**PROYECTO DE LEY**

**LEY ESTATUTARIA No. DEL**

**“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”**

**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:

1. Al Tratamiento de datos personales, registrados en cualquier base de datos o archivo, realizado por cualquier persona natural o jurídica, de carácter público o privado, o por cualquier otra entidad independientemente del Estado en que resida o tenga su domicilio, o del Estado donde se encuentren los datos personales o del o de los medios utilizados, siempre que el Tratamiento, parcial o totalmente:

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

b) esté relacionado con la oferta de bienes o servicios, a título oneroso o no, a Titulares ubicados en Colombia, o

c) esté relacionado con el control del comportamiento de los Titulares, si tal comportamiento tiene lugar en el Estado colombiano.

2. Cuando así lo disponga el derecho internacional público.

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

**Parágrafo.** Los Responsables y Encargados del Tratamiento de datos personales a gran escala 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 para la debida atención de los asuntos relacionados con el cumplimiento de la Ley 1581 de 2012.

**Artículo 3.** Adiciónese un Artículo 2A a la Ley 1581 de 2012, del siguiente tenor:

**Artículo 2A.** Las disposiciones contenidas en esta Ley no serán aplicables al Tratamiento de datos personales contenidos en bases de datos o archivos:

a) mantenidos en un ámbito exclusivamente personal o doméstico;

b) de información periodística y otros contenidos editoriales;

c) que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

d) que tengan como fin y contengan información de inteligencia y contrainteligencia;

e) que estén 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; y

f) que estén sometidos a reserva estadística conforme a la Ley 2335 de 2023, y por las leyes que la modifiquen o subroguen.

**Parágrafo 1.** Los principios, derechos y garantías sobre protección de datos personales establecidos en esta Ley serán aplicables a todas las bases de datos o archivos incluidas las indicadas en los literales c, d, e y f 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 las bases de datos o archivos exceptuados prevea principios, derechos o garantías 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 derechos y garantías establecidos en esta Ley solo podrán ser limitados mediante normas especiales en la medida en que ello sea necesario y proporcional para salvaguardar la seguridad pública, la defensa de la Nación, la protección de la salud pública y los derechos y libertades de terceros. Las limitaciones y restricciones deben ser reconocidas de manera expresa mediante una norma de rango legal, salvaguardando la integridad de los datos personales y restringiendo su uso estricto a los fines que persiga dicha norma, con el propósito de brindar certeza suficiente a los Titulares acerca de la naturaleza y los alcances del Tratamiento.

**Artículo 4.** Adiciónense los siguientes literales al Artículo 3 de la Ley 1581 de 2012:

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

(…)

h) **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 identificarla o verificar su identidad de manera única;

1. **Datos genéticos:** Datos personales de carácter sensible relativos a las características hereditarias o adquiridas de una persona natural, que proporcionan información única sobre aspectos de su fisiología, desarrollo biológico o estado de salud, y que han sido obtenidos, directa o indirectamente, mediante procedimientos científicos que permiten identificar dichas características;

j) **Tratamiento automatizado de datos personales:** Toda operación o conjunto de operaciones realizadas sobre datos personales mediante procesos tecnológicos o sistemas informáticos, sin intervención humana directa, cuyos objetivos son, entre otros, analizar, evaluar o clasificar información, o predecir eventos o tomar decisiones con base en datos personales;

k) **Elaboración de perfiles:** Tratamiento automatizado 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 con el fin de tomar decisiones sobre ella;

l) **Tratamiento de datos personales a gran escala:** Tratamiento, a través de medios tecnológicos, de gran cantidad de datos personales relativos a un elevado número de Titulares, que por su magnitud pueda entrañar riesgos para los derechos fundamentales;

m) **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

n) **Datos de investigación científica:** Datos generados o recopilados durante el desarrollo de un proyecto de investigación; los cuales se convierten en evidencia temprana del proceso de investigación y que sirven para validar, verificar, reproducir o certificar los resultados finales de dicha investigación y que sólo adquieren significado en el contexto de esta.

**Artículo 5.** Subróguese el literal e), y adiciónese el literal i) y un parágrafo al 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:** Los Responsables del Tratamiento deberán tomar las medidas apropiadas para proveer a los Titulares información suficiente sobre las actividades de Tratamiento al que son o serán sometidos sus datos personales, incluidas las finalidades específicas del Tratamiento, la forma en que se concretan los principios del Tratamiento y el listado de derechos y garantías de los Titulares, entre otra información relevante. La información deberá proveerse de manera proactiva o a solicitud del interesado y deberá ser accesible, estar disponible por diversos medios y presentarse de manera clara y sencilla.

(…)

**i) Principio de responsabilidad demostrada:** Los Responsables del Tratamiento de datos personales deben ser capaces de demostrar que han implementado medidas apropiadas, oportunas, eficaces y demostrables para dar cumplimiento a los principios y deberes previstos en la Ley 1581 de 2012 y en su reglamentación, en forma proporcional a la naturaleza jurídica del Responsable y, cuando aplique, a su tamaño empresarial; a la naturaleza de los datos personales objeto del Tratamiento; al tipo de Tratamiento realizado; y a los riesgos que dicho Tratamiento pueda representar para los derechos de los Titulares.

j) **Principio de equidad y no discriminación:** Los Responsables y Encargados del Tratamiento que realicen tratamiento automatizado de datos personales, entre otros, a través de sistemas de Inteligencia Artificial, deberán tomar medidas para garantizar que el diseño, entrenamiento y operación de los sistemas cuenta con medidas para prevenir, detectar y mitigar sesgos que generen discriminación directa o indirecta, garantizando un trato justo y no discriminatorio.

**Parágrafo.** En el Tratamiento de datos personales vinculados a actividades científicas, tecnológicas y de innovación deberán aplicarse de manera reforzada los principios de finalidad, transparencia y responsabilidad demostrada, con el fin de garantizar la integridad de los datos, la confianza en la investigación y la preservación de su valor científico.

**Artículo 6.** 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.**

El Tratamiento de datos personales de niños, niñas y adolescentes debe orientarse a la garantía de sus derechos fundamentales y deberá responder siempre al principio del interés superior del niño.

El Tratamiento de los datos personales de los niños y las niñas menores de catorce años, a falta de otra base que legitime su Tratamiento, sólo será lícito si consta la autorización del representante legal, con el alcance que determine el mismo.

El Tratamiento de los datos personales de los niños y niñas mayores de catorce años, a falta de otra base que legitime su Tratamiento, deberá fundarse en su autorización previa, libre, informada, específica para uno o varios fines, e inequívoca. Salvo que para el caso exista norma legal que exija la declaración de voluntad del representante legal para la celebración del acto o negocio jurídico, en cuyo contexto se solicita la autorización.

Cuando se realice Tratamiento de datos personales de menores de dieciocho años en entornos digitales a través de aplicaciones o plataformas vía Internet, el Responsable del Tratamiento tomará las medidas razonables para verificar que la autorización sea otorgada en los términos aquí previstos.

Es tarea del Estado y de las entidades educativas de todo tipo proveer información y capacitar a docentes, representantes legales y tutores sobre las ventajas del Tratamiento de información personal y también sobre los riesgos a los que se enfrentan niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales. Asimismo, el Estado y las entidades educativas deben divulgar información acerca del uso responsable y seguro de los datos personales, el derecho a la intimidad y la protección de la información personal. El Gobierno Nacional reglamentará la materia.

