurídica, de carácter público o privado, o por cualquier otra entidad, sin importar el medio utilizado, el país de residencia o domicilio de los sujetos obligados, ni el lugar donde se encuentren ubicados los datos, siempre que suceda alguna de las siguientes circunstancias:

a) El tratamiento se lleve a cabo en el territorio del Estado colombiano, o

b) Las actividades de tratamiento estén relacionado con la oferta de bienes o servicios, a título oneroso o no, a titulares ubicados en Colombia, o

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

2. Cuando así lo disponga el derecho internacional público.

3. Cuando medie disposición legal o contractual que así lo determine.

4. A todo sujeto obligado, que aun sin estar establecido en Colombia, actúa en virtud de una misión diplomática, embajada u oficina consular.

Las disposiciones contenidas en esta ley no serán aplicables a los siguientes tratamientos:

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

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

c) 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;

d) Los realizados por autoridades competentes que tengan como fin y contengan información de inteligencia y contrainteligencia y que sea realizado por una autoridad pública con competencia para ello;

e) Los regulados por la Ley 1266 de 2008, y por las leyes que la modifiquen o subroguen, excepto lo referido al régimen sobre transferencias internacionales de datos personales.

Parágrafo 1°. Los derechos y principios sobre protección de datos personales establecidos en esta ley serán aplicables a todos los tratamientos incluidos los indicadas en el numeral 4 del presente artículo, con los límites dispuestos en esta ley y sin reñir con los datos amparados por una reserva legal. En el evento en que la normatividad especial que regule el tratamiento en los sistemas de información, las bases de datos o archivos exceptuados prevea derechos o principios que tengan en consideración las finalidades específicas del tratamiento y la naturaleza especial de los datos, los mismos aplicarán de preferencia a los previstos en la presente ley.

Parágrafo 2°. Los responsables y encargados del tratamiento de datos personales no domiciliados en el Estado colombiano deberán activar un canal de contacto y designar, por escrito, un representante con plenos poderes ante la Autoridad Nacional de Protección de Datos Personales, y/o establecer una sucursal en el país, para la debida atención de los asuntos relacionados con el cumplimiento de la Ley 1581 de 2012. El Gobierno nacional en un término de seis (6) meses a partir de la promulgación de la presente ley, reglamentará las condiciones y el momento a partir del cual será exigible la obligación de contar con dicho representante o sucursal.

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 los literales a), e y g), y adiciónese los literales h), i), j), k), l), m), n), o), p), q), r), s), t) y u) del artículo 3° de la Ley 1581 de 2012 en los siguientes términos:

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

a) Autorización: Consentimiento previo, expreso, libre, inequívoco, informado y específico del Titular o su representante, manifestado mediante una declaración o una clara acción afirmativa para llevar a cabo el tratamiento de datos personales.

(...)

e) **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;

(...)

g) 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;

h) 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.

i) 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.

j) Datos genéticos: Datos Personales sobre las características hereditarias de una persona natural, obtenida por procedimientos científicos, que proporcionan información única sobre la fisiología, desarrollo biológico o estado de salud;

k) 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;

l) 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;

m) Elaboración de perfiles: Toda forma de tratamiento de datos personales mediante el cual se evalúa o caracteriza a una persona natural, se predice su comportamiento o se infiere información que le concierne;

n) 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;

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. Los datos seudonimizados conservarán su carácter de datos personales;

p) 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;

q) 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 a los derechos fundamentales;

r) 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;

s) Evaluación de impacto en protección de datos personales: Proceso preventivo y sistemático orientado a identificar, analizar y mitigar los posibles riesgos derivados del tratamiento de datos personales para los derechos y libertades de los titulares. Este procedimiento permite describir detalladamente las operaciones de tratamiento, evaluar su necesidad y proporcionalidad, así como establecer medidas de seguridad y cumplimiento que respondan al nivel de riesgo identificado;

t) Tecnologías de mejora de la privacidad: Conjunto de herramientas, metodologías y procedimientos que permiten realizar el tratamiento de los datos personales de una manera segura, reforzando su confidencialidad y reduciendo los riesgos de identificación, empleando técnicas como la anonimización, la seudonimización o el cifrado u otras medidas equivalentes. Estas medidas deberán integrarse en los procesos de tratamiento desde su diseño y por defecto.

Artículo 4°. Modifíquese el literal e), adiciónense los literales i), j), k), l), m) y n), y deróguese el literal c) del artículo 4° de la Ley 1581 de 2012, en los siguientes términos:

Artículo 4°. ***Principios para el tratamiento de datos personales.*** En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

(…)

e) Principio de transparencia: En el tratamiento debe garantizarse el derecho del Titular a obtener, en cualquier momento y sin restricciones, información clara y suficiente 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.

(…)

i) 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…

De igual manera, adoptarán de manera progresiva el uso de tecnologías de mejora de la privacidad, con el fin de garantizar la protección de los datos personales, desde el diseño y por defecto.

La Autoridad Nacional de Protección de Datos Personales expedirá guías y lineamientos que permitan a los responsables y encargados, especialmente a las micro, pequeñas y medianas empresas, implementar las medidas de responsabilidad demostrada en forma gradual y proporcional.

j) Principio de lealtad y no discriminación: 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.

k) Principio de minimización: La recolección de datos personales deberá limitarse a los datos adecuados, pertinentes y estrictamente necesarios en relación con las finalidades específicas, explícitas y legítimas para las cuales se realiza el tratamiento.

l) 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.

m) 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.

n) 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.

Artículo 5°. Adiciónese el siguiente inciso al artículo 5° de la Ley 1581 de 2012:

También se entenderán como datos sensibles los datos de geolocalización, los datos relativos a la identidad o expresión de género, los datos genéticos y los neurodatos.

Artículo 6°. Adiciónese el siguiente el literal f) al artículo 6° de la Ley 1581 de 2012, en los siguientes términos:

Artículo 6°. ***Tratamiento de datos sensibles.*** Se prohíbe el tratamiento de datos sensibles, excepto cuando:

(...)

f) El Tratamiento sea necesario para el cumplimiento de obligaciones legales y el ejercicio de derechos específicos del responsable del tratamiento o del titular.

