REPÚBLICA DE COLOMBIA

GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA
www.imprenta.gov.co

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

AÑO XXXIII - Nº 1157 | Bogotá, D. C., jueves, 15 de agosto de 2024 | EDICIÓN DE 60 PÁGINAS

DIRECTORES: GREGORIO ELJACH PACHECO
SECRETARIO GENERAL DEL SENADO
www.secretariasenado.gov.co

JAIME LUIS LACOUTURE PEÑALOZA
SECRETARIO GENERAL DE LA CÁMARA
www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

CÁMARA DE REPRESENTANTES

PROYECTOS DE LEY ESTATUTARIA

Bogotá, D. C., 6 de agosto de 2024

Representante

JAIME RAÚL SALAMANCA

Cámara de Representantes

Secretario General

JAIME LUIS LACOUTURE PEÑALOZA

Cámara de Representantes

Referencia: **Radicación Proyecto de Ley Estatutaria número 152 de 2024 Cámara,** *por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales.*

Respetado Señor Presidente y Secretario,

En nuestra condición de miembros del Congreso de la República y en uso del derecho consagrado en la Constitución Política de Colombia y en la Ley 5ª de 1992, nos permitimos poner a consideración de la honorable Cámara de Representantes el siguiente proyecto de ley estatutaria: *"por la cual se dictan disposiciones para el Régimen General de 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,

ANA CAROLINA ESPITIA JEREZ
Senadora de la República

MARÍA DEL MAR PIZARRO GARCÍA
Representante a la Cámara por Bogotá
Partido Colombia Humana

SANTIAGO OSORIO MARIN
Representante a la Cámara
Coalición Alianza Verde - Pacto Histórico

ALEJANDRO GARCÍA RÍOS
Representante a la Cámara por Risaralda
Partido Alianza Verde

JHON FREDI VALENCIA CAICEDO
Representante a la Cámara
Citrep No. 11 Ptyo

CRISTÓBAL CAICEDO ANGULO
Representante a la Cámara por Valle del Cauca
- Pacto Histórico

HÉCTOR DAVID CHAPARRO
Representante a la Cámara
Partido Liberal

CRISTIAN DANILO AVENDAÑO FINO
Representante a la Cámara por Santander
Partido Alianza Verde

PABLO CATATUMBO TORRES VICTORIA
Senador de la República

MARÍA FERNANDA CARRASCAL ROJAS
Representante a la Cámara por Bogotá

DUVALIER SÁNCHEZ ARANGO
Representante a la Cámara por Valle del Cauca -
Alianza Verde

LUIS DAVID SUAREZ CHADID
Representante a la Cámara por Sucre
Partido Conservador

JUAN CAMILO LONDOÑO BARRERA
Representante a la Cámara por Antioquia
Partido Alianza Verde

PROYECTO DE LEY ESTATUTARIA
NÚMERO 152 DE 2024 CÁMARA

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

El Congreso de la República,

DECRETA:

TÍTULO I

DISPOSICIONES GENERALES

CAPÍTULO I

Objeto, ámbito de aplicación y definiciones

Artículo 1°. ***Objeto***.

La presente ley establece las normas relativas a la protección de las personas naturales en lo que respecta a la protección y tratamiento de sus datos personales y las normas relativas a la libre circulación de tales datos.

De igual manera, la presente ley protege los derechos y garantías fundamentales de las personas naturales y, en particular, su derecho fundamental a la protección de los datos personales, en los términos descritos en el artículo 15 de la Constitución Política.

Artículo 2°. ***Ámbito de la aplicación material.***

1. La presente ley se aplica al tratamiento de los datos personales.
2. El régimen de protección de

datos personales establecido en la presente ley no será de aplicación:

a) A los tratamientos efectuados por una persona natural en un ámbito exclusivamente personal o doméstico.

b) A los tratamientos realizados por parte de las autoridades competentes con fines de prevención, investigación, detección, o procesamiento judicial de actos delictivos incluido el lavado de activos y el financiamiento del terrorismo, la ejecución de sanciones penales, así como la de protección frente a amenazas a la seguridad y defensa nacional y su prevención.

c) A los tratamientos que tengan como finalidad cumplir con la actividad periodística y otros contenidos editoriales.

d) A los tratamientos que tengan como fin y contengan información de inteligencia y contrainteligencia.

e) A los tratamientos realizados en virtud de la Ley 1266 de 2008

Parágrafo primero. 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.

Parágrafo segundo. El Gobierno nacional, reglamentará sobre el tratamiento de datos personales tratados para fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos, la financiación del terrorismo y la ejecución de sanciones penales.

Parágrafo tercero. Los principios sobre protección de datos serán aplicables a todos los tratamientos de datos personales, incluidos los exceptuados en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal.

En el evento que la normatividad especial regule los tratamientos de datos personales exceptuados prevea principios que tengan en consideración la naturaleza especial de los datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

Artículo 3°. ***Ámbito territorial.***

1. La presente ley se aplica al tratamiento de datos personales en el contexto de las actividades de los responsables o del encargado con domicilio y/o residencia en territorio nacional, independientemente de que el tratamiento tenga lugar o no en Colombia.
2. La presente ley se aplica al tratamiento de datos personales de titulares que residan en territorio nacional por parte de un responsable o encargado no establecido en Colombia, cuando las actividades de tratamiento estén relacionadas con:

a) La oferta de bienes o servicios a dichos titulares con residencia en Colombia, independientemente de si estos son de carácter oneroso o no.

b) El control del comportamiento, en la medida en que este tenga lugar en Colombia.

3. Por un responsable o encargado que no esté establecido en Colombia, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud del derecho internacional público.

Artículo 4°. ***Definiciones***. A efectos de la presente ley se entenderá por:

1. “Anonimizarían”: procedimiento técnico que modifica de manera irreversible los datos personales con el fin que no pueda atribuirse a un titular;
2. “Autoridad de protección de datos”: entidad pública que tiene como objetivo principal inspeccionar, vigilar y controlar la aplicación del Régimen General de Protección de Datos establecido en esta ley y las demás disposiciones que la desarrollen, modifiquen, adicionen o complementen, garantizando la protección de los derechos de los titulares y el efectivo cumplimiento de los deberes de quienes intervengan en el tratamiento de los datos personales.
3. “Base de datos”: todo conjunto de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado.
4. “Bloqueo de datos”: medidas técnicas y organizativas adoptadas por parte del responsable o encargado del tratamiento, que permitan la identificación y reserva de los datos para impedir y/o evitar su tratamiento.

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

21. “Servicio de la sociedad de la información”: para efectos de la presente ley se entenderá como todo servicio prestado por solicitud de un consumidor de servicios, a través de equipos electrónicos y/o tecnologías que facilitan la creación, distribución y manipulación de la información, sin que las partes estén presentes simultáneamente.
22. “Seudonimización”: tratamiento de datos personales que ya no puedan atribuirse a un titular sin utilizar información adicional. Dicha información debe figurar por separado, estar sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.
23. “Titular”: persona natural cuyos datos personales son objeto de Tratamiento.
24. “Transferencia internacional de datos personales”: tratamiento que supone un flujo de datos, en el que un responsable y/o encargado del tratamiento ubicado en el territorio nacional, envía y/o habilita accesos a datos personales a destinatarios y/o encargados que se encuentran están fuera del territorio nacional.
25. “Tratamiento”: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como pueden ser, la recogida, registro, organización, estructuración, conservación, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
26. “Tratamiento a gran escala: es aquel que afecta a una gran cantidad de datos que se refieren a un elevado número de titulares y que entraña un alto riesgo. Su valoración dependerá de la proporción de la población correspondiente, el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento, el alcance geográfico y la duración o permanencia del tratamiento.