**Parágrafo 1.** Las disposiciones contenidas en el presente artículo no afectarán las disposiciones especiales referentes al establecimiento de edades mínimas para efectos civiles, penales, laborales u otros regímenes jurídicos, respecto de la validez y consecuencias de ciertos actos jurídicos.

**Parágrafo 2.** Está prohibida la elaboración de perfiles de menores de dieciocho años que facilite conductas que puedan perjudicar su desarrollo físico o mental, o que se realice con fines comerciales, como marketing directo o publicidad orientada al comportamiento.

**Artículo 7.** Subróguese el literal a) del Artículo 8 de la Ley 1581 de 2012 y adiciónense los siguientes literales a dicho Artículo:

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

a) Conocer, actualizar, rectificar y suprimir sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Estos derechos se podrán ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error o aquellos cuyo Tratamiento esté expresamente prohibido, no haya sido autorizado o no sea necesario; o cuando se haya cumplido el término de caducidad del dato o cuando sea necesario para proteger otros derechos fundamentales;

(…)

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 solicitar la reconsideración de la decisión y la intervención de un ser humano;

h) Oponerse al Tratamiento de sus datos personales o solicitar su limitación 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;

i) Solicitar y recibir una copia de sus datos personales en un formato estructurado y comúnmente utilizado que permita su transferencia a otro Responsable cuando la información se encuentre previamente en una base de datos estructurada y 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.

**Artículo 8.** 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) Sea necesario para el ejercicio de las funciones legales o constitucionales de las autoridades públicas, siempre que se realice en el marco de sus funciones, y según lo establecido en la Constitución y en la Ley;

b) Sea necesario para el cumplimiento de un deber constitucional o 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) Esté precedido de la autorización previa, libre, informada, específica para uno o varios fines, e inequívoca del Titular de los datos personales.

La autorización deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

**Artículo 9.** Adiciónese el literal f, al Artículo 10 de la Ley 1581 de 2012:

**Artículo 10. Casos en que no es necesaria la autorización.**La autorización del Titular no será necesaria cuando se trate de:

(…)

f) El Tratamiento legítimo de datos personales, realizado de conformidad con los literales a, b, c y d, del artículo 9, de la presente Ley.

**Artículo 10.** Subróguese el Artículo 16 de la Ley 1581 de 2012, el cual quedará así:

**Artículo 16. Requisito de procedibilidad***.* Para efectos de la garantía de su derecho fundamental al habeas data, en los términos definidos en el artículo 8 de la presente Ley, el Titular o causahabiente sólo podrá elevar queja o solicitud ante las Autoridades de Protección de Datos Personales una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

**Artículo 11.** Adiciónense los siguientes literales al Artículo 17 de la Ley 1581 de 2012:

**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:

(…)

p) 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;

q) Respetar los derechos de los Titulares consagrados en el artículo 8 de la presente Ley;

r) Realizar el Tratamiento de datos personales siempre que tenga una base legítima para ello, en los términos de la presente Ley, atendiendo a criterios de protección de datos personales por diseño y por defecto en dichos Tratamientos;

s) Respetar en sus actividades de Tratamiento de datos personales los principios contenidos en el artículo 4 de la presente Ley;

t) Realizar evaluaciones de impacto en protección de datos personales cuando realice Tratamiento de datos personales a gran escala o cuando en el desarrollo de una actividad que involucre el Tratamiento de datos personales, sea probable que exista un alto riesgo de afectación a los derechos de los Titulares;

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

v) Designar un oficial de protección de datos cuando realice Tratamiento de datos personales a gran escala;

w) Informar a los Titulares sobre los incidentes de seguridad en los que sus datos personales se hayan visto afectados;

x) Abstenerse de recolectar datos personales por medios indirectos, usando programas o técnicas computarizadas, incluyendo Inteligencia Artificial, que permitan inferirlos o deducirlos de otros datos, para cualquier fin.

**Artículo 12.** Adiciónense los siguientes literales al Artículo 18 de la Ley 1581 de 2012:

**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:

(…)

m) Respetar los derechos de los Titulares consagrados en el artículo 8 de la presente Ley;

n) Respetar en sus actividades de Tratamiento de datos personales los principios contenidos en el artículo 4 de la presente Ley;

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

p) Designar un oficial de protección de datos cuando se realice Tratamiento de datos personales a gran escala a nombre del Responsable;

q) Formalizar mediante un contrato de encargo o de transmisión la prestación de servicios de Tratamiento de datos personales con el Responsable.

**Artículo 13.** 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 Autoridad Nacional de 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, 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 14.** 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.

**Artículo 15.** Subróguese y adiciónense los siguientes literales 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 Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio 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;

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

p) 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.

q) Las demás que le sean asignadas por Ley.

**Artículo 16.** 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:

1. Velar por la observancia de los principios para el Tratamiento de Datos Personales establecidos en el artículo 4 de la presente Ley.
2. 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.
3. Promover la incorporación de buenas prácticas en materia de protección de datos personales en la gestión pública.
4. Iniciar investigaciones disciplinarias cuando identifique presuntas infracciones al régimen de protección de datos por parte de funcionarios públicos.
5. 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.
6. 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.
7. Coordinar con la Superintendencia de Industria y Comercio las actuaciones necesarias en casos donde se requiera una acción conjunta, sin perjuicio de las competencias sancionatorias de dicha entidad.
8. 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.
9. 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.
10. 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;
11. 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 17.** 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.

**Artículo 18.** 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 19.** 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 Autoridad Nacional de Protección de Datos Personales podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional hasta por el equivalente de 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 20.** Adiciónese un literal g, 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.

**Artículo 21.** 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 está permitida a países que proporcionen niveles adecuados de protección. Se entiende que un país ofrece un nivel adecuado de protección de datos personales cuando cumpla con 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 que la presente Ley exige a los sujetos obligados.

La transferencia internacional de datos personales a Estados que no ofrecen niveles adecuados de protección deberá ir acompañada de garantías adicionales que aseguren que se mantenga un nivel de protección similar al que exige la presente Ley y sus decretos reglamentarios.

Las garantías adicionales podrán ser aportadas de las siguientes formas: el Responsable podrá: solicitar declaración de conformidad ante la Autoridad Nacional de Protección de Datos Personales; adoptar normas corporativas vinculantes aprobadas por la Autoridad Nacional de Protección de Datos Personales cuando se trate de transferencias entre empresas de un grupo empresarial, independientemente de su ubicación geográfica; o emplear cláusulas contractuales modelo aprobadas por la Autoridad Nacional de Protección de Datos Personales. Para estos efectos, la Autoridad Nacional de Protección de Datos Personales queda facultada para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

**Parágrafo 1.** La transferencia internacional de datos personales a Estados que no ofrecen niveles adecuados de protección, y en la que no se brinden garantías adicionales, se podrá realizar solo excepcionalmente si la misma se adelanta de conformidad con las bases que legitiman el Tratamiento definidas en esta Ley.

**Parágrafo 2.** Las disposiciones contenidas en el presente artículo serán aplicables a toda actividad de Tratamiento incluyendo las referidas en el artículo 2 A de la presente Ley.