Artículo 7°. Modifíquese el artículo 7° de la Ley 1581 de 2012, el cual quedará así:

Artículo 7°. ***Tratamiento de datos personales de 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 primero. 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 segundo. 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 tercero. 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 sólo podría concederse nuevamente por el mutuo acuerdo de los representantes, o mediante decisión judicial que declare su representación legal.

Parágrafo cuarto. 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 los literales a), b) y c), subróguese el literal e), y adiciónese los literales g), h), i), k), l), m) y un parágrafo al artículo 8° de la Ley 1581 de 2012, en los siguientes términos:

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. Estos derechos se podrán ejercer, entre otros, frente a datos desactualizados, parciales, inexactos, incompletos, fraccionados o que induzcan a error o cuando sea necesario para proteger otros derechos fundamentales;

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;

(…)

e) Oponerse al tratamiento de sus datos personales, entre otros, cuando el tratamiento carezca de una base legítima que lo fundamente, afecte sus derechos fundamentales o se adelante con fines de publicidad o marketing directo, incluida la elaboración de perfiles en la medida que esté relacionado con dicha actividad;

(...)

g) No ser objeto de decisiones que limiten sus derechos fundamentales, tengan efectos discriminatorios o le afecten significativamente basadas únicamente en el tratamiento automatizado de sus datos personales o en la elaboración de perfiles. De presentarse, el titular tendrá derecho a expresar su punto de vista, recibir una explicación clara, accesible y suficiente sobre la lógica, los criterios y los factores determinantes utilizados, solicitar la reconsideración de la decisión y la intervención de un ser humano. Todo ello, sin comprometer secretos comerciales, la propiedad intelectual ni los derechos de terceros.

Cuando la decisión automatizada se fundamente en el cumplimiento de un contrato o en la ley, el titular conservará el derecho a la intervención humana y a la explicación clara y suficiente.

h) Solicitar y recibir una copia de sus datos personales en un formato estructurado y comúnmente utilizado que permita su transferencia a otro responsable cuando ello no suponga una carga excesiva o irrazonable para el responsable. Cuando sea técnicamente posible, el titular puede solicitar que sus datos personales se transfieran directamente de responsable a responsable.

i) Suprimir sus datos personales, entre otros, cuando, su tratamiento esté expresamente prohibido, no haya sido autorizado o el titular revoque su autorización y el tratamiento no se funde en otra base legitimadora, no sea necesario, se haya cumplido el término de caducidad del dato, o cuando de ello dependa el goce y la protección de otros derechos fundamentales.

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

k) 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;

l) 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;

m) Obtener una indemnización por los daños causados por el indebido tratamiento de sus datos personales.

Parágrafo. Cuando el encargado del tratamiento reciba una solicitud presentada por un titular para el ejercicio de cualquiera de los derechos previstos en el presente artículo, deberá informarle en el término de dos (2) días hábiles, la identificación, la dirección física o electrónica y el número de teléfono del responsable del tratamiento y, cuando resulte procedente, remitirle la solicitud para que este le dé el trámite correspondiente, de conformidad con la normativa aplicable.

Artículo 9°. Subróguese 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 cuando:

a) El titular haya otorgado autorización previa para el tratamiento de sus datos personales para uno o varios fines específicos. La autorización deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior;

b) Sea necesario para el cumplimiento de un deber legal exigible al responsable del tratamiento;

c) Sea necesario para el cumplimiento de obligaciones nacidas de un negocio jurídico celebrado por el titular, para la ejecución de un contrato en el que el titular es parte o para la aplicación, a petición de este, de medidas precontractuales;

d) Sea necesario para proteger la vida o la salud del titular o de otra persona natural;

e) Sea necesario para el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución o la ley;

f) Sea 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 primero. Lo dispuesto en el literal f) no será de aplicación al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.

Parágrafo segundo. 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.

Artículo 10. Subróguese el artículo 10 de la Ley 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.

Artículo 11. Adiciónese los literales e), f), g), h), i), j) y k) del artículo 12 de la Ley 1581 de 2012, en los siguientes términos:

Artículo 12. ***Deber de informar al titular.*** El responsable del tratamiento deberá informar al titular, de manera clara y expresa, en el momento en que obtenga los datos personales, ya sea directamente o a través de terceros, sobre lo siguiente:

(...)

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

f) Los destinatarios de los datos personales, si los hubiera;

g) 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;

h) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar dicho plazo;

i) 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;

j) 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;

k) La fuente de la que proceden los datos personales cuando estos no hubieran sido obtenidos directamente del titular.

Artículo 12. Modifíquese los literales b), c), h), i) y n), y adiciónese los siguientes literales o), p), q), r), s), t), u, v), w), x), y), z) y un parágrafo al artículo 17 de la Ley 1581 de 201, en los siguientes términos:

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:

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;

(...)

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

i) 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;

r) Informar a la autoridad nacional de protección de datos personales, dentro de las setenta y dos (72) horas siguientes a su detección, los incidentes de seguridad que comprometan datos personales. De igual manera, deberá comunicar a los titulares afectados cuando tales incidentes impliquen un alto riesgo para el ejercicio de sus derechos y libertades.