CAPÍTULO II

Principios y condiciones relativas a la protección de datos

Artículo 5°. *Principios relativos al tratamiento*.

1. El tratamiento de datos personales debe darse en virtud de los siguientes principios:

a) “Principio de Legalidad”: el tratamiento de los datos personales debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.

b) “Principio de lealtad”: las finalidades con la que se recolectan datos personales encontrarán sus límites en la presente ley y no podrán obtenerse por vías fraudulentas, engañosas, ni por acciones que puedan calificarse como dolosas.

c) “Principio de transparencia”: exige que la Información facilitada a los titulares sea concisa, accesible e inteligible, utilizando un lenguaje claro y sencillo.

d) “Principio de limitación de la finalidad”: los datos deben ser recogidos con fines determinados, explícitos y legítimos, y serán tratados ulteriormente de manera incompatible con dichos fines; el tratamiento ulterior de los datos personales con fines de archivo en interés público, investigación científica, histórica o estadística no se considerará incompatible con los fines iniciales.

e) “Principio de minimización de datos”: sólo se deben recabar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

f) “Principio de exactitud”: los datos de carácter personal deberán ser exactos de tal forma que respondan con veracidad a la situación actual del titular. Si fuera necesario, actualizados; se adoptarán todas las medidas razonables para rectificar o suprimir, sin demora injustificada, los factores que introducen las inexactitudes en los datos personales con respecto a los fines para los que se tratan. Los datos facilitados directamente por el titular se considerarán exactos.

g) “Principio de limitación del plazo de conservación”: los datos deben ser mantenidos de forma que se permita la identificación de los titulares durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se trate exclusivamente en cumplimiento de un deber legal o contractual, atendiendo a las disposiciones aplicables a los aspectos administrativos, contables, fiscales, jurídicos, con fines de archivo en interés público, investigación científica, histórica o estadística, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente ley a fin de proteger los derechos y garantías de los titulares.

h) “Principio de integridad”: consiste en implantar las medidas de seguridad técnicas y organizativas que garantice que el dato no sea alterado de manera no autorizada. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

i) “Principio de confidencialidad”: los responsables y encargados del tratamiento

de datos, así como todas las personas que intervengan en cualquier fase del tratamiento, tendrán el deber de garantizar que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. El responsable y/o encargado del tratamiento están obligados a garantizar la reserva de la información, inclusive después de finalizado el tratamiento.

El principio señalado será complementario de los deberes de secreto profesional de conformidad con su normativa aplicable.

j) "Principio de seguridad": los sujetos que participen en cualquier etapa del tratamiento deberán realizar análisis de riesgos, orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten, con el fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

k) "Principio de proporcionalidad": durante el ciclo de vida de los datos, el responsable velará porque el tratamiento sea idóneo respecto a los fines; necesario en cuanto no existan otras medidas para conseguir el fin perseguido; y equilibrado respecto al beneficio que dicho tratamiento proporciona y su impacto sobre los derechos y garantías fundamentales de los titulares.

l) "Principio de explicabilidad": los responsables del tratamiento deben ser capaces de explicar de manera clara y comprensible a los titulares cómo se están utilizando sus datos personales y cómo se toman las decisiones en función de ellos. Los encargados del tratamiento asistirán al responsable en el cumplimiento de esta obligación.

m) "Principio de responsabilidad demostrada" "accountability": El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en la presente ley, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de protección de datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

Artículo 6°. ***Bases que legitiman el tratamiento.***

1. El tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones:

a) El titular dio su consentimiento previo para el tratamiento de sus datos personales para uno o varios fines específicos.

b) El tratamiento es necesario para la ejecución de un contrato en el que el titular es parte o para la aplicación de medidas precontractuales solicitadas por el titular.

c) El tratamiento es necesario para el cumplimiento de un deber legal aplicable al responsable del tratamiento.

d) El tratamiento es necesario en casos de urgencia médica o sanitaria del titular o de otra persona natural.

e) El tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable del tratamiento por la Constitución y la ley.

f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan sobre los intereses, derechos y garantías fundamentales del titular que requieran la protección de datos personales. Es fundamental que exista una relación relevante entre el titular y el responsable, en particular cuando el titular sea un menor de edad. Se debe realizar un examen de ponderación que garantice que el tratamiento sea lícito, necesario y equilibrado en relación con los derechos del titular.

Lo dispuesto en este literal no será aplicable al tratamiento realizado por entidades públicas en el ejercicio de sus funciones.

2. Cuando la base jurídica que legitima el tratamiento sea el cumplimiento de un deber legal o el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas la finalidad de este debe estar fundamentada en normativa con rango de ley vigente.

Parágrafo primero. La normativa vigente a la que se refiere el numeral 2 del presente artículo podrá contener disposiciones específicas para adaptar la aplicación de la presente ley, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los titulares afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo. La normativa vigente cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

Parágrafo segundo. Las normativas expedidas con posterioridad a la presente ley podrán introducir disposiciones que cumplan con los criterios establecidos en el presente Régimen General de Protección de Datos con respecto al tratamiento, en cumplimiento del numeral 1, literal c) y e), fijando de

manera precisa requisitos específicos de tratamiento y otras medidas de conformidad con la presente ley.

Artículo 7°. ***Tratamientos con finalidades diferentes a las iniciales***.

Cuando se quiera tratar los datos personales para una finalidad diferente a la que fueron recogidos, y ese nuevo tratamiento no esté basado en el consentimiento del titular o en una norma específica que sea necesaria y proporcional en una sociedad democrática, el responsable del tratamiento deberá considerar si el nuevo tratamiento es compatible con la finalidad original. Para ello, tomará en cuenta lo siguiente:

a) La relación entre la finalidad original y la nueva finalidad de tratamiento de los datos personales.

b) El contexto en que se recogieron los datos personales, especialmente la relación entre los titulares y el responsable del tratamiento.

c) La naturaleza de los datos personales, especialmente si son datos sensibles o relacionados con antecedentes penales, anotaciones judiciales o contravencionales.

d) Las posibles consecuencias para los titulares por el nuevo tratamiento de sus datos.

e) La existencia de garantías adecuadas, como el cifrado o la seudonimización de los datos.

Artículo 8°. ***Condiciones para el consentimiento*.**

1. Cuando el tratamiento se base en el consentimiento del titular, el responsable deberá ser capaz de demostrar que aquel otorgó el consentimiento de forma previa el tratamiento de sus datos personales.

2. Corresponderá al responsable del tratamiento, demostrar la existencia del consentimiento del titular por cualquier medio de prueba admisible en derecho.

3. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, debiendo constar cada finalidad de forma separada, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción de la presente ley.