**Artículo 22. Vigencia y derogatorias**. La presente Ley rige a partir de su promulgación, modifica los artículos 2, 3, 4, 7, 8, 9, 10, 16, 17, 18, 19, 21, 23, 24 y 26 de la Ley 1581 de 2012 y deroga todas las disposiciones que le sean contrarias.

**Firmas:**

**DIANA MARCELA MORALES ROJAS**

Ministra de Comercio, Industria y Turismo

**YESENIA OLAYA REQUENE**

Ministra de Ciencia, Tecnología e Innovación

**EXPOSICIÓN DE MOTIVOS**

**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”**

# **Justificación general**

Después de 13 años de su expedición, la Ley Estatutaria 1581 de 2012, Ley General de Protección de Datos Personales, ha cumplido tres grandes propósitos. Logró definir, con un buen nivel de aceptación, las reglas generales para la garantía del derecho fundamental a la protección de datos personales. Estableció un sistema de vigilancia y control exitoso, principalmente en cabeza de la Superintendencia de Industria y Comercio, que ha ampliado y fortalecido la garantía administrativa de dicho derecho fundamental. Y ha cimentado una cultura de protección de datos personales en Colombia, tanto en el sector privado como en el sector público.

Para la elaboración de la Ley 1581 de 2012, el Congreso de la República de entonces se nutrió de varias fuentes. Tomó algunos conceptos de la prolífica jurisprudencia de la Corte Constitucional en materia de Habeas Data, replicó algunos elementos de su antecesora Ley 1266 de 2008, sobre Habeas Data Financiero, y siguió también, en parte, el modelo de la Ley Orgánica 15/1999 de Protección de Datos de España que, a su vez, transponía la Directiva Europea 95/46/CE, en materia de tratamiento automatizado de datos personales.

Desde la promulgación de la Ley 1581 de 2012, las actividades de tratamiento de datos personales, objeto principal de su regulación, han experimentado cambios sustanciales. Estos cambios han estado asociados a una transformación radical de la economía mundial y a un vertiginoso desarrollo tecnológico. Todo ello incluye, el fabuloso crecimiento de los modelos de negocio basados en datos, el aumento de flujos transfronterizos de datos, la deslocalización de la información, las dinámicas extraterritoriales de tratamiento de datos, la incorporación de sistemas de inteligencia artificial, la automatización en la toma de decisiones y la elaboración masiva de perfiles individuales, entre muchos otros. Estas nuevas circunstancias han traído grandes beneficios, pero también nuevos riesgos y desafíos para la libertad, la igualdad, la intimidad y la identidad de los seres humanos. Han provocado intensas reflexiones sobre la mejor manera de proteger los derechos fundamentales y de controlar los posibles abusos de los poderes emergentes asociados al tratamiento de los datos personales.

La reforma que ahora se propone busca actualizar el marco regulatorio actual, hacerle algunos ajustes, incluir nuevos principios, derechos y deberes, y precisar y fortalecer los mecanismos de control y de garantía del derecho fundamental a la protección de datos personales.

La actualización busca equilibrar las oportunidades tecnológicas con la protección efectiva de los derechos fundamentales, balancear nuevamente las relaciones entre el poder informático y la libertad personal, remediar algunos defectos congénitos de la Ley 1581 de 2012, permitir mejores condiciones para el flujo transfronterizo de datos personales y el crecimiento económico, y en general, afinar el sistema de garantías de la Ley.

Esta reforma no pretende crear un nuevo marco regulatorio. Tiene la intención de fortalecer y actualizar el existente a partir de las lecciones aprendidas y del reconocimiento de los mejores estándares en la materia. En algunos puntos, esta reforma se alinea con los mejores estándares internacionales como los contenidos en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y en la Ley General de Protección de Datos Personales de Brasil (LGPD). En otros puntos, la reforma es producto de los aprendizajes de la experiencia colombiana, de la prolija actividad de nuestra Corte Constitucional y de la experiencia de más de 10 años de la Autoridad de Protección de Datos Personales.

Enseguida se hará una breve justificación del contenido puntual de la reforma propuesta.

## *En cuanto al ámbito de aplicación*

El ámbito de aplicación de la Ley 1581 de 2012 debe ampliarse para adaptarse a las dinámicas actuales del entorno digital. Hoy en día, varias de las afectaciones que sufren los Titulares de los datos personales provienen de tratamiento de datos personales adelantado por empresas extranjeras sin presencia física en Colombia, lo que dificulta la supervisión efectiva y la garantía de los derechos.

Por ello, es necesario que la Ley no se limite a los Tratamientos realizados por empresas con presencia en territorio colombiano, sino que también abarque aquellos casos en los que se realiza Tratamiento de datos personales, parcial o totalmente, en el territorio colombiano o se traten datos personales de nacionales colombianos, sin importar el lugar donde se encuentre el Responsable del Tratamiento y sin importar el medio o los medios con los cuales se realiza el tratamiento, lo que incluye por ejemplo, la recolección o el análisis de los datos por medios directos o indirectos, o si la obtención de los datos personales y su enriquecimiento se logra a través de inferencias o de otros medios facilitados por las técnicas o los programas de computación.

Este enfoque ha sido adoptado por varias jurisdicciones. Tal es el caso de la Unión Europea con el RGPD, Brasil con la LGPD, así como países de la región como Ecuador, Perú, Chile y Uruguay, e incluso algunos estados de EE. UU., como California. Estas normas se aplican a empresas que ofrecen bienes o servicios a residentes del territorio donde efectivamente se adelanta el Tratamiento de los datos personales, aunque no tengan presencia física en ellos.

Para concretar esta idea, la reforma propuesta incorpora criterios claros para precisar el ámbito de aplicación de la Ley orientados a facilitar su eficacia frente a empresas que operan internacionalmente, domiciliadas o no en Colombia, pero que recolectan de forma directa o no datos personales en Colombia, o que por otros medios los detentan y enriquecen, por loque de alguna forma adelantan el Tratamiento de datos personales, parcial o totalmente, en Colombia, o respecto de personas domiciliadas o con residencia en Colombia.

Adicionalmente, y con el propósito de garantizar la eficacia de las normas en materia de protección de datos, el proyecto propone que estas empresas, cuando adelanten tratamiento de datos personales a gran escala, deberán habilitar un canal de contacto y designar, por escrito, un representante ante la Autoridad Nacional de Protección de Datos Personales. Este representante deberá estar habilitado con plenos poderes y tener la capacidad de gestionar y atender los asuntos relacionados con el cumplimiento de la Ley 1581 de 2012. A través de este canal de contacto, y de la designación de este representante, la Autoridad Nacional de Protección de Datos Personales podrá, entre otras, solicitar información, requerir colaboración, elevar requerimientos, efectuar notificaciones y comunicar decisiones.

## *En cuanto a las excepciones al ámbito de aplicación*

Todas las excepciones al ámbito de aplicación previstas en la Ley 1581 de 2012 se mantienen. Sin embargo, por técnica legislativa se propone separar en dos artículos las reglas generales que fijan el ámbito de aplicación de la Ley, de aquellas actividades de Tratamiento exceptuadas. Se introduce también una precisión puntual en materia de reserva estadística, en donde se cambia la referencia a la anterior ley de censos, Ley 79 de 1993, por la referencia a la Ley 2335 de 2023, que la subrogó y está actualmente vigente. Y finalmente, se extiende el deber de respetar los derechos y los principios establecidos en esta Ley, incluso cuando se adelanten actividades de Tratamiento consideradas excluidas, y se incorpora la ratio de la Corte Constitucional en materia de exclusiones, fijada en la Sentencia C-748 de 2011, bajo la idea de que el derecho fundamental a la protección de datos personales no puede quedar desprovisto de protección en el caso de las actividades excluidas y que, en todo caso, la legislación que se cree para regular de forma específica tales materias debe respetar el principio de proporcionalidad y el contenido mínimo del derecho fundamental al habeas data.