(…)

o) Tomar medidas razonables para verificar que la autorización sea otorgada en los términos previstos en el artículo 7° de la presente ley, y abstenerse de incurrir en las prohibiciones previstas en dicho artículo, con el fin de garantizar el derecho a la protección de datos personales de niños, niñas y adolescentes;

p) 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;

q) Aplicar medidas técnicas y organizativas apropiadas tanto con anterioridad como durante el Tratamiento de datos personales a fin de cumplir los principios y los derechos de los titulares establecidos en la presente ley, atendiendo a criterios de protección de datos personales por diseño y por defecto en dichos tratamientos;

r) Respetar en sus actividades de tratamiento de datos personales los principios contenidos en el artículo 4° de la presente ley;

s) Realizar evaluaciones de impacto en protección de datos personales cuando se realice tratamiento de datos personales a gran escala, tratamiento automatizado o semiautomatizado, incluida la elaboración de perfiles, o cuando en el desarrollo de una actividad o varias actividades de tratamiento, sea probable que exista un alto riesgo de afectación a los derechos de los titulares, incluyendo, en todo caso, el tratamiento automatizado de datos sensibles.

t) Implementar medidas apropiadas, oportunas, eficaces y demostrables para garantizar el adecuado cumplimiento de la presente ley y de sus normas reglamentarias;

u) Designar un oficial de protección de datos cuando realice tratamiento de datos personales a gran escala, cuando se realice tratamiento de datos sensibles como parte actividad principal o cuando el tratamiento lo lleve a cabo una autoridad u organismo público;

v) Garantizar que las transferencias internacionales cumplan las condiciones establecidas en la presente ley y sus decretos reglamentarios;

w) Formalizar mediante un contrato la prestación de servicios de tratamiento de datos con el encargado en el que se establezcan de manera clara las condiciones, finalidades, obligaciones y medidas de seguridad aplicables al tratamiento, garantizando el cumplimiento de la presente ley y de las instrucciones impartidas por el responsable.

x) Incorporar de manera progresiva, tecnologías de mejora de la privacidad en los sistemas y procesos de tratamiento de los datos personales, especialmente, en aquellos que involucren análisis de datos automatizados o tratamiento de datos a gran escala, con el fin de minimizar los riesgos de identificación, exposición o uso indebido de los datos personales.

y) 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;

z) 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 lo relacionado con 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 13. Modifíquese los literales c), e), f), j) y k), subróguese los literales g) y h), y adiciónense los siguientes literales m), n), ñ), o), p), q) y r) del artículo 18 de la Ley 1581 de 2012, en los siguientes términos:

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:

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 de datos, informará inmediatamente al responsable;

(...)

e) 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;

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

g) Respetar en sus actividades de tratamiento de datos personales los principios contenidos en el artículo 4° de la presente ley;

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

(...)

j) 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;

k) Informar 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;

(…)

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

n) Implementar medidas apropiadas, oportunas, eficaces y demostrables para garantizar el adecuado cumplimiento de la presente ley y sus normas reglamentarias;

ñ) Designar un oficial de protección de datos cuando se realice tratamiento de datos personales a gran escala, cuando se realice tratamiento de datos sensibles como parte actividad principal o cuando el tratamiento lo lleve a cabo una autoridad u organismo público;

o) Formalizar mediante un contrato de encargo la prestación de servicios de tratamiento de datos personales con el responsable;

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

q) Devolver al responsable los datos personales objeto del encargo cuando finalice la relación contractual o se cumpla su objeto;

r) 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 14. Modifíquese el título del Capítulo 1, del Título VII, de la Ley 1581 de 2012, el cual quedará así: "De las Autoridades de Protección de Datos Personales", así como el artículo 19, de la Ley 1581 de 2012, el cual quedará así:

Artículo 19. ***Autoridad Nacional de Protección de Datos Personales.*** La Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales ejercerá las funciones de Autoridad Nacional de Protección de Datos Personales de manera imparcial, autónoma e independiente.

La Delegatura para la Protección de Datos Personales fungirá como garantía administrativa del derecho fundamental a la protección de datos personales. Tendrá a su cargo las funciones de inspección, vigilancia y control para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

La titularidad de la delegatura para la protección de datos personales estará a cargo de un superintendente delegado para la protección de datos personales que será nombrado por el Superintendente de Industria y Comercio, por un período de cuatro (4) años, sin posibilidad de reelección inmediata, previa convocatoria pública, de una lista conformada por personas que, por sus antecedentes personales, profesionales y de conocimiento en la materia, aseguren independencia de criterio, eficiencia y objetividad. El Gobierno nacional reglamentará lo relacionado con el procedimiento para su nombramiento.

Parágrafo 1°. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

Parágrafo 2°. El Ministerio de Ciencia, Tecnología e Innovación actuará como autoridad técnica asesora en materia de Tratamiento de datos científicos, datos derivados de investigaciones y datos asociados a tecnologías emergentes, de conformidad con sus competencias. La Superintendencia de Industria y Comercio y la Procuraduría General de la Nación podrán requerir su concepto especializado para la formulación de guías, lineamientos y estándares técnicos que involucren el tratamiento de datos personales en el manejo de información científica, tecnológica o de innovación.

Artículo 15. Adiciónese el siguiente artículo 19A a la Ley 1581 de 2012:

Artículo 19A. ***De la Procuraduría Delegada con funciones de Protección de Datos Personales.*** La Procuraduría General de la Nación tendrá un plazo máximo de seis (6) meses, contados a partir de la entrada en vigencia de esta ley, para la puesta en funcionamiento de una Procuraduría Delegada con funciones de protección de datos personales, mediante la cual ejercerá las funciones constitucionales y legales relacionadas con la promoción y garantía del derecho fundamental a la protección de datos personales en el sector público y velará por el cumplimiento de los principios y deberes establecidos en la presente ley.

El Procurador Delegado con funciones de Protección de Datos Personales será de libre nombramiento y remoción del Procurador General de la Nación.

Parágrafo 1°. Lo establecido en el presente artículo se hará mediante redistribución de la planta interna de la Procuraduría General de la Nación dentro del marco del presupuesto aprobado para la respectiva vigencia fiscal.

Parágrafo 2°. Las funciones de la Procuraduría Delegada con funciones de Protección de Datos Personales se ejercerá sin perjuicio de las competencias de la Superintendencia de Industria y Comercio sobre entidades públicas que actúen como responsables o encargados del tratamiento.