4. El responsable establecerá mecanismos o procedimientos que permitan al titular manifestar su consentimiento mediante un acto afirmativo que refleje una manifestación de voluntad previa, expresa, libre, inequívoca, informada y específica. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.

5. Si el responsable del tratamiento solicita el consentimiento del titular durante la ejecución de un contrato y este no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al titular que manifieste expresamente su negativa al tratamiento.

6. El titular tendrá derecho a revocar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará la legalidad del tratamiento basada en el consentimiento previo a la revocatoria. Será tan fácil revocar el consentimiento como darlo.

Artículo 9°. ***Consentimiento de niños, niñas y adolescentes.***

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de dieciséis años. Se exceptúan los supuestos en que la ley exija la asistencia del representante legal para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de dieciséis años, fundado en el consentimiento, sólo será lícito si consta el consentimiento del representante legal, con el alcance que determine el mismo.

3. En relación con la oferta directa a menores de edad de servicios de la sociedad de la información, le serán aplicables las reglas establecidas en el numeral 1 y 2 del presente artículo teniendo en cuenta la tecnología disponible. Cuando concurra la situación descrita en el numeral 2, el responsable del tratamiento adoptará todas las medidas razonables con los recursos que dispone, para verificar que el consentimiento fue dado o autorizado por el representante legal del menor.

4. El numeral 1 no afectará las disposiciones especiales referentes al establecimiento de edades mínimas para efectos civiles y penales, respecto de la validez y consecuencias de ciertos actos jurídicos.

5. El tratamiento de datos personales de menores de edad siempre debe responder al interés superior del menor y asegurar el respeto de sus derechos fundamentales.

Parágrafo. En caso de lo dispuesto en el numeral 2, cuando la representación legal del menor de dieciséis años es ejercida por más de una persona, se presume que el consentimiento de uno obedece a la voluntad de todos. En el supuesto de que, uno de los representantes no esté de acuerdo, puede revocar el consentimiento ante el responsable del tratamiento, y sólo podría concederse nuevamente por el mutuo

acuerdo de los representantes, o mediante decisión judicial que declare su representación legal.

Artículo 10. ***Tratamiento de datos sensibles.***

1. Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas y la afiliación sindical, organizaciones sociales, de derechos humanos, datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, los datos relativos a la salud, datos relativos al sexo o características biológicas, identidad o expresión de género y orientación sexual de una persona natural.
2. El numeral 1 no será de aplicación cuando concurra alguna de las siguientes excepciones:

a) Cuando el titular dio su consentimiento previo y expreso para el tratamiento de dichos datos personales para uno o más fines específicos, excepto cuando la ley impida al titular levantar la prohibición mencionada en el numeral 1.

b) Cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral o de la seguridad social, en la medida en que así lo autorice la ley o una convención colectiva de trabajo con arreglo a la normatividad vigente, que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del titular.

c) Cuando el tratamiento sea necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto que el titular se encuentre incapacitado física o jurídicamente para autorizar dicho tratamiento.

d) Cuando el tratamiento sea realizado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otra organización sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los titulares.

e) Cuando el tratamiento se refiera a datos personales que el titular de forma libre y voluntaria decida hacer públicos. No debe ser una divulgación de datos accidental, inadvertida o involuntaria.

f) Cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones y/o procedimientos administrativos y/o judiciales, así como procedimientos extrajudiciales o cuando sea un órgano judicial que actúe en ejercicio de su función.

g) Cuando el tratamiento sea necesario por razones de interés público, para la prestación de servicios públicos o por parte de entidades que ejerzan funciones públicas, sobre la base de la normativa que los faculta para ejercer dichas funciones; el tratamiento debe ser proporcional al objetivo perseguido, respetando el derecho a la protección de datos, **estableciendo** medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del titular.

h) Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluaciones médicas ocupacionales del trabajador, diagnóstico médico, prestación de asistencia o tratamiento médico, gestión de los sistemas y prestación de servicios de salud, sobre la base de la normativa o en virtud de un contrato con un profesional de la salud, sin perjuicio de las condiciones y garantías contempladas en el numeral 3 del presente artículo.

i) Cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transnacionales graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de la norma, que establezca medidas adecuadas y específicas para proteger los derechos y garantías del titular, en particular el secreto profesional. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y garantías de las personas naturales.

j) El tratamiento es necesario con fines de archivo en interés público, investigación científica, histórica o estadística; este debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos, establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

3. Los datos personales a los que se refiere el numeral 1 podrán tratarse a los fines citados en el numeral 2, literal h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de

secreto profesional de acuerdo con el artículo 74 de La Constitución Política de Colombia.

Parágrafo. Cuando por alguna de las causales a las que se refiere el numeral segundo se deban tratar datos sensibles referentes al sexo, identidad o expresión de género y orientación sexual, deberán hacer uso de todas las categorías identitarias diversas, como personas intersexuales y no binarias. En el supuesto de que el titular del dato haya dado su consentimiento para el tratamiento de los datos aquí referidos y ejercite los derechos de rectificación y supresión, no se le exigirán requisitos adicionales para comprobar esta información.

Artículo 11. ***Tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.***

El tratamiento de datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales, así como las medidas de seguridad conexas, además de cumplir con las obligaciones establecidas en la presente ley, sólo podrá realizarse bajo la supervisión de las entidades competentes, quienes deberán garantizar la protección adecuada de los derechos y garantías de los titulares.

Artículo 12. ***Tratamiento de datos relativos a sanciones administrativas y/o disciplinarias*****.**

1. El tratamiento de datos relativo a sanciones administrativas y/o disciplinarias, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los organismos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el numeral anterior, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias, habrán de contar con el consentimiento del titular o estar autorizados por una norma, en la que se regularán, en su caso, garantías adicionales para los derechos de los titulares.

3. Fuera de los supuestos señalados en los numerales anteriores, los tratamientos de datos referidos a infracciones, sanciones administrativas y/o disciplinarias sólo serán posibles cuando sean llevados a cabo por abogados y/o agentes oficiosos y que tengan por objeto recoger la información facilitada por sus representados para el ejercicio de sus funciones.

Parágrafo. Lo descrito en el presente artículo se aplicará igualmente a las sanciones disciplinarias de los servidores públicos.

TÍTULO II

DEBER DE INFORMACIÓN Y DERECHOS DE LOS TITULARES

CAPÍTULO I

Transparencia e información

Artículo 13. ***Transparencia e información al titular.***

1. El responsable del tratamiento tomará las medidas pertinentes para facilitar al titular toda la información indicada en los artículos 14 y 15, así como cualquier comunicación correspondiente a los ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un menor. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. A petición del titular, la información podrá facilitarse verbalmente siempre que se acredite la identidad del mismo por medios adecuados.

2. El responsable del tratamiento facilitará al titular mecanismos sencillos y ágiles para el ejercicio de sus derechos en virtud de la presente ley. En caso de que el responsable no esté en condiciones de identificar al titular, no se aplicarán los artículos relativos al ejercicio de derechos de los artículos 18 al 23, salvo que el titular facilite información adicional que permita su identificación.

3. El responsable del tratamiento facilitará al titular información relativa a sus actuaciones sobre la base de una solicitud de ejercicio de derechos, dentro de los 15 días hábiles contados a partir del día siguiente a la fecha de su recibo.

Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al titular los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Cuando el titular presente la solicitud por medios electrónicos, la información se facilitará por dichos medios cuando sea posible, a menos que el titular solicite que se facilite de otro modo que no represente una carga desproporcionada para el responsable.

4. El responsable del tratamiento tiene la obligación de contestar las solicitudes de ejercicio de derechos de forma completa y de fondo. En todas las contestaciones de ejercicio de derechos, se deberá informar la posibilidad de presentar una queja ante la autoridad de protección de datos.

5. La información facilitada en virtud de los artículos 14 y 15, así como cualquier comunicación correspondiente a los

ejercicios de los derechos o de un incidente de seguridad de los datos personales al titular en virtud de la presente ley, serán a título gratuito.

Para tal efecto, se podrá considerar reiterativo el ejercicio del derecho de acceso en más de una ocasión en menos de un mes, a menos que exista causa legítima para ello. El responsable deberá demostrar a la autoridad de protección de datos, cuando ésta así lo requiera, que la conducta del titular es carente de fundamento legal, temeraria y/o reiterativa.

6. Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad del titular que radicó una solicitud de ejercicio de derechos, podrá requerir a éste información adicional necesaria para confirmar su identidad.

7. La información que deba facilitarse a los titulares en virtud de los artículos 14 y 15 podrá compartirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. Los responsables tendrán en cuenta a los titulares con discapacidades.

8. La Autoridad de protección de datos establecerá las reglas, símbolos e imágenes mediante las cuales el responsable del tratamiento o el encargado podrán dar cumplimiento al deber de información, comunicación de políticas de tratamiento de la información, divulgación de información sobre seguridad de datos, notificación de derechos de los titulares de datos, así como otras circunstancias en las que sea necesario su aplicación.

Artículo 14. ***Información que deberá facilitarse cuando los datos personales se obtengan del titular.***

1. Cuando se obtienen de un titular datos personales relativos a este, el responsable del tratamiento, en el momento en que estos se obtienen, le facilitará toda la información indicada a continuación:

a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.

b) Los datos de contacto del oficial de protección de datos o área encargada de la protección de datos personales.

c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.

d) Los destinatarios de los datos personales, si los hubiera.

e) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel adecuado de protección de la autoridad de protección de datos. En los casos de las transferencias indicadas en los artículos 49 o 51, la información referente a las garantías adecuadas o apropiadas, y los medios para obtener una copia de estas o al hecho de que se hayan prestado.

f) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.

g) La descripción y ejercicio de los derechos que le asisten al titular.

h) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación.

i) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.

j) Cuando la comunicación de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles consecuencias de no facilitar tales datos.

k) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.

2. Cuando el responsable proyecte uno o varios tratamientos de datos personales con finalidades diferentes a las iniciales, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 1 del presente artículo.

3. Las disposiciones de los numerales 1 y 2 no serán aplicables en la medida en que el titular ya disponga de la información y exista prueba de ello.

Artículo 15. ***Información que deberá facilitarse cuando los datos personales no se hayan obtenido del titular.***

1. Cuando los datos personales no se hayan obtenido del titular, el responsable del tratamiento le facilitará a este la siguiente información:

a) Nombre o razón social, domicilio, dirección, correo electrónico y teléfono, u otro medio

de contacto, si lo hubiera, del responsable y, en su caso, de su representante legal.

b) Los datos de contacto del oficial de protección de datos o área encargada de datos personales.

c) Los fines del tratamiento a que se destinan los datos personales y la base legitimadora del tratamiento.

d) Las categorías de datos personales de que se trate.

e) Los destinatarios de los datos personales, si aplica.

f) En caso de ser procedente, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una declaración de nivel de adecuado de protección de la autoridad de protección de datos, o, en el caso de las transferencias indicadas en la presente ley referente a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

g) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.

h) La descripción y ejercicio de los derechos que le asisten al titular.

i) Cuando el tratamiento esté basado en el consentimiento o en el consentimiento para tratar datos sensibles, la existencia del derecho a revocar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a la revocación.

j) El derecho a presentar una queja ante la autoridad de protección de datos, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos.

k) Cuando la comunicación de datos personales sea un requisito legal o contractual, o un requisito necesario para suscribir un contrato, el titular debe estar informado de las posibles consecuencias de no facilitar tales datos.

l) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.

2. El responsable del tratamiento facilitará al titular la información indicada en el numeral 1:

a) Dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se trate dichos datos.

b) Sí los datos personales han de utilizarse para comunicación con el titular, a más tardar en el momento de la primera comunicación a dicho titular.

c) Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al titular, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente en virtud del numeral 2.

4. Las disposiciones de los apartados 1 a 4 no serán aplicables en la medida en que:

a) El titular ya disponga de la información.

b) La comunicación de dicha información resulte imposible o suponga una carga desproporcionada, en particular para el tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística, a reserva de las condiciones y garantías indicadas en la presente ley, o en la medida en que la obligación mencionada en el numeral 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos y garantías fundamentales del titular, inclusive haciendo pública la información.

c) La obtención o la comunicación esté expresamente establecida por la legislación nacional que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los derechos y garantías fundamentales del titular.

d) Cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por la legislación nacional.

Artículo 16. ***Aviso de privacidad***

1. Cuando los datos personales sean obtenidos del titular, el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en la presente ley, facilitando al titular la información básica a la que se refiere el numeral siguiente e indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata al resto de la información.

2. La información básica a la que se refiere el numeral anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante legal, si aplica.

b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 18 al 27 de la presente ley.

Si los datos obtenidos del titular fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el titular deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre éste o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 25 de la presente ley.

3. Cuando los datos personales no hubieran sido obtenidos del titular, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 de la presente ley facilitando a aquel la información básica señalada en el numeral anterior, indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.

b) Las fuentes de las que procedieron los datos.

CAPÍTULO II

Ejercicio de los derechos

Artículo 17. ***Disposiciones generales sobre ejercicio de los derechos.***

1. Los derechos reconocidos en la presente ley, podrán ejercerse directamente o con el acompañamiento de los apoyos señalados en la Ley 1996 de 2019 y la Ley 1306 de 2009 o cualquier norma que la adicione, modifique o sustituya, o por medio de representante legal.

2. El responsable del tratamiento estará obligado a informar al titular sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el titular. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar por otro medio y deberá redireccionarse al área encargada de atender de fondo la solicitud presentada por el titular.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los titulares de sus derechos si así se estableciera en el contrato o acto jurídico que les vincule. En ningún caso ello significa pérdida de la responsabilidad que recae en el responsable del tratamiento.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulada por el titular recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en la presente ley, se aplicará lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad o representante legal podrán ejercitar en nombre y representación de los menores de edad los derechos de acceso, rectificación, cancelación, oposición o cualquier otro que pudieran corresponderles en el contexto de la presente ley, respetando siempre el interés superior del menor y su derecho a ser escuchado o expresar su opinión en función de su edad y madurez.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en la presente ley.

8. El ejercicio de uno o varios de los derechos no afectará negativamente al titular para el ejercicio de los demás derechos y garantías contenidos en esta norma siempre que ello fuere posible.