## *En cuanto a las definiciones*

El proyecto propone incluir algunas definiciones clave en el contexto de las tecnologías emergentes. La incorporación de estos conceptos no solo brindará mayor claridad interpretativa, sino que facilitará la adecuada aplicación de la Ley.

Entre las definiciones propuestas figura la de datos biométricos. Este término, a pesar de estar mencionado en la Ley vigente, no cuenta con una definición legal precisa. Esta omisión ha generado ambigüedades que han dificultado su interpretación y aplicación, especialmente al tratarse de datos sensibles que requieren una protección reforzada. Una definición clara es indispensable, considerando el alto componente técnico que estos datos implican y la necesidad de establecer límites y garantías frente a su uso.

También incluye una definición de datos genéticos, ligada a dos factores, uno ontológico, ligado a las características hereditarias únicas de las personas, su desarrollo biológico o estado de salud, y otro técnico, relacionado con la aplicación de procedimientos científicos para su extracción. La información genética por su relación con los datos de salud y por estar especialmente ligada al ámbito de lo privado, tiene un vínculo fuerte con el derecho a la intimidad personal y familiar, y ostenta el carácter de información sensible.

El proyecto también incluye una definición de Tratamiento automatizado de datos personales a partir de dos factores: primero, el ontológico, ligado al desarrollo de procesos o procedimientos tecnológicos sobre datos personales llevados a cabo sin intervención humana directa, y segundo, el funcional, que permite entre otras analizar la información, predecir eventos o escenarios, o tomar decisiones sobre las personas con base en datos personales. Esta definición será muy importante para la definición del alcance de los nuevos derechos aquí reconocidos, en especial, el derecho a no estar sometido a decisiones automatizadas que tengan como efecto la limitación de los derechos fundamentales, la discriminación o la generación de consecuencias adversas que lo afecten de manera significativa

En una línea similar, el proyecto incluye también una definición de elaboración de perfiles. Gran parte del Tratamiento actual de datos personales, en especial los que involucran sofisticados algoritmos de Inteligencia Artificial, implica procesos de perfilamiento que permiten segmentar, clasificar y evaluar a las personas, y que, en muchos casos, sirven de base para decisiones automatizadas. Esta definición permitirá precisar el alcance de los derechos y los deberes previstos en la ley, en especial, los que guardan relación con los riesgos de discriminación, de decisiones arbitrarias o de afectación a los derechos de los Titulares con ocasión de la elaboración de perfiles.

Asimismo, se propone incluir la definición de Tratamiento de datos personales a gran escala, con el fin de identificar a qué tipo de organizaciones o Tratamientos se aplican ciertas obligaciones reforzadas. Esto resulta especialmente relevante para el establecimiento posterior, por vía reglamentaria, de umbrales objetivos y razonables en la aplicación de medidas como las evaluaciones de impacto.

En línea con lo anterior, se propone introducir la definición de evaluaciones de impacto en protección de datos personales. Frente a Tratamientos de alto riesgo para los derechos y libertades de los Titulares, los análisis de riesgos tradicionales pueden resultar insuficientes. Por ello, se propone esta figura como un instrumento adecuado que, desde las etapas de diseño, desarrollo y operación del producto, servicio o proceso, permitan anticipar, identificar y mitigar riesgos a lo largo del ciclo de vida del dato. Estas evaluaciones se configuran como herramientas idóneas para materializar el principio de responsabilidad demostrada y la protección por diseño y por defecto.

Por último, se propone la inclusión de la definición de datos de investigación científica con el propósito de concretar los deberes relacionados con la protección de los datos personales en el contexto del desarrollo y la conclusión de proyectos de investigaciones científicas.

## *En cuanto a los principios del Tratamiento de datos personales*

El proyecto propone un ajuste al contenido del principio de transparencia con el fin de ampliar su contenido y de hacerlo concordante con su nombre. El nuevo entendimiento del principio de transparencia incluye el deber de los Responsables del Tratamiento de proveer a los Titulares y al público en general información suficiente y pertinente sobre las actividades de Tratamiento que realiza o realizará , la manera en que en estas actividades se aplican y concretan los principios del Tratamiento de datos personales, los derechos y las garantías de los Titulares y toda aquella información que se estime relevante en función y en el contexto específico de las actividades de Tratamiento. La propuesta retoma el deber de proveer información sobre los datos personales a su Titular, reconocido en la tipificación vigente del principio de transparencia, y lo amplía a proveer información sobre el ejercicio de los demás derechos de los Titulares.

Sobre este punto, se incluye la doble dimensión de la transparencia (activa o proactiva y pasiva o a solicitud del Titular) y se establece que la información a suministrar debe ser accesible, debe encontrarse disponible por diversos medios (análogos, digitales, audiovisuales, etc.) y debe presentarse de manera clara y sencilla con tal de que facilite la comprensión de un usuario promedio, según el contexto del Tratamiento a partir del tipo de datos personales, o del tipo de Titulares (niños y niñas, población de especial protección constitucional, personas en situación de discapacidad, etc.)

Asimismo, el proyecto propone incluir en el elenco de los principios de la Ley, el principio de responsabilidad demostrada. Si bien este principio fue incorporado al ordenamiento jurídico colombiano en el Decreto Reglamentario 1377 de 2013, y en la Ley 2157 de 2021, que reformó la Ley de Habeas Data Financiero, este proyecto busca incluirlo también en la Ley General de protección de datos personales. Con ello se persigue que las actuaciones de los Responsables y de los Encargados del Tratamiento de datos personales estén orientadas a su realización.

La responsabilidad demostrada exige adoptar un enfoque proactivo y preventivo en el Tratamiento de la información personal. De tal forma que no baste contar con documentos, políticas o procedimientos bien elaborados, sino que sea necesario materializarlos en la práctica, asegurar que las medidas implementadas para garantizar los derechos fundamentales y para cumplir con los principios y deberes de la Ley sean pertinentes, eficaces y sobre todo demostrables.

Finalmente, el proyecto incluye el principio de equidad y no discriminación con énfasis especial en el tratamiento automatizado de datos personales, entre otros, a través de sistemas de Inteligencia Artificial. Esto con el fin de que tanto Responsables, como Encargados, tomen medidas razonables para garantizar que en el diseño, entrenamiento y operación de sus sistemas de información se prevengan, detecten y mitiguen los sesgos que generen discriminación directa o indirecta, a partir del tratamiento de datos personales, con el fin de garantizar así un trato justo y no discriminatorio.

## *En cuanto al Tratamiento de datos de niños, niñas y adolescentes (NNA)*

La Ley 1581 de 2012 establece una prohibición general al Tratamiento de datos personales de NNA, salvo que se trate de datos de naturaleza pública. Esta prohibición general es desproporcionada y a pesar de que así fue establecido por la Corte Constitucional en la parte motiva de su Sentencia C-748 de 2011, sigue vigente.