Artículo 16. Subróguese y adiciónense los literales k), l), m), n), ñ), o) y p) al artículo 21 de la Ley 1581 de 2012, el cual quedará así:

Artículo 21. ***Funciones de la Autoridad Nacional de Protección de Datos Personales.*** La Superintendencia de Industria y Comercio a

través de la Delegatura para la Protección de Datos Personales ejercerá las siguientes funciones:

(…)

k) Promover y realizar acciones de cooperación internacional, investigación y armonización normativa, en especial con las autoridades de protección de datos personales de otros Estados, con el fin de garantizar y hacer efectivo el cumplimiento de los principios y deberes consagrados en la presente ley;

l) Celebrar acuerdos de cooperación con entidades públicas o privadas, nacionales o extranjeras, en el ámbito de su competencia y para el cumplimiento de sus funciones;

m) Coordinar acciones con la Procuraduría Delegada con funciones para la Protección de Datos Personales orientadas al cumplimiento de los principios y deberes de la presente ley; entre otras, compartir información, trasladar pruebas, realizar visitas e impartir instrucciones conjuntas;

n) Emitir órdenes administrativas de obligatorio cumplimiento para entidades públicas o privadas con el fin de garantizar el debido tratamiento de los datos personales y los derechos de los titulares de los datos personales;

ñ) Desarrollar y promover códigos de conducta y mecanismos de certificación para contribuir a la correcta aplicación de la presente ley;

o) Coordinar con el Ministerio de Ciencia, Tecnología e Innovación el diseño y promoción de lineamientos y buenas prácticas para el tratamiento de datos personales en el desarrollo de proyectos de investigación, desarrollo tecnológico e innovación, incluidos los que utilicen inteligencia artificial, biotecnología, nanotecnología o cualquier otra tecnología.

p) Las demás que le sean asignadas por ley.

Artículo 17. Adiciónese el siguiente artículo 21A a la Ley 1581 de 2012:

Artículo 21A. ***Funciones de vigilancia preventiva sobre autoridades y control disciplinario de servidores públicos por parte de la Procuraduría General de la Nación.*** La Procuraduría General de la Nación ejercerá las siguientes funciones:

a) Velar por la observancia de los principios para el Tratamiento de Datos Personales establecidos en el artículo 4° de la presente ley;

b) Velar por la garantía de los derechos de los titulares reconocidos en el artículo 8° de la presente ley y emitir alertas o recomendaciones preventivas ante riesgos que puedan afectar su goce o ejercicio;

c) Promover la incorporación de buenas prácticas en materia de protección de datos personales en la gestión pública;

d) Iniciar investigaciones disciplinarias cuando identifique presuntas infracciones al régimen de protección de datos por parte de funcionarios públicos;

e) Requerir la realización de evaluaciones de impacto en protección de datos personales, cuando las entidades públicas decidan implementar sistemas, aplicaciones o tecnologías que impliquen tratamiento de datos personales a gran escala o tratamiento automatizado de datos personales, y pronunciarse sobre dichas evaluaciones por la vía de recomendaciones;

f) Realizar seguimiento al uso de sistemas de inteligencia artificial, big data, biometría, georreferenciación, sistemas de vigilancia y otras tecnologías que procesen datos personales por parte de entidades del Estado, a efectos de prevenir afectaciones a la intimidad, la libertad, la igualdad o la dignidad de las personas;

g) Coordinar con la Superintendencia de Industria y Comercio las actuaciones necesarias en casos donde se requiera una acción conjunta, sin perjuicio de las competencias de dicha entidad;

h) Ejecutar visitas periódicas e inspecciones in situ, utilizando indicadores y herramientas de control que permitan identificar deficiencias y riesgos en la gestión de datos personales;

i) Elaborar informes de las visitas y evaluaciones realizadas, de las recomendaciones y de los planes de acción ordenados, y establecer un sistema para su seguimiento y verificación que incluya términos e indicadores;

j) Desarrollar estrategias de capacitación, divulgación y asesoría técnica dirigidas a entidades públicas, con el fin de fortalecer la cultura institucional de protección de datos personales;

k) Las demás que le sean asignadas por ley.

Parágrafo. Cuando las evaluaciones de impacto en protección de datos personales involucren el Tratamiento de datos científicos, datos genéticos o datos derivados de proyectos de investigación e innovación, la Procuraduría General de la Nación podrá solicitar concepto técnico al Ministerio de Ciencia, Tecnología e Innovación, sin perjuicio de las competencias de las demás autoridades.

Artículo 18. Adiciónese el siguiente artículo 21B a la Ley 1581 de 2012:

Artículo 21B. ***Cooperación interinstitucional en la protección de datos personales.*** Las entidades del Estado deberán prestar a la Superintendencia de Industria y Comercio y a la Procuraduría General de la Nación la colaboración necesaria para el cumplimiento de sus funciones como Autoridades de Protección de Datos Personales. Esta cooperación incluirá, entre otros, el suministro de información, la participación en mesas de trabajo y demás mecanismos de coordinación interinstitucional, la disposición para el desarrollo de actividades conjuntas de inspección y control, la formulación de políticas públicas, la atención de emergencias de seguridad de la información y la promoción de buenas prácticas institucionales.

Cuando el tratamiento de datos personales sea realizado por entidades públicas, la Procuraduría

General de la Nación podrá actuar en forma coordinada con la Superintendencia de Industria y Comercio, sin perjuicio de sus competencias constitucionales.

La Defensoría del Pueblo, los personeros municipales o cualquier entidad y/o funcionario público que reciba una denuncia ciudadana relacionada con vulneración al régimen de protección de datos personales deberá proceder a dar traslado inmediatamente a la Superintendencia de Industria y Comercio y/o a la Procuraduría General de la Nación, según corresponda por competencia.

Artículo 19. Adiciónese el siguiente artículo 21C a la Ley 1581 de 2012:

Artículo 21C. ***Funciones del Ministerio de Ciencia, Tecnología e Innovación en el Tratamiento de datos científicos y tecnológicos.*** El Ministerio de Ciencia, Tecnología e Innovación, en coordinación con la Superintendencia de Industria y Comercio y la Procuraduría General de la Nación expedirá lineamientos técnicos para promover la protección y el uso ético de datos científicos, datos derivados de investigación e innovación y datos asociados a tecnologías emergentes, en armonía con los principios y derechos consagrados en la presente ley. Estos lineamientos deberán alinearse con los estándares nacionales e internacionales y promover la interoperabilidad, la reutilización responsable y la preservación de datos de investigación.