Artículo 18. ***Derecho de acceso.***

1. El titular tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, el derecho de acceso a tales datos, y entre otra, a la siguiente información:

a) Los fines del tratamiento.

b) Las categorías de datos personales de que se trate.

c) Los destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales.

d) El plazo previsto de conservación de los datos personales o, en su defecto, los criterios utilizados para determinar este plazo.

e) La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al titular, u oponerse a dicho tratamiento.

f) El derecho a presentar una queja ante la autoridad de protección de datos.

g) Cuando los datos personales no se hayan obtenido del titular, cualquier información disponible sobre su origen.

h) La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular.

2. Cuando se transfieran datos personales a tercer país u organización internacional, el titular tendrá derecho a ser informado de las garantías adecuadas relativas a la transferencia en virtud de la presente ley.

3. El responsable del tratamiento facilitará al titular una copia de los datos personales objeto de tratamiento. Cuando el titular presente la solicitud por medios electrónicos, a menos que solicite expresamente otro método de entrega, la información se facilitará en un formato electrónico de uso común. La entrega de la información no afectará negativamente los derechos y garantías de otras personas naturales.

Artículo 19. ***Derecho de rectificación.***

1. El titular tendrá derecho a obtener del responsable del tratamiento, la rectificación en condiciones de equidad de los datos personales inexactos, parciales, incompletos, fraccionados o que induzcan a error que le concierne, teniendo en cuenta los fines del tratamiento.

2. En el caso de solicitudes relacionadas con situaciones que tengan consecuencias jurídicas significativas, el responsable del tratamiento podrá requerir pruebas que respalden la inexactitud de los datos, sin que esto suponga una carga desproporcionada para el titular.

Artículo 20. ***Derecho de supresión.***

1. El titular tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le concierne, el cual estará obligado a suprimir los datos personales cuando concurra alguna de las siguientes circunstancias:

a) Los datos personales ya no serán necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

b) El titular retire el consentimiento en que se basa el tratamiento de conformidad con la presente ley y este no se fundamente en otra base legitimadora.

c) El titular se oponga al tratamiento con arreglo a la presente ley y no prevalezcan otros motivos legítimos.

d) Los datos personales hayan sido tratados ilícitamente.

e) Los datos personales deben suprimirse para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.

f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de edad mencionados en la presente ley.

g) La autoridad de protección de datos determine que en el tratamiento ha incurrido en conductas contrarias a la Constitución o la presente ley.

2. Cuando haya cedido los datos personales y esté obligado, en virtud de lo dispuesto en el numeral 1, a suprimir dichos datos, el responsable del tratamiento teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los destinatarios o terceros que estén tratando los datos personales de la solicitud del titular de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los numerales 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) Para ejercer el derecho a la libertad de expresión e información.

b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la ley que se aplique al responsable del tratamiento, o para el cumplimiento de una función realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

c) Por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 10, numeral 2, literales h) e i), y numeral 3 de la presente ley.

d) Con fines de archivo en interés público, investigación científica, o estadística, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.

e) Para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.

Artículo 21. ***Derecho a la limitación del tratamiento.***

1. El titular tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las siguientes condiciones:

a) El titular impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.

b) El tratamiento sea ilícito y el titular se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.

c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de reclamos administrativos o judiciales.

d) El titular se haya opuesto al tratamiento en virtud de la presente ley, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del numeral 1, dichos

datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del titular; o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales; o con miras a la protección de los derechos de otra persona natural o jurídica o por razones de interés público.

3. Todo titular que haya obtenido la limitación del tratamiento con arreglo al numeral 1, será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 22. ***Obligación de notificar la rectificación o supresión de datos personales o la limitación del tratamiento.***

El responsable del tratamiento notificará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo a esta ley, a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado y esté en condición de demostrarlo. El responsable informará al titular acerca de dichos destinatarios, si éste así lo solicita.

Artículo 23. ***Derecho a la portabilidad de los datos.***

1. El titular tendrá derecho a recibir los datos personales que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común, lectura mecánica e interoperable y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) El tratamiento esté basado en el consentimiento o en un contrato con arreglo a esta ley.

b) El tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el numeral 1, el titular tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el numeral 1 del presente artículo se entenderá sin perjuicio de lo dispuesto en esta ley. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una función realizada en interés público, en el ejercicio de poderes o funciones públicas conferidas al responsable del tratamiento.

4. El derecho mencionado en el numeral 1 no afectará negativamente los derechos y garantías de otras personas naturales.

5. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

Artículo 24. ***Derecho de oposición.***

1. El titular tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de un tratamiento basado en lo dispuesto en esta ley, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las garantías del titular, o para la formulación, el ejercicio o la defensa de reclamaciones administrativas o judiciales.

2. Cuando el tratamiento de datos personales tenga por objeto marketing y publicidad directa, el titular tendrá derecho a oponerse en todo momento al tratamiento de sus datos personales, incluida la elaboración de perfiles en la medida en que esté relacionada con marketing y publicidad. Cuando el titular se oponga al tratamiento con fines de marketing y publicidad directa, los datos personales dejarán de ser tratados para **tal fin.**

3. A más tardar en el momento de la primera comunicación con el titular, el derecho indicado en los numerales 1 y 2 será mencionado explícitamente al titular y será presentado claramente y al margen de cualquier otra información.

4. En el contexto de la utilización de servicios de la sociedad de la información, el titular podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

5. Cuando los datos personales se traten con fines de investigación científica, histórica o estadística, el titular tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de sus datos personales, salvo que sea necesario, para el cumplimiento de una función realizada en interés público o en el ejercicio de funciones públicas.

Artículo 25. ***Decisiones individuales automatizadas, incluida la elaboración de perfiles.***

1. Todo titular tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, en los que no medie intervención humana alguna, incluida la elaboración de perfiles, que le produzca efectos jurídicos o le afecte significativamente de modo similar.

2. El numeral 1 no se aplicará, si la decisión:

a) Es necesaria para la celebración o la ejecución de un contrato entre el titular y un responsable del tratamiento.

b) Está autorizada por una ley que se aplique al responsable del tratamiento, siempre que se establezcan medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.

c) Se basa en el consentimiento explícito del titular.

3. En los casos a que se refiere el numeral 2, literales a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y garantías fundamentales del titular, como mínimo el derecho a obtener intervención humana por parte del responsable, expresar su punto de vista, recibir una explicación de la decisión e impugnar la decisión.

4. Las decisiones a las que se refiere el numeral 2, no se basarán en datos sensibles contemplados en esta ley, salvo que se apliquen las excepciones previstas en la presente ley y se hayan tomado medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.

Artículo 26. ***Derecho a presentar una queja ante la autoridad de protección de datos.***

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo titular que considere que su derecho fundamental a la protección de datos ha sido vulnerado por infracción a la presente ley, tendrá derecho a presentar una queja ante la autoridad de protección de datos.

2. El titular o quien represente sus intereses sólo podrá elevar queja ante la autoridad de protección de datos, una vez que haya agotado el requisito de procedibilidad, esto es, la presentación de una solicitud previa, con ejercicio de derechos, ante el responsable o el encargado según sea el caso siempre que, habiendo transcurrido el término establecido en esta ley para la solución del reclamo previo, el sujeto obligado no se hubiese pronunciado o, de existir respuesta, esta no satisfaga los intereses del titular.