En el contexto social contemporáneo, altamente digitalizado, resulta necesario cambiar esta regla y superar la habilitación del Tratamiento ligada a la autorización de quienes detentan la autoridad parental. El proyecto propone lograr un mejor equilibrio entre protección a la niñez y autonomía progresiva. Es innegable que los menores de 18 años interactúan activamente en espacios digitales, espacios que hoy son esenciales para el acceso a la educación, la salud, la comunicación, a la recreación y a otros servicios. Por tanto, es necesario ajustar el marco legal para permitir el Tratamiento de datos personales de niños, niñas y adolescentes bajo condiciones específicas y con salvaguardas reforzadas.

En tal sentido, el proyecto propone que los adolescentes a partir de los 14 años tengan libertad para otorgar consentimiento para el Tratamiento de sus datos personales, sin el concurso de sus padres o representantes. Y se propone mantener la regla según la cual, para el Tratamiento de datos personales de niños y niñas menores de 14 años, sí será indispensable la autorización de sus representantes legales. Esta diferenciación reconoce la evolución de las capacidades humanas, conforme a la doctrina de la autonomía progresiva, y busca garantizar un entorno de protección adaptado a cada etapa del desarrollo de los seres humanos.

Este enfoque se encuentra respaldado por instrumentos internacionales. El artículo 5 de la Convención sobre los Derechos del Niño reconoce expresamente la autonomía progresiva, entendida como la capacidad creciente de los NNA para tomar decisiones informadas a medida que adquieren madurez y competencias. UNICEF, en su documento “El derecho de los niños, niñas y adolescentes a ser oídos”, explica que dicha autonomía implica involucrarlos activamente en los procesos que les afectan, permitiéndoles transitar hacia la vida adulta con responsabilidad y conciencia.

Desde el punto de vista del desarrollo cognitivo, estudios clásicos como los de Jean Piaget y Bärbel Inhelder (1958) señalan que entre los 12 y 15 años las personas ingresan en la fase del pensamiento operacional formal, caracterizada por el desarrollo del razonamiento lógico, la comprensión de hipótesis y la capacidad para evaluar consecuencias. Estos hallazgos respaldan científicamente la distinción normativa en torno a la edad y la capacidad de los adolescentes para tomar decisiones informadas sobre su información personal.

El enfoque propuesto por este proyecto equilibra la protección reforzada que requieren los NNA con el reconocimiento de sus capacidades en desarrollo y propone una regulación más realista, adaptada y respetuosa de sus derechos en el entorno digital.

En este sentido, por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea (RGPD) permite a los Estados miembros de la Unión Europea fijar la edad de consentimiento entre los 13 y los 16 años, reconociendo que, al alcanzar la adolescencia, muchos menores ya tienen la capacidad para ejercer sus derechos de manera más autónoma.

En línea con esta aproximación, el RGPD establece que los menores merecen una protección específica, especialmente frente a Tratamientos de datos personales con fines de mercadotecnia, elaboración de perfiles y servicios ofrecidos directamente a ellos. En efecto, uno de los cambios más significativos en la relación entre la sociedad y la tecnología se evidencia en cómo esta impacta a los niños, niñas y adolescentes (NNA). Si bien este grupo poblacional se beneficia ampliamente de las tecnologías de la información y las comunicaciones, también enfrenta riesgos particulares que deben ser abordados con especial atención.

En línea con esta consideración, el proyecto propone establecer un deber específico en cabeza de las plataformas digitales y demás Responsables cuyos servicios supongan la recolección y el Tratamiento de datos personales de niños, niñas y adolescentes, de adoptar medidas razonables para verificar que la autorización se haya otorgado en los términos establecidos por la ley, ya sea directamente por el adolescente o por sus representantes legales.

El proyecto también mantiene los deberes en cabeza del Estado y de la sociedad, en especial, de las entidades educativas, de proveer información y capacitar a docentes, padres y tutores sobre las ventajas y los riesgos a los que se enfrentan niños y niñas en relación con las actividades de Tratamiento de datos personales.

Por último, el proyecto propone la prohibición de elaborar perfiles de menores de 18 años que faciliten conductas que puedan perjudicar su desarrollo físico o mental, o que se adelanten con fines comerciales, como marketing directo o publicidad orientada al comportamiento.

## *En cuanto a los derechos de los Titulares*

El proyecto propone la inclusión del derecho a suprimir los datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se suma a los derechos a conocer, actualizar y rectificar los datos personales ya reconocidos en el artículo 15 de la Constitución y reiterados en la Ley vigente. El derecho a suprimir (borrar o eliminar) los datos personales de un archivo o base de datos fue reconocido por la Corte Constitucional en las Sentencias T-414 de 1992 y SU-082 de 1995, en relación con el habeas data financiero, y posteriormente en relación con el habeas data general, en los casos de las Sentencias SU-458 de 2012 y T-987 de 2012, entre muchos otros.

Estos cuatro derechos, el núcleo básico del derecho fundamental al habeas data, se podrán ejercer frente a todo tipo de datos y, en especial, entre otros, frente a datos inexactos, incompletos, desactualizados o que induzcan a error, o cuyo Tratamiento esté expresamente prohibido, no haya sido autorizado o no sea necesario, o cuando se haya cumplido el término de caducidad del dato, o cuando sea indispensable para la protección de otros derechos fundamentales como el buen nombre, la intimidad, la igualdad, la libertad personal, el trabajo, la salud o la vivienda digna, entre otros. Este ajuste, en clave de derechos, reafirma la centralidad del poder del titular de controlar sus datos y de participar en su tratamiento. Refuerza su poder para hacer valer los principios y deberes consagrados en la Ley, y para proteger sus intereses y demás derechos fundamentales. En últimas, reivindica la función del "habeas data" como un "derecho medio" como una garantía de otros derechos fundamentales.

Por otra parte, este proyecto reconoce nuevos derechos ligados a la transformación tecnológica, especialmente a partir de la expansión de la Internet, el desarrollo de la inteligencia artificial y el uso de plataformas digitales. Las nuevas dinámicas de poder que estas tecnologías engendran, y la necesidad de reivindicar frente a ellas espacios de libertad, siguen siendo la justificación constitucional para el reconocimiento de nuevos derechos.

Entre los nuevos derechos que este proyecto reconoce está el de no ser objeto de decisiones basadas únicamente en el Tratamiento automatizado de datos personales, incluida la elaboración de perfiles, cuando estas decisiones limiten sus derechos fundamentales, tengan efectos discriminatorios o le afecten significativamente.

Las decisiones automatizadas, adoptadas sin intervención humana pueden afectar gravemente los derechos y libertades de las personas, al definir, por ejemplo, si alguien accede o no a un crédito, a un servicio o a un empleo, o si alguien es multado o sancionado. Esta forma de poder debe encontrar límites en el orden jurídico. El nuevo derecho que aquí se reconoce incluye la posibilidad del Titular de oponerse y cuestionar las decisiones producto de Tratamientos automatizados que limiten sus derechos fundamentales o lo afecten significativamente, y obliga a los Responsables que adelantan este tipo de Tratamientos a incluir la intervención humana efectiva. Esto supone el deber de los Responsables de disponer que una persona humana revise el caso cuando así lo solicite el Titular afectado, y que esta persona humana tenga competencias para evaluar el contexto, pueda pronunciarse sobre la lógica subyacente del sistema automatizado y, si hay mérito, pueda modificar o revertir decisiones injustas o desproporcionadas.