Artículo 20. Subróguese el primer inciso, los literales a) y c) y el parágrafo del artículo 23 de la Ley 1581 de 2012, los cuales quedarán así:

Artículo 23. ***Sanciones.*** La Superintendencia de Industria y Comercio a través de la Delegatura para la 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 diez mil (10.000) 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;

(…)

c) Cierre definitivo de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

(…)

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada, las sociedades de economía mixta y las empresas industriales y comerciales del Estado. Cuando la Autoridad Nacional de Protección de Datos Personales advierta el presunto incumplimiento de los principios o deberes previstos en la presente ley por parte de una autoridad pública, remitirá la actuación a la Procuraduría General de la Nación para lo de su competencia. En todo caso, la Procuraduría General de la Nación podrá llevar a cabo de oficio las investigaciones que considere pertinentes.

Artículo 21. Adiciónense los siguientes literales al artículo 24 de la Ley 1581 de 2012:

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:

(...)

g) La implementación efectiva de medidas de responsabilidad demostrada;

h) El grado de cooperación con la autoridad de protección de datos con el fin de contener o mitigar los posibles efectos adversos de la infracción;

i) La existencia de un oficial de protección de datos, cuando no fuere obligatorio**.**

Artículo 22. Modifíquese el artículo 26 de la Ley 1581 de 2012, el cual quedará así:

Artículo 26. ***Transferencias internacionales de datos.*** La transferencia internacional de datos personales se sujetará a las siguientes reglas:

1. La transferencia internacional de datos personales estará permitida a países que proporcionen niveles adecuados de protección. Se entenderá que un Estado ofrece un nivel adecuado de protección de datos personales cuando cumpla los estándares fijados por la Autoridad Nacional de Protección de Datos Personales sobre la materia, los cuales, en ningún caso, podrán ser inferiores a los previstos en la presente ley para los sujetos obligados.

2. Cuando la transferencia internacional de datos personales se realice a países que no ofrezcan niveles adecuados de protección, se deberá implementar garantías adicionales que aseguren un nivel de protección equivalente al previsto en la presente ley y en sus decretos reglamentarios. Las garantías adicionales podrán consistir en cualquiera de los siguientes mecanismos:

a) Declaración de conformidad ante la Autoridad Nacional de Protección de Datos Personales;

b) Normas corporativas vinculantes aprobadas por la Autoridad Nacional de Protección de Datos Personales, cuando se trate de transferencias entre empresas pertenecientes a un mismo grupo empresarial, con independencia de su ubicación geográfica;

c) Cláusulas contractuales modelo aprobadas por la Autoridad Nacional de Protección de Datos Personales.

Para estos efectos, la Autoridad Nacional de Protección de Datos Personales podrá requerir la información que considere necesaria y adelantar las actuaciones pertinentes para verificar la suficiencia

y el cumplimiento de las garantías adicionales previstas en el presente artículo.

3. Cuando el país de destino no ofrezca niveles adecuados de protección y no sea posible implementar las garantías adicionales previstas en el numeral anterior, se podrá realizar solo excepcionalmente cuando se trate de:

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 acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

e) Transferencias necesarias para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales adoptadas a solicitud del titular;

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

Parágrafo. Las disposiciones del presente artículo serán aplicables a toda transferencia internacional de datos personales, incluso cuando esta se origine en actividades de tratamiento previstas en el artículo 2° de la presente ley.

Artículo 23. ***Vigencia y derogatorias.*** La presente ley rige a partir de su promulgación, modifica los artículos 2°, 3°, 4°, 5°, 6°, 7°, 8°, 12, 17, 18, 19, 21, 23, 24 y 26; subroga los artículos 9° y 10; adiciona los artículos 19A, 21A, 21B y 21C a la Ley 1581 de 2012; y deroga todas las disposiciones que le sean contrarias.

Cordialmente,

MARÍA FERNANDA CARRASCAL ROJAS Representante a la Cámara por Bogotá	DUVALIER SÁNCHEZ ARANGO Senador de la República

EXPOSICIÓN DE MOTIVOS

PROYECTO DE LEY ESTATUTARIA NÚMERO 282 DE 2026 CÁMARA

por la cual se modifica parcialmente la Ley 1581 de 2012 y se dictan otras disposiciones relativas al derecho fundamental a la protección de datos personales.

Son las 6:47 de la mañana en Bogotá. Antes de que una persona pronuncie una sola palabra, ya ha dejado un rastro: la alarma de su teléfono registró la hora en que despertó, la aplicación del clima supo que consultó el pronóstico, el operador celular localizó su posición exacta, y la app de transporte calculó, con base en sus trayectos anteriores, hacia dónde probablemente se dirige. No ha salido de la cama y ya existe, en algún servidor, una versión digital de su rutina más íntima.

Nadie la obligó a entregar esa información. Ella misma activó la ubicación, aceptó los términos y condiciones, configuró sus preferencias. Ahí está la trampa: nadie vigila a esta persona en contra de su voluntad. Ella se expone, cada mañana, de manera voluntaria.

El filósofo surcoreano-alemán Byung-Chul Han ha llamado la atención sobre esta paradoja: la sociedad contemporánea ya no se controla mediante la prohibición o el castigo, sino mediante el exceso de transparencia y la ilusión de libertad. El viejo poder decía "no puedes"; el poder digital dice "puedes, comparte, exponte, sé auténtico", y precisamente porque parece una invitación y no una orden, nadie se resiste a ella. La persona que publica su ubicación, que responde encuestas de salud en una app, que deja que un reloj inteligente registre su ritmo cardíaco durante el sueño, no siente que está siendo vigilada. Siente que se está expresando.