Artículo 27. ***Derecho a presentar una denuncia ante la Autoridad de protección de datos.***

1. Quien tenga conocimiento sobre hechos que deriven en el posible incumplimiento de las disposiciones establecidas en esta ley, tendrá derecho a presentar una denuncia ante la **autoridad de protección** de datos, persiguiendo la protección del interés colectivo y el derecho a la protección de los datos personales.

2. La denuncia podrá presentarse a nombre propio o de forma anónima. Si quien presenta la denuncia solicita a la autoridad de protección de datos la reserva de su identidad, ésta deberá adoptar las medidas técnicas necesarias para evitar a terceros conocer los datos personales del denunciante.

3. La autoridad de protección de datos tendrá la obligación de examinar integralmente las denuncias presentadas por los ciudadanos. Con base en los hechos presentados, los documentos aportados y las indagaciones preliminares que realice, determinará si existe mérito o no para iniciar una investigación administrativa y, como resultado de ellas, establecerá las medidas que sean necesarias para hacer efectivo el derecho a la protección de los datos personales conforme a lo establecido en la presente ley.

TÍTULO III

RESPONSABLE DEL TRATAMIENTO Y ENCARGADO DEL TRATAMIENTO

CAPÍTULO I

Obligaciones generales

Artículo 27. ***Deberes del responsable 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:

1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.

2. Establecer una base jurídica que legitime el tratamiento de datos personales de acuerdo con lo establecido en el artículo 6° de la presente ley.

3. Implementar medidas de seguridad de conformidad con el artículo 35, a fin de garantizar y demostrar que el tratamiento es conforme con la presente ley. Revisar y actualizar dichas medidas cuando sea necesario.

4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley.

5. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos a lo que haya tenido acceso y adoptar las demás medidas necesarias para que la información suministrada a este, se mantenga actualizada.

6. Garantizar el pleno ejercicio de los derechos que le conciernen a los titulares en los términos previstos en los artículos 18 al 27 de la presente ley y en las demás normas que la modifiquen o adicionen.

7. Cumplir con el deber de información contenido en los artículos 14 y 15 de la presente ley

8. Notificar a la autoridad de protección de datos, cuando se presenten incidentes de seguridad de conformidad con el artículo 36 de la presente ley.
9. Comunicar los incidentes de seguridad, cuando sea el caso, a los titulares afectados de conformidad con el artículo 37 de la presente ley.
10. Cumplir las instrucciones y requerimientos que imparta la autoridad de protección de datos.
11. Elaborar evaluaciones de impacto sobre la privacidad, cuando sea el caso, en los términos descritos en el artículo 38 de la presente ley.
12. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.
13. Llevar un registro de las actividades del tratamiento en los términos descritos en el artículo 33 de la presente ley.
14. Realizar una revisión interna o externa, a los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, al menos cada dos años, para verificar el cumplimiento de la presente ley.

Con carácter extraordinario deberá realizarse dicha revisión siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de la presente ley. Con dicha revisión se reiniciará el cómputo de los dos años señalados en el inciso anterior.

15. Cooperar con la autoridad de protección de datos cuando lo solicite.
16. Elegir un encargado o encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento cumpla con los requisitos establecidos en el artículo 32 de la presente ley y garantice la protección de los derechos del titular.
17. Nombrar un Oficial de protección de datos personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.
18. Demostrar el cumplimiento del código de conducta al que se haya adherido, de conformidad con el artículo 42 de la presente ley.
19. Mantener los compromisos que le ha permitido acceder a un mecanismo de certificación de certificación en los términos descritos en el artículo 45 de la presente ley.

Artículo 29. ***Deberes del encargado 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:

1. Aplicar los principios contemplados en la presente ley en el tratamiento de datos personales.
2. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe alguno de los principios contemplados en la presente ley o cualquier otra disposición en materia de protección, informará inmediatamente al responsable.
3. Utilizar los datos personales objeto de tratamiento, sólo para la finalidad del encargo. En ningún caso podrá utilizar los datos para fines propios.
4. Llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, de conformidad con el artículo 33 de la presente ley.
5. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento.
6. No subcontratar ninguna de las prestaciones que formen parte del encargo, salvo que cuente con autorización expresa del responsable.
7. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del encargo, incluso después de que finalice el mismo.
8. Garantizar que el personal, con acceso a datos personales objeto del encargo reciba formación sobre protección de datos y se comprometa por escrito a mantener la confidencialidad y cumplir con las medidas de seguridad. El encargado debe mantener a disposición del responsable y/o la autoridad competente, la documentación que demuestre el cumplimiento de estas obligaciones.
9. El encargado informará al responsable del tratamiento, sobre cualquier incidente de seguridad relacionado con los datos personales objeto del tratamiento, proporcionando toda la información pertinente necesaria para documentar y notificar el incidente a la autoridad de protección de datos.
10. Nombrar un Oficial de Protección de Datos Personales, cuando sea el caso, en los términos descritos en el artículo 39 de la presente ley.
11. Garantizar que las transferencias internacionales cumplan las condiciones establecidas en el Título VI de la presente ley.
12. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando sea

el caso, de conformidad con el artículo 38 de la presente ley.

13. Poner a disposición del responsable o de la Autoridad de Protección de Datos, toda la información necesaria para demostrar el cumplimiento de sus obligaciones.

14. Implantar las medidas de seguridad acordadas con el responsable del tratamiento, así como aquellas que correspondan en función del riesgo asociado a la prestación del servicio.

15. Eliminar o devolver al responsable del tratamiento los datos personales, así como los soportes en los que estén almacenados, una vez finalizada la prestación del servicio. La devolución debe incluir la eliminación completa de los datos almacenados en los equipos informáticos utilizados por el encargado, a menos que existan excepciones legales y/ o contractuales.

16. Cooperar con la autoridad de protección de datos cuando lo solicite.

Artículo 30. ***Protección de datos desde el diseño y por defecto.***

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y garantías de las personas naturales, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos de la presente ley y proteger los derechos de los titulares.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles.

Tendrá acceso únicamente el personal autorizado, salvo que se modifique en razón de las circunstancias del tratamiento.

3. Para el cumplimiento de lo establecido en los numerales 1 y 2, el responsable del tratamiento tendrá en cuenta:

a) La protección de los datos personales de forma proactiva y no reactiva.

b) La protección de los datos personales preventiva y no correctiva.

c) La privacidad como configuración predeterminada.

d) La protección de los datos en el ciclo de vida completo de su tratamiento, es decir, desde la recolección hasta su posible supresión.

e) La transparencia en el tratamiento de los datos.

f) La prevalencia de la privacidad como interés del titular.

4. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 60, como elemento que acredite el cumplimiento de las obligaciones establecidas en los numerales 1 y 2 del presente artículo.

Artículo 31. ***Corresponsables del tratamiento.***

1. Cuando dos o más responsables determinen conjuntamente los fines y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo, sus respectivas responsabilidades en el cumplimiento de las obligaciones impuestas por la presente ley, en particular, en el ejercicio de los derechos de los titulares y sus obligaciones de suministro de información, a las cuales se refiere la presente ley.