Asimismo, el proyecto reconoce los derechos de oposición y de limitación del Tratamiento. Estos derechos permitirán al Titular impedir o limitar el Tratamiento de sus datos personales cuando el Tratamiento sea ilícito, no esté de acuerdo con alguna de las modalidades de tratamiento no cobijadas por deber legal o contractual, los datos no sean necesarios para una o varias de las finalidades que motivaron su recolección, haya una afectación de derechos fundamentales, se adelante con fines de publicidad o marketing directo, o mientras se resuelve una reclamación o controversia sobre la legitimidad de su Tratamiento.

Por último, el proyecto propone reconocer el derecho a la portabilidad de los datos personales. Este derecho es una concreción técnica del derecho a mantener el control sobre la propia información. En un entorno digital caracterizado por la portabilidad de los servicios y la proliferación de proveedores esto permitirá que, a petición del interesado, los Titularas reciban sus datos en un formato estructurado, de uso común y lectura mecánica que facilite su transferencia. El reconocimiento de este derecho fomenta la competencia entre Responsables, empodera a los usuarios, y refuerza el control individual sobre la información personal. Este derecho permitiría, por ejemplo, materializar iniciativas concretas como la contenida en el artículo 89 de la Ley 2294 de 2023, sobre datos abiertos para la inclusión financiera.

## *En cuanto a las bases que legitiman el Tratamiento*

Uno de los aspectos trascendentales de esta propuesta legislativa es la ampliación de las bases legales que legitiman el Tratamiento de datos personales en Colombia. Esta precisión normativa responde a la necesidad de contar con un marco jurídico que, sin debilitar las garantías fundamentales de los Titulares, ofrezca las claridades que la Ley actual no provee.

Hasta ahora, en el marco de la Ley 1581 de 2012, la autorización del Titular ha sido el principal fundamento para legitimar el Tratamiento de datos personales, lo cual, aunque necesario, resulta insuficiente frente a la complejidad de los flujos necesarios de información personal, tanto en el caso de la interacción de las personas con el Estado, como en el caso de las interacciones sociales y comerciales entre particulares. La experiencia de la Unión Europea con el RGPD y de los otros países de la región que han actualizado recientemente su normativa (Brasil, Chile, Ecuador y Perú) muestra que es fundamental contar con bases que legitiman el Tratamiento distintas al consentimiento y hacerlas explícitas.

La reforma mantiene el consentimiento previo, informado y expreso como base legitimadora del Tratamiento, y suma otras hipótesis, relacionadas con la protección de los derechos fundamentales, el principio de legalidad y el deber de cumplir los contratos. De tal forma que en adelante no se requiera el consentimiento expreso del Titular, cuando el Tratamiento de la información personal sea necesario para el ejercicio de las funciones legales y constitucionales de las autoridades públicas, la celebración y la ejecución de los contratos, así como el cumplimiento de las obligaciones nacidas de la celebración de negocios jurídicos, el cumplimiento de otros deberes legales por parte del Responsable o Encargado, o cuando ello sea necesario para proteger la vida o la salud de una persona natural.

## *En cuanto a los deberes de los Responsables y Encargados del Tratamiento*

Este proyecto de ley propone introducir algunos ajustes en los deberes de los Responsables y Encargados del Tratamiento, con el fin de fortalecer la protección efectiva de los datos personales y armonizar el marco colombiano con los estándares internacionales.

* + 1. Nuevos deberes de los Responsables del Tratamiento

El proyecto de Ley propone incluir entre los deberes de los Responsables el de respetar los derechos de los Titulares, reconocidos en el artículo 8 de la Ley, y el de ajustar sus actividades de Tratamiento de datos personales a los principios del Tratamiento de datos personales, establecidos en el artículo 4, de la Ley. El establecimiento de estos deberes parece obvio, pero no está reconocido así en la Ley actualmente vigente. El proyecto subsana este vacío.

Asimismo, reconoce como deberes explícitos de los Responsables tomar medidas específicas y adecuadas con el fin de garantizar el derecho a la protección de datos personales de niños, niñas y adolescentes, en los términos previstos por el artículo 7, sobre todo, las relacionadas con la necesidad de obtener su consentimiento previo, libre y expreso después de los 14 años, o el de sus representantes legales, como por ejemplo, la implementación de medidas para la verificación de edad y para evitar la recolección de datos personales a partir de la apertura de cuentas o del registro de menores de 14 años. Asimismo, se incluye el deber explícito de abstenerse de incurrir en las prohibiciones previstas en el artículo 7 de la presente Ley orientadas también a garantizar el derecho a la protección de datos personales de niños, niñas y adolescentes.

Adicionalmente, este proyecto propone incluir entre los deberes de los Responsables el de asegurar que toda operación sobre datos personales esté amparada por una base legal válida, conforme a lo previsto en la Ley. Esta obligación exige no solo justificar el Tratamiento, sino además documentar y poder demostrar dicha justificación ante las autoridades de protección de datos personales o frente a los Titulares.

Asimismo, incorpora de manera expresa el deber de aplicar los principios de protección de datos personales desde el diseño y por defecto, lo que implica que la protección de datos personales debe integrarse en todas las fases de desarrollo de productos, servicios y operaciones tecnológicas, de forma preventiva y estructural. Este enfoque obliga a adoptar medidas técnicas y organizativas desde antes de que empiece el Tratamiento de los datos personales, de forma que solo se traten aquellos datos personales estrictamente necesarios para las finalidades legítimas y durante el tiempo necesario para ello.

En los casos en que se lleven a cabo Tratamientos a gran escala o que, por su naturaleza, generen un alto riesgo para los derechos y libertades de los Titulares, los Responsables deberán realizar evaluaciones de impacto en protección de datos personales. Estas evaluaciones deben identificar, valorar y mitigar los riesgos asociados, y forman parte del enfoque de gestión preventiva que exige el principio de responsabilidad demostrada.

Asimismo, se propone incluir los deberes de designar un oficial de protección de datos personales cuando se realicen Tratamientos de datos personales a gran escala, y de informar a los Titulares sobre incidentes de seguridad que puedan haber comprometido sus datos personales, de manera oportuna, transparente y comprensible, facilitando la adopción de medidas correctivas por parte de los afectados.

Finalmente, se incluye el deber de abstenerse de recolectar datos personales por medios indirectos, usando programas o técnicas computarizadas, incluyendo Inteligencia Artificial, que permitan inferir datos personales o deducirlos de otros datos, para cualquier fin. Este deber debe interpretarse de conformidad con el principio de libertad y con las bases que legitiman el tratamiento que este proyecto propone. De tal forma que es claro que el tratamiento indiscriminado de datos personales utilizando distintos programas o técnicas de computación está prohibido, en tanto riñe con el carácter y con el contenido de los derechos al habeas data y a la protección de datos personales como auténticos derechos fundamentales.

* + 1. Nuevos deberes de los Encargados del Tratamiento

El proyecto de Ley propone incluir también entre los deberes de los Encargados el de respetar los derechos de los Titulares, reconocidos en el artículo 8 de la Ley, y el de ajustar sus actividades de Tratamiento de datos personales a los principios del Tratamiento de datos personales, establecidos en el artículo 4, de la Ley. El establecimiento de estos deberes parece obvia, pero no está reconocida así en la Ley actualmente vigente. El proyecto subsana este vacío.