Ese es el giro que hace especialmente difícil legislar sobre datos personales en el siglo XXI: ya no se trata de un Estado o una empresa espiando a ciudadanos pasivos, sino de ciudadanos que, con entusiasmo, construyen su propio expediente. El sujeto se convierte, al mismo tiempo, en vigilante y vigilado de sí mismo. Y como no hay un carcelero visible al cual resistir, tampoco hay una alarma clara que dispare la defensa.

Esta es la razón por la que el derecho no puede seguir apoyando toda la arquitectura de protección de datos en un solo pilar: el consentimiento. Durante años, la lógica ha sido simple -si la persona aceptó, no hay problema-. Pero un consentimiento otorgado en segundos, sobre un formulario de treinta páginas que nadie lee, dentro de una cultura que premia la exposición constante de la vida privada, no es realmente una decisión libre e informada. Es, en el mejor de los casos, una autorización dada bajo las reglas de un juego que la propia persona no diseñó.

Por eso, actualizar el marco legal es reconocer que la autorregulación del mercado y la buena voluntad del usuario no bastan para proteger un derecho fundamental, y que corresponde al Estado establecer bases jurídicas adicionales -más allá del clic de "acepto"- para que el tratamiento de datos personales sea legítimo.

Esto no es una advertencia abstracta. Solo entre 2013 y 2023, la Superintendencia de Industria y Comercio recibió más de 161.000 quejas por presunta vulneración al *habeas data* -una cifra que casi se multiplicó por diez en una década, en la misma medida en que más colombianos empezaron a hacer su vida -bancaria, sentimental, laboral, médica- a través de una pantalla.

Cada uno de esos expedientes tiene, en el fondo, la misma estructura: alguien entregó información

pensando que ejercía una libertad, y descubrió después que había perdido el control sobre ella.

Actualizar la Ley 1581 de 2012 es, entonces, una respuesta a esa paradoja: la de una sociedad que se cree libre porque comparte, sin advertir que esa misma transparencia voluntaria es también la forma más eficaz de control que se ha inventado. La presente iniciativa parte de esa premisa: que proteger los datos personales no es limitar la libertad digital de los colombianos, sino devolverles el control real sobre una libertad que hoy ejercen sin saber que, al mismo tiempo, los excluye.

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.

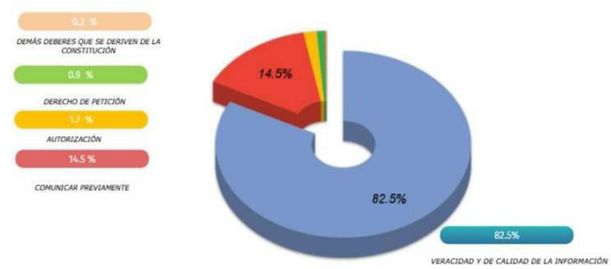
Tabla 2. Quejas presentadas durante (2013-2023 parcial)

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:

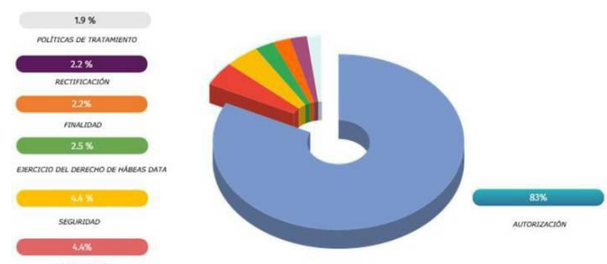
Imagen 1. Número de quejas



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

De1igual 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 2025-2026 bajo el número de radicado PLE 274 de 2025 Cámara, y previamente 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.

Se realizaron dos audiencias públicas así:

En un primer momento, se realizó el día siete (7) 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's, 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.

Posteriormente, se realizó otra audiencia pública el 25 de septiembre de 2025 dio lugar a debate en torno al Proyecto de Ley número 274 de 2025 el cual modifica parcialmente la Ley 1581 de 2012, donde se garantiza el derecho fundamental a la protección de datos personales. En el desarrollo de la audiencia se evidenciaron intervenciones significativas, las cuales demuestran perspectivas enriquecedoras para tener en cuenta dentro del proyecto de ley.

En primera instancia, la intervención de Juan Carlos Upegui, quien es delegado de la Superintendencia de Industria y Comercio, estuvo encaminada a mantener el modelo de regulación actual provisto en el Proyecto de Ley número 1581, resaltando la importancia de la finalidad de la ley en materia de elementos clave para su legislación en América Latina, resaltando la soberanía como factor indispensable en el tratamiento de la información, sin embargo, hace una observación frente al reconocimiento de nuevos derechos.

Seguidamente, se contó con la participación de Sebastián León Giraldo, académico de la Universidad de Los Andes, profundizó en asuntos de derechos fundamentales y la incidencia que poseen las instituciones frente al cumplimiento de los mismos en distintos ámbitos del contexto social colombiano como lo son la educación, la salud y la economía; por tal razón, considera importante garantizar y proteger el derecho a la protección de datos, siendo necesario, involucrar un análisis constitucional para la plena revisión y observación de datos sensibles.

Por otro lado, la incidencia que tuvo la Defensoría del Pueblo como ponente virtual, se vio orientada por sugerir el artículo 1° de integración de la Sentencia T-067 de 2023. Así mismo, defiende como artículo 2°, la extinción de datos perpetrada en el manejo del derecho de hábeas data. Su intervención priorizo la efectividad de mecanismos judiciales en el tema y un ajuste necesario con el Ministerio de Relaciones Exteriores y las Superintendencias con el fin de implementar y coordinar la nueva medida expuesta en el PL 247/2025 C.