2. El acuerdo indicado en el numeral 1, reflejará adecuadamente las funciones y relaciones respectivas de los corresponsables en relación con los titulares. Se pondrán a disposición del titular los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el numeral 1, los titulares podrán ejercer los derechos que les reconoce la presente ley frente a cada uno de los responsables.

Artículo 32. ***Encargado del tratamiento.***

1. El encargado del tratamiento no recurrirá a otro encargado sin la autorización, específica o general, del responsable ya sea por escrito o por mensajes de datos suficientes y verificables.

Cuando la autorización para el subencargo del tratamiento sea general, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

2. El tratamiento debe regirse por un contrato u otro acto jurídico con arreglo a las leyes civiles o mercantiles, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza, la finalidad del tratamiento, el tipo de titulares, categorías de datos personales, las obligaciones y los derechos del responsable. Dicho contrato estipulará, en particular, que el encargado:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país u organización internacional, salvo que esté obligado a ello en virtud de un mandato legal que se aplique al encargado. En tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que dicho mandato lo prohíba por razones importantes de interés público.

b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza contractual.

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

d) Respetará las condiciones indicadas en la presente ley para recurrir a un subencargado del tratamiento.

e) Asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los titulares o podrá comprometerse a resolver, por cuenta del responsable y dentro de los plazos establecidos en esta ley, las solicitudes de ejercicio de derechos.

f) Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en la presente ley, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.

g) A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud de una disposición legal o por motivos de responsabilidad derivada de su relación.

h) Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

3. El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe la presente ley u otras disposiciones en materia de protección de datos.

4. Cuando un encargado del tratamiento recurra a un subencargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este subencargado, las mismas obligaciones de protección de datos que las estipuladas en el contrato entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones de la presente ley. Si el subencargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo que respecta al cumplimiento de las obligaciones del otro.

5. La adhesión del encargado y/o subencargado del tratamiento a un código de conducta aprobado o a un mecanismo de certificación aprobado como lo indica esta ley, podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a las que se refiere el presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato que menciona los numerales 2 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales modelo, las cuales hacen alusión a los numerales 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable, encargado o subencargado de conformidad con esta ley.

7. La autoridad de protección de datos podrá fijar cláusulas contractuales modelo, para los contratos a los que hacen mención los numerales 2 y 4 del presente artículo.

8. El contrato al cual se refieren los numerales 2 y 4 deberá constar por escrito, inclusive en formato electrónico.

9. Sin perjuicio de lo dispuesto en esta ley, si un encargado o subencargado del tratamiento infringe la presente ley, al determinar los fines y medios del tratamiento, será considerado responsable con respecto a dicho tratamiento.

10. El responsable del tratamiento podrá exigir a los encargados que sean proveedores de servicios tecnológicos, aplicaciones e infraestructura tecnológica, con los que esté adherido o se vaya a adherir a través de condiciones generales de contratación, que demuestre el cumplimiento de la presente ley. En caso de que el proveedor ignore las solicitudes realizadas por los responsables o incumpla con la presente ley, los responsables podrán denunciar dicha situación ante la autoridad de protección de datos, de conformidad con lo establecido en el artículo 27 de la presente ley.

Lo anterior no exonera al responsable del tratamiento del cumplimiento de las obligaciones establecidas en el artículo 28 de la presente ley.

Parágrafo primero. Las obligaciones establecidas en esta ley para los encargados del tratamiento serán de aplicación directa para quienes, en atención a lo dispuesto en los numerales 2 y 4 del presente artículo, adquieran la calidad de subencargados.

Parágrafo segundo. El encargado del tratamiento y cualquier persona que actúe bajo el control del responsable o del encargado y tenga acceso a datos personales, sólo podrán tratar dichos datos siguiendo instrucciones del responsable, a menos que no estén obligados a ello en virtud de una disposición legal.

Artículo 33. ***Registro de las actividades de tratamiento.***

1. Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su control. Dicho registro deberá contener toda la información indicada a continuación:

a) El nombre y los datos de contacto del responsable y, cuando sea el caso, del corresponsable, y del oficial de protección de datos o área encargada.

b) Los fines del tratamiento.

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

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

e) Los encargados que intervienen en el tratamiento.

f) De ser procedente, las transferencias de datos personales a otro país o una organización internacional, incluida la identificación de dicho país u organización internacional y, en el caso de las transferencias indicadas en el artículo 33 de la presente esta ley relativa a la documentación de garantías adecuadas.

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

h) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la remisión al documento que las contenga.

i) Los responsables del tratamiento, deben inscribir sus registros de actividades ante el Registro Nacional de las Actividades, administrado por la autoridad de protección de datos y de libre consulta para los ciudadanos.

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

a) El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y del oficial de protección de datos o área encargada.

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

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

d) De ser procedente, las transferencias de datos personales a otro país u organización internacional, incluida la identificación de dicho país u organización internacional y en el caso de las transferencias indicadas en esta ley, relativo a la documentación de garantías adecuadas.

e) Una descripción general de las medidas técnicas y organizativas de seguridad en los términos descritos en el artículo 35 de esta ley o la remisión al documento que las contenga.

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

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

5. Los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas, harán público el registro de sus actividades de tratamiento accesible por medios electrónicos, en el que constará la información establecida en el presente artículo.

Artículo 34. ***Bloqueo de los datos.***

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los Jueces y Tribunales, Fiscalía General de la Nación o las Administraciones Públicas competentes, en particular de la autoridad de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo, se procederá a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.
4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información, de manera que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.
5. La autoridad de protección de datos, dentro del ámbito de sus competencias, podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de titulares afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los titulares, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO II

Seguridad de los datos

Artículo 35. ***Seguridad del tratamiento.***

1. Teniendo en cuenta el estado de la técnica, los costos de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad, variables para los derechos y garantías de los titulares, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad, se tendrá en cuenta los riesgos que presente el tratamiento de datos, en particular, la destrucción, pérdida, alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales.
3. La adhesión a un código de conducta aprobado de conformidad con el artículo 42 o a un mecanismo de certificación aprobado de conformidad con el artículo 45, así como, la adopción de directrices dadas por la autoridad de protección de datos o indicaciones proporcionadas por un oficial de protección de datos podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el numeral 1 del presente artículo.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales, sólo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello por la ley.

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

1. En caso de incidente de seguridad de los datos personales, el responsable del tratamiento lo notificará a la autoridad de protección de datos de conformidad con esta ley, sin demora injustificada y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicho incidente de seguridad constituya un riesgo para los derechos y las garantías de las personas naturales. Si la notificación a la autoridad de protección de datos no tiene lugar en el plazo de 72 horas, deberá ir acompañada de los motivos que expliquen la dilación.
2. El encargado del tratamiento notificará, sin demora injustificada, al responsable del tratamiento, los incidentes de seguridad de los datos personales de los que tenga conocimiento.
3. La notificación contemplada en el numeral 1 deberá, como mínimo:

a) Describir la naturaleza del Incidente de seguridad de los datos personales y, cuando sea posible, el número aproximado, tipo de titulares afectados, las categorías de datos y el número aproximado de registros de datos personales afectados.

b) Comunicar el nombre y los datos de contacto del oficial de protección de datos o de otro punto de contacto, en el que pueda obtenerse más información.