Además de estos deberes, el proyecto propone incluir como un deber específico el de observar los mandatos del principio de responsabilidad demostrada, lo que implica implementar medidas efectivas de cumplimiento y estar en capacidad de evidenciar su adecuada gestión frente al Responsable o ante las autoridades.

Asimismo, se propone que los Encargados, cuando realicen Tratamiento de datos personales a gran escala por cuenta del Responsable, deberán designar un oficial de protección de datos personales, con funciones análogas a las del Responsable, garantizando así corresponsabilidad en la cadena del Tratamiento.

Finalmente, se establece el deber de que toda relación entre Responsable y Encargado se formalice en un contrato de encargo o transmisión de datos personales, en el que se definan de manera clara las instrucciones, responsabilidades, medidas de seguridad y mecanismos de supervisión, de conformidad con los principios de legalidad, lealtad y transparencia.

## *En cuanto a las autoridades públicas con funciones relacionadas con la protección de datos personales*

La reforma busca robustecer la garantía del derecho al Tratamiento de datos personales. Para esto, fortalece el modelo dual propuesto por la Ley 1581 de 2012, que dividió las funciones de garantía administrativa del derecho a la protección de datos personales entre la Superintendencia de Industria y Comercio (SIC) y la Procuraduría General de la Nación (PGN). Asimismo, fortalece la coordinación y colaboración de estas entidades con el Ministerio de Ciencia, Tecnología e Innovación.

En esta dirección, el proyecto dispone que en el término de seis meses el Procurador General deberá habilitar, poner en funcionamiento o asignarle a una procuraduría delegada ya existente, las funciones que en materia de difusión y promoción y garantía del derecho fundamental a la protección de datos personales son propias de la Procuraduría General de la Nación y que este proyecto precisa.

La Procuraduría General de la Nación tendrá sobre todo funciones preventivas orientadas a asegurar el cumplimiento de los principios y deberes de la Ley 1581 de 2012 frente a las autoridades públicas. En efecto, el proyecto establece de forma específica algunas de las funciones de la Procuraduría en relación con la protección de datos personales, orientadas por el criterio de la vigilancia preventiva, el cumplimiento de la Constitución y la Ley, y la promoción y defensa de los derechos humanos, todo en consonancia con la misionalidad constitucional de la Procuraduría General de la Nación.

Asimismo, se reafirma la competencia de la Procuraduría General de la Nación para ejercer la acción disciplinaria en el caso en que los servidores públicos incumplan los deberes previstos en la Ley 1581 de 2012, competencia que no depende, ni dependerá, de una remisión previa de los casos por parte de la Delegatura para la protección de datos personales de la SIC.

Por otra parte, el proyecto reafirma el rol de la Delegatura para la protección de datos personales de la SIC como Autoridad Nacional de Protección de Datos Personales, y amplía sus funciones con una perspectiva estratégica. Entre las nuevas facultades propuestas se encuentran: a) desarrollar y promover diferentes instrumentos orientados al cumplimiento de la ley (códigos de conducta, guías sectoriales y mecanismos de certificación voluntaria), b) impulsar acciones de cooperación internacional con el fin de articular medidas de protección, c) garantizar el cumplimiento transfronterizo de los derechos de los Titulares, d) expedir órdenes administrativas de obligatorio cumplimiento y finalmente, y esto es importante destacarlo, la función de coordinar acciones con la Procuraduría Delegada con funciones para la Protección de Datos Personales orientadas al cumplimiento de los principios y deberes de la Ley, el intercambio de información, el traslado de pruebas y la realización de acciones de manera conjunta en pro de la garantía del derecho fundamental a la protección de datos personales y de asegurar el efectivo cumplimiento de la Ley.

Asimismo, el proyecto busca fortalecer su rol institucional como Autoridad Nacional de Protección de Datos Personales, al establecer que el nombramiento en el cargo de delegado para la protección de datos personales se efectuará previa convocatoria pública con valoración de los méritos de las y los candidatos. Asimismo, propone establecer que el ejercicio del cargo lo será para un periodo fijo de cuatro años, con el fin de asegurar continuidad y estabilidad en la gestión de la agenda de la Autoridad y en general de la política pública de protección de datos personales del Estado colombiano.

Esta propuesta persigue afianzar el rol de la Autoridad Nacional de Protección de Datos Personales como una auténtica garantía administrativa del derecho fundamental a la protección de datos personales, cuyo titular tendrá un periodo fijo que le permita actuar con autonomía e independencia. Una garantía administrativa con estas características de independencia y autonomía facilita la realización de transferencias internacionales de datos personales entre el Estado colombiano y otros Estados, y entre empresas colombianas y extranjeras, y mejora las condiciones para la celebración de negocios y la concreción de acuerdos internacionales. Adicionalmente, este ajuste puntual sobre nombramiento y permanencia del titular de la Autoridad Nacional de Protección de Datos allanaría el camino para lograr una decisión de adecuación por parte de la Comisión Europea, lo cual, estiman algunos expertos, abriría la posibilidad de incrementar los negocios con la Comunidad Europea entre un 6 y un 14%[[1]](#footnote-1).

Por último, el proyecto de ley refuerza la coordinación y cooperación interinstitucional entre las autoridades de protección de datos personales y el Ministerio de Ciencia, Tecnología e Innovación. Esta coordinación materializa el principio constitucional de colaboración armónica entre los diferentes órganos y entidades del Estado, de conformidad con el artículo 113 de la Constitución Política de 1991. El proyecto propone que el Ministerio de Ciencia, Tecnología e Innovación tenga un rol protagónico en la formulación de conceptos, la creación de guías y la expedición de lineamientos sobre el Tratamiento de datos personales relacionados con información científica, tecnológica o de innovación. Esto con el propósito de que, mediando una adecuada coordinación entre las entidades, se fortalezca la confianza en la administración pública y se cree un entorno propicio para la innovación tecnológica y la investigación científica, basado en la adecuada protección de datos personales.

## *En cuanto a las sanciones y los criterios para graduar las sanciones*

El proyecto propone incrementar el tope máximo de las sanciones económicas, pasando de dos mil (2.000) a diez mil (10.000) salarios mínimos legales mensuales vigentes (SMLMV) al momento de su imposición. Adicionalmente, se incorpora un criterio alternativo o complementario para la imposición de sanciones, permitiendo fijarlas en función del cinco por ciento (5%) de los ingresos operacionales del infractor en el año fiscal inmediatamente anterior al de la imposición de la sanción.

Este enfoque busca evitar que las multas resulten ineficaces o irrelevantes en relación con la capacidad económica de grandes actores, en especial aquellos del ecosistema digital que operan a gran escala o transnacionalmente. Al mismo tiempo, se promueve la proporcionalidad al vincular la sanción con la dimensión económica del infractor.