En tercera instancia, se evidenció la intervención de la asesora Paula Forero Barrera de la honorable Representante *María Fernanda Carrascal*, quien es autora del Proyecto de Ley número 214 de 2025 Cámara. Propone luchar por la protección y garantía de los datos personales, en tanto que, debe haber una redefinición de reglas que no son claras en la ley vigente, por ejemplo la ampliación de derechos de titulares, datos desmaterializados, la participación ciudadana en torno a las dinámicas de manipulación de los datos personales. Sugiere un mayor fortalecimiento de la Superintendencia de Industria y Comercio (SIC), al igual que, articular las entidades pertinentes para configurar funciones determinadas, impulsando inicialmente la del Consejo Nacional de Bioética. Incentivando la transparencia, la protección y el manejo de datos personales de manera responsable.

Natalia Forero perteneciente a la Cámara Colombiana de Comercio Electrónico, planteó fortalecer los derechos de los y las titulares, abordando la necesidad de que hayan definiciones amplias sobre conceptos que pueden causar controversias jurídicas, al igual que la transparencia proactiva dadas las cargas excesivas para organizaciones. Reiteró el no a decisiones automatizadas y limitar la protección que genere impactos negativos sobre los ciudadanos. Reglamentación sobre transferencia de datos en el comercio internacional donde prevalezca un equilibrio en el manejo de datos.

Posterior a ella, la intervención de Sara Patricia Mora, especialista en protección de datos y ciberseguridad de la firma de abogados Legaltech, mencionó la importancia de focalizar los derechos

de infantes, con la ola de tecnologías en manos de menores de edad, y la supervisión constante para su protección enmarcada en la responsabilidad de protección de datos. La confusión persistente a nivel conceptual sobre el tratamiento de datos automatizado con decisiones automatizadas, puede generar malentendidos en su utilidad. En particular, resaltó el papel de los datos personales como base de la economía nacional, siendo los primeros manejados de manera neutral.

Diana Bernal Representante del Consejo Nacional de Bioética y Universidad del Rosario. Menciona los datos hipersensibles en salud y la conciliación de los proyectos de ley, así como el derecho al olvido garantizado y como deber limitado en las entidades de salud. La protección de datos a menores de edad es una garantía que el Estado tiene que dar a la población. Prestar mayor atención cuando no se está en condición de dar consentimiento y establecer una revisión de cuentas en tratamiento de datos periódicamente.

Adolfo Enrique Gómez, practicante de la Asociación Colombiana de Datos y Privacidad, Menciona la importancia de la PL 274/2025 para aterrizar cambios de flujo internacional en materia de datos y el aumento de la competitividad de Colombia como puerto de protección de datos. Sus observaciones están basadas en la aplicación del proyecto excluye una serie de datos por lo tanto presenta contradicción en el tratamiento de datos y se puede malinterpretar. Debe haber evaluación de inclusión de principios como la minimización de tratamiento de la información encaminada a datos realmente necesarios, teniendo en cuenta las bases legitimadoras del proceso tanto constitucional y legal.

La participación del abogado Víctor Andrés Ayale Lemos, mantuvo una postura a favor del proyecto de ley, argumentando que la actualización de la ley vigente es necesaria y debe mantenerse con el mismo interés legítimo, siendo un punto inicial para el fortalecimiento institucional en función de materializar los derechos de los ciudadanos. La regulación es vital en Colombia, del mismo modo que los usos de las herramientas para gestionarlo sean efectivas y enfocadas a la población vulnerable. El balance normativo resulta ser útil para el debido cumplimiento de la ley.

Luis Félix Barriga Palomino, docente de la Universidad Javeriana de Cali, presenta observaciones al proyecto de ley. Se debe pensar en una unificación legislativa más que en una reforma. Recomienda en virtud de la incertidumbre jurídica pensar en las reglas de conflicto básicas establecidas en el Código Civil Colombiano. En materia de datos de personas fallecidas se debe ahondar más puesto que pueden haber conflictos en los causahabientes, por ejemplo, un enfoque patrimonial importante. Resalta el papel dual de la procuraduría delegada para protección de datos. En materia de IA, requiere la protección de datos en materia de gestión de datos. En consideraciones transversales, debe enfocarse a las MiPYMES, pues puede afectar la carga operacional empresarial, debe existir un régimen especial de protección de datos personales.

Nicolle Rendón, establece la necesidad de la reforma de la Ley 1581 de 2012 en virtud del avance tecnológico en clave del tratamiento de datos personales. Argumentó que se deben incluir principios que busquen reforzar la protección de datos debido a que se había omitido el derecho de oposición en la Ley 1581. En materia de decisiones automatizadas, se busca establecer el oficial de datos y lo considera una figura importante y debe estar presente. La ponente argumenta que no es clara la definición de datos científicos como datos personales sujetos a protección, ya que son datos muy amplios. Por último, sugiere que se incluya el principio de lealtad, el cual considera de derecho comparado y es fundamental en la protección de datos personales.

Juan Diego Castañeda de la Fundación Karisma, realizó su intervención del proyecto enfatizando mejorar los siguientes puntos, en tema de datos sensibles como datos biométricos, su uso está prohibido y solo es válido en ciertos casos. La Corte Constitucional dijo que el tratamiento de datos biométricos debe tener autorización judicial y la misma debe gozar del principio de proporcionalidad. Por tanto, se requiere una ley estatutaria. Se deben estructurar mis casos específicos en tema de tratamiento de datos sensibles, es importante armonizar ambos proyectos de ley para fortalecer el principio de legalidad.

La doctora Gabriela Lis manifiesta que Colombia con la Ley 1581 dio el primer paso importante en la protección de datos personales, pero actualmente requiere una actualización, es una necesidad jurídica. de esta forma, hay una importancia de la ampliación de bases sociales para la protección de datos, se debe contar con múltiples bases legales de protección en virtud de las realidades sociales y tecnológicas actuales. Se previene el fraude por ejemplo, ese es un interés legítimo por medio del cual se hace necesaria la protección de datos. Está reforma permitirá que Colombia se alinee con los estándares internacionales en la protección de datos personales.