También se incluyen algunos ajustes en el parágrafo. En especial, respecto de la expresión que indica que las sanciones consagradas en la ley: "sólo aplican para las personas de naturaleza privada." para incluir la expresión "así como a las sociedades de economía mixta y las empresas industriales y comerciales del estado", por cuanto, tal como se encuentra redactada, resulta incompatible con el principio de igualdad consagrado en el artículo 13 de la Constitución. En efecto, la norma citada podría ajustarse en virtud del principio de igualdad, toda vez que en el modelo del Estado Social de Derecho, con una economía abierta, las personas de naturaleza pública denominadas sociedades de economía mixta y las empresas del Estado que desarrollan actividades comerciales e industriales actúan en las mismas condiciones de mercado que las entidades privadas.

Asimismo, se incorpora una causal de atenuación como criterio adicional para la graduación de las sanciones: la implementación efectiva de las medidas derivadas del principio de responsabilidad demostrada. En este sentido, se instruye a la Autoridad para que valore como atenuante de las sanciones, cuando para ello haya mérito, la existencia de políticas, controles, medidas técnicas y organizativas orientadas a prevenir daños, siempre que hayan sido desplegadas con antelación al incumplimiento del deber, y de forma diligente y verificable.

Con estos ajustes, se busca transitar hacia un modelo sancionatorio más justo, disuasivo y equilibrado, que combine el castigo de conductas lesivas con el reconocimiento de prácticas responsables y preventivas, en línea con estándares internacionales.

## *En cuanto a las Transferencias Internacionales de Datos Personales*

Uno de los aspectos clave para consolidar un entorno digital confiable y fomentar los negocios en la economía global es contar con reglas claras y coherentes sobre las transferencias internacionales de datos personales. En un contexto marcado por el uso masivo de servicios digitales, computación en la nube, plataformas transfronterizas e infraestructura tecnológica distribuida, el flujo constante de datos personales entre diferentes jurisdicciones es cotidiano e intensivo.

Este escenario exige garantizar que los Titulares de los datos personales no pierdan sus derechos ni la capacidad de ejercerlos, incluso cuando su información sea transferida a otro Estado. La protección de datos personales debe seguir al dato, sin importar su localización geográfica, y mantenerse consistente con el estándar ofrecido en el Estado de origen.

En consecuencia, la reforma establece que las transferencias internacionales de datos personales no deben ser entendidas como una práctica prohibida, sino como una realidad inherente a la globalización económica y tecnológica, que debe ser regulada de forma responsable. El objetivo es que tales transferencias solo puedan realizarse a países que ofrezcan un nivel adecuado de protección, comparable al previsto en la legislación colombiana, de conformidad con un mecanismo de reconocimiento que podrá ser definido por la Autoridad Nacional de Protección de Datos Personales.

Cuando se trate de transferencias hacia países que no cuenten con un nivel adecuado, se permitirán únicamente si se implementan mecanismos complementarios de protección, como cláusulas contractuales modelo, normas corporativas vinculantes, códigos de conducta aprobados, certificaciones reconocidas, o medidas técnicas y organizativas adicionales que garanticen la seguridad y legalidad del Tratamiento.

Este enfoque permite un equilibrio entre la necesidad de habilitar flujos de datos internacionales y la obligación de proteger los derechos fundamentales de los Titulares, posicionando a Colombia como un país confiable para la inversión, el comercio y la innovación tecnológica, sin debilitar su marco de garantías.

# **Conclusiones**

El presente proyecto de ley propone una serie de reformas puntuales y a la vez estratégicas a la Ley 1581 de 2012 en materia de protección de datos personales. Lejos de constituir un simple ajuste técnico, esta propuesta responde a una transformación profunda del entorno social, económico y tecnológico del país y del mundo, en el que el Tratamiento intensivo, automatizado y transfronterizo de datos personales plantea nuevos riesgos, pero también abre oportunidades sin precedentes.

Desde el punto de vista jurídico esta reforma actualiza y fortalece el marco normativo contenido en la Ley 1581 de 2012, sin sustituirlo. Extiende y precisa el ámbito de aplicación de ley, para incluir a empresas transnacionales que tratan datos personales en Colombia pero que no están domiciliadas en Colombia, reconoce principios como la responsabilidad demostrada, incorpora nuevos derechos como el de revisar y exigir intervención humana frente a decisiones automatizadas adversas, introduce nuevas figuras como las evaluaciones de impacto, nuevas definiciones como la de datos biométricos y elaboración de perfiles, establece nuevas bases legales para el Tratamiento y robustece la capacidad institucional de las autoridades de protección de datos personales. Con estas propuestas el proyecto responde al llamado de garantizar la efectividad de los derechos fundamentales al habeas data, a la protección de datos personales, a la intimidad, a la igualdad, a la identidad y a la libertad, en los desafiantes y cambiantes entornos de las transformaciones tecnológicas.

Desde el punto de vista social y de derechos fundamentales, la propuesta tiene una orientación clara hacia la protección efectiva de las personas naturales. Amplía la gama de derechos de los Titulares, incorpora enfoques diferenciados para poblaciones vulnerables como niños, niñas y adolescentes, establece mecanismos concretos para prevenir daños, y asegura que todas las personas tengan herramientas para mantener el control sobre sus datos y para incidir en la forma en se adelanta su Tratamiento, incluso en los entornos complejos del ecosistema internet, las decisiones automatizadas y el despliegue de nuevas tecnologías.

Desde la dimensión económica y de política pública, esta iniciativa apunta a un entorno normativo coherente con los estándares internacionales, que proporcione seguridad jurídica a la industria, a los inversionistas y a los emprendedores digitales. Una regulación clara y garantista que genere confianza a todos los actores, permita la circulación transfronteriza de datos personales con Estados que exigen niveles adecuados de protección, y mejore la reputación internacional de Colombia como destino seguro para el desarrollo de negocios tecnológicos y digitales..

Además, otorga nuevas herramientas a las autoridades de protección de datos personales. En el contexto de nuestro régimen híbrido de supervisión, el proyecto fortalece la garantía del derecho a la protección de datos personales, el cumplimiento de los principios y deberes de la Ley 1581 de 2012, y el ejercicio de las funciones diferenciadas de prevención y sanción, y de inspección, vigilancia y control, en cabeza tanto de la Procuraduría General de la Nación como de la Superintendencia de Industria y Comercio.

Este proyecto de ley se enmarca en una visión de Estado centrada en las personas, que reconoce que el Tratamiento de datos personales es un elemento estructural de la vida social y económica contemporánea. Un proyecto de ley que protege sin frenar, que habilita sin relativizar derechos, y que posiciona a Colombia en el grupo de Estados que entienden que tanto el Estado digital, como la economía digital, solo son legítimos si están fundados en la confianza, la transparencia, la legalidad y el respeto por la dignidad humana.

**Firmas:**

**DIANA MARCELA MORALES ROJAS**

Ministra de Comercio, Industria y Turismo

**YESENIA OLAYA REQUENE**

Ministra de Ciencia, Tecnología e Innovación

1. Ferracane et al. Digital Trade, Data Protection and EU Adequacy Decisions. CITP Working Paper 6 (11 octubre 2023) (Publicado en Inglés) Disponible en: https://citp.ac.uk/wp-content/uploads/Ferracane-et-al-Adequacy-paper\_Oct2023\_CITP\_WP6.pdf Ferracane y otros. *Los efectos en el comercio de las decisiones de adecuación de la Unión Europea.* (3 de julio de 2023) (Publicado en inglés) Disponible en: <https://cepr.org/voxeu/columns/trade-effects-eu-adequacy-decisions> [↑](#footnote-ref-1)