Andrés Orlando Peña Andrade, asesor de la Procuraduría delegada en Derechos Humanos. Profundizó en cómo la extraterritorialidad extiende la responsabilidad a entidades que incluso traten datos de nacionales en otro territorio extranjero y permiten garantizar el control efectivo y el derecho de hábeas data. El Ministerio público en cabeza de la procuraduría de protección de datos es fundamental para velar por los derechos humanos de los ciudadanos. En tema de datos post mortem, las redes sociales implican intereses patrimoniales y cuestiona cómo se tratará la protección de esos datos personales.

Adolfo Enrique Gómez practicante en protección de datos y *habeas data* en el país. Observaciones

a los proyectos de ley, excluye algunas bases de datos, pero a la vez le hace extensible a las mismas derechos y obligaciones, lo que genera ambigüedad. En tema de lavado de activos y terrorismo menciona más control respecto de la ley de protección de datos. Considera relevante la inclusión de principios de límite de plazo, que con criterios de temporalidad se establezca la certeza de los datos. Considera importante y fundamental la inclusión del oficial de protección de datos, su uso es relevante en entidades públicas. Celebra la divulgación al derecho de la portabilidad, así como el derecho al olvido, importante que la iniciativa legislativa pueda tener un régimen de transición.

Diego Casas Correal, representante Cámara Comercio de Tunja, manifiesta preocupación en la aplicación extraterritorial porque genera efectos negativos y de impacto en el ecosistema digital. Indica que existe el riesgo de generar inseguridad jurídica.

Manuel Santiago Casas quien es representante de la Cámara de Comercio de Tunja. Menciona los nuevos retos de recolección masiva donde juega un papel fundamental el valor de los proyectos de ley, ampliación de nuevas categorías en el tratamiento de datos y recomendaciones pedagógicas para que llegue a la práctica cotidiana por medio de exigencia de programas de acción ciudadana y empresarial en protección de datos. Sugiere convenios con las distintas instituciones involucradas en el proceso de *habeas data*. La protección de datos es un pilar de la democracia digital, la transparencia y el trabajo empresarial conjunto.

Miguel Ángel Álvarez Pérez ponente de la Fundación pro género y justicia, resalta la importancia de las identidades diversas, así mismo, insistir en el reconocimiento del tratamiento y protección de datos en proyectos de ley ya que actualmente las minorías han sido marginadas y desprovistas de los espacios políticos, es así como en la implementación y ejecución del proyecto de ley haya un enfoque diferencial.

Sandra Ortiz representante de la Universidad Externado de Colombia, sugiere que se pueda precisar en el marco de supervisión de la vigilancia de datos ya que puede existir burocracia y demoras en los trámites, falta de competencia para tener conocimiento de estos conflictos. Es pertinente un régimen más robusto tanto para el sector público como privado y generar medidas correctivas en entidades públicas. En la ley de datos es necesario hacer sensibilización con las Pymes donde prevalezcan estándares mínimos en intervención humana e inteligencia artificial. De igual manera, tener presente el tratamiento de datos para menores de edad. Es un avance significativo respecto a actualización de la legislación de protección de datos.

Estella Vanegas, ponente de ADAPRI (Asociación Colombiana de Datos y Privacidad). Advierte la necesidad de actualizar la legislación de protección de datos, la mejora de cultura y oficial de protección de datos en cuanto a las herramientas de los dos proyectos que se implementan, no son adecuadas. Para MiPYMES entrar de manera proporcional en tema de tratamiento de bases de datos, es un régimen de transitoriedad, adicional de las exigencias requeridas para las funciones con las cuales cuenta la empresa. En tema de menores de edad reconoce la participación de ellos en niveles virtuales y digitales, sin embargo, la regulación en materia de educación no es tan clara, por lo tanto, se requiere un cumplimiento evidenciable en la práctica. Es indispensable trabajar conjuntamente en este tema.

Germán López, representante de la Cámara Colombiana de Informática y Comunicaciones. La implementación del ámbito de aplicación en los proyectos de ley pueden ser riesgosos. En tema de IA la implementación de este control también puede ser peligroso. Existen temas de inseguridad jurídica, dificultades en los roles del ecosistema digital. Estarán enviando sus comentarios posteriormente, se tocará el tema de los principios que se buscan implementar en el proyecto de ley.

A partir de la presente audiencia pública se estima el mejor desarrollo del Proyecto de Ley número 274 de 2025 fundamentado en las intervenciones enriquecedoras para el mismo.

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, Expediente 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 sólo 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 qué 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 pérdidas 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 quanom* 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 a los establecido en la Guía para la Implementación del Principio de Responsabilidad Demostrada (a*ccountability*), 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 continuo 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 pérdida 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 número 1377 de 2013. Siendo la transferencia entendida como una "Cesión"[1] en *strictu 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.

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)

---

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%20tra nsferencias%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%20tra nsferencias%20internacionales.pdf

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 Dijín, la suplantación de identidad creció 409% en el 2020, debido a la pandemia del Covid-19 (Certicámara/ Dijin, 2020)[3]. Muchas de las víctimas de suplantación manifiestan no haber compartido sus datos personales con extraños, y en muchas ocasiones, sólo 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 expreso, 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 punendi*, que debe regirse por los principios de legalidad, tipicidad, debido proceso, proporcionalidad e independencia de la sanción penal. En esta nueva propuesta legislativa no sólo 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 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.

[3] Referenciado en: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-20 20-debido-a-la-pandemia-3151651

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, aún 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 éstos 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".

5. 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

6.1. 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.

6.2. 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 demostrada**, 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.

6.3. 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 [...]".

6.4. <u>Fundamento jurisprudencial:</u>

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 sólo 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 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 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 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 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 1° 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.

8. 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 sólo 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 modifica parcialmente la Ley 1581 de 2012 y se dictan otras disposiciones relativas al derecho fundamental a la protección de datos personales***, para que sea tramitado, y con el apoyo de las y los Congresistas sea discutido y aprobado.

MARÍA FERNANDA CARRASCAL ROJAS Representante a la Cámara por Bogotá	DUVALIER SÁNCHEZ ARANGO Senador de la República