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

d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento, para poner remedio al incidente de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información descrita en el numeral 3 del presente artículo, simultáneamente con la notificación de un incidente de seguridad, y en la medida que esta condición persista, la información se facilitará de manera gradual sin demora injustificada.

5. El responsable del tratamiento documentará cualquier incidente de seguridad de los datos personales, incluidos los hechos relacionados con este, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de protección de datos, verificar el cumplimiento de lo dispuesto en el presente artículo.

6. Los datos personales contenidos en la notificación de un incidente de seguridad y que fueron comunicados a la autoridad de protección de datos, proveedores de tecnologías y servicios de seguridad, podrán ser tratados exclusivamente durante el tiempo y alcance necesario para su análisis, detección, protección y respuesta ante el incidente, adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

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

1. Cuando sea probable que el incidente de seguridad de los datos personales entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento lo comunicará al titular sin demora injustificada.

2. La comunicación al titular contemplada en el numeral 1 del presente artículo, deberá describir en un lenguaje claro y sencillo la naturaleza del incidente de seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 36, numeral 3, literales b), c) y d).

3. La comunicación al titular a la que se refiere el numeral 1, no será necesaria si se cumple alguna de las siguientes condiciones:

a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por el incidente de seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.

b) El responsable del tratamiento ha tomado medidas ulteriores que garantizan que ya no exista la probabilidad de que se materialice el alto riesgo para los derechos y garantías del titular.

4. Cuando la comunicación a los titulares suponga un esfuerzo desproporcionado para el responsable del tratamiento, éste podrá optar por una comunicación pública o una medida de difusión semejante, de manera que se informe efectivamente a los titulares.

5. Cuando el responsable no haya comunicado al titular el incidente de seguridad de los datos personales, la autoridad de protección de datos, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo comunique o podrá confirmar que se cumple alguna de las condiciones mencionadas en el numeral 3.

CAPÍTULO III

Evaluación de impacto relativa a la protección de datos y consulta previa

Artículo 38. ***Evaluación de impacto relativa a la protección de datos y consulta previa***.

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y garantías de las personas naturales, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento solicitará asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos, a los que se refiere el numeral, 1 se requerirá en especial cuando:

a) Se realice evaluación sistemática y exhaustiva de aspectos personales de personas naturales, que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que les afecten significativamente de forma similar.

b) Tratamiento a gran escala de datos sensibles o de los datos personales relativos a antecedentes penales, anotaciones judiciales o contravencionales.

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

d) Se efectúen tratamientos sobre neurodatos.

4. La autoridad de protección de datos establecerá y publicará una lista de los tipos de operaciones de tratamiento, que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el numeral 1.

5. La evaluación a la que se refiere el numeral 1 del presente artículo, deberá incluir como mínimo:

a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

c) Una evaluación de los riesgos para los derechos y garantías de los titulares a los que se refiere el numeral 1.

d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente ley, teniendo en cuenta los derechos y garantías de los titulares y de otras personas afectadas.

6. El cumplimiento de los códigos de conducta aprobados, a los que se refiere el artículo 38, por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

7. Cuando el tratamiento de datos se base en un deber legal o en un interés público y esté regulado por una ley o normativa específica aplicable al responsable del tratamiento, que detalle la operación específica de tratamiento o conjunto de operaciones, y que ya incluya una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general, los numerales 1 a 6 no se aplicarán, a menos que una ley o normativa posterior lo requiera.

8. En caso de ser necesario, el responsable examinará si el tratamiento es conforme a la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

9. El responsable del tratamiento consultará previamente a la autoridad de protección de datos antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares. Si la autoridad de protección de datos considera que el tratamiento previsto supone un alto riesgo, asesorará por escrito al responsable, y en su caso al encargado, sobre las medidas técnicas y organizativas que se deberán adoptar antes del tratamiento de los datos. La autoridad de protección de datos deberá emitir un concepto en el menor tiempo posible.

Parágrafo. La zona de acceso público a la que se refiere el numeral 3 literal c) del presente artículo, hace referencia a cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas naturales, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad.

CAPÍTULO IV

Oficial de protección de datos

Artículo 39. ***Designación del Oficial de protección de datos***.

1. El responsable y el encargado del tratamiento designarán un oficial de protección de datos siempre que:

a) El tratamiento lo lleve a cabo los sujetos mencionados en los artículos 39 y 40 de la Ley 489 de 1998, incluyendo la Rama Judicial, la Rama Legislativa, los Órganos de Control, la Organización Electoral, fundaciones y otros organismos de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas.

b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de los titulares a gran escala.

c) Las actividades principales del responsable o del encargado, consistan en el tratamiento a gran escala de datos sensibles y de datos relativos a antecedentes penales, anotaciones judiciales o contravencionales, y/o sanciones administrativas.

d) La autoridad de protección de datos podrá definir nuevas indicaciones en las que se deba designar un Oficial de protección de datos y estipulará las condiciones y particularidades para dicha designación.

2. Un grupo empresarial podrá nombrar un único oficial de protección de datos, siempre que sea fácilmente accesible desde cada una de las empresas que pertenecen al grupo.

3. Cuando el responsable o el encargado del tratamiento sea una entidad u organismo público, se podrá designar un único oficial de protección de datos para varias de estas entidades u organismos, teniendo en cuenta su estructura administrativa y tamaño.

4. En casos distintos de los contemplados en el numeral 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a sectores a los que pertenezcan los responsables o encargados, podrán designar de forma voluntaria un oficial de protección de datos.
5. El oficial de protección de datos será designado siempre que cuente con un perfil legal o un perfil interdisciplinario con conocimientos legales y experiencia en protección de datos. Además, se verificará su capacidad para desempeñar las funciones indicadas en esta ley.
6. El oficial de protección de datos podrá vincularse con el responsable o el encargado del tratamiento por medio de un contrato de prestación de servicios o un contrato laboral.
7. El responsable o el encargado del tratamiento publicará los datos de contacto del oficial de protección de datos y los comunicará a la autoridad de protección de datos en un plazo de quince (15) días hábiles.

Las designaciones, nombramientos y ceses de los oficiales de protección de datos, tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria, también deberán ser notificadas en el mismo término.

8. La autoridad de protección de datos, mantendrá en el ámbito de sus competencias, una lista actualizada de oficiales de protección de datos que será accesible a través de medios electrónicos.
9. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento, podrán establecer la dedicación completa o a tiempo parcial del oficial, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos y garantías de los titulares.

Artículo 40. ***Posición del oficial de protección de datos.***

1. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relacionadas con la protección de datos personales.
2. El responsable y el encargado del tratamiento respaldarán al oficial de protección de datos en el desempeño de las funciones estipuladas en la presente ley, facilitando los recursos necesarios para el desempeño de dichas funciones, el acceso a los datos personales y a las operaciones de tratamiento.
3. El responsable y el encargado del tratamiento garantizarán que el oficial de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurrieren en dolo o negligencia grave en su ejercicio. El oficial de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.
4. Los titulares podrán ponerse en contacto con el oficial de protección de datos, en relación a todas las cuestiones correspondientes al tratamiento de sus datos personales y al ejercicio de sus derechos y garantías al amparo de la presente ley.
5. El oficial de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el artículo 74 de la Constitución Política.
6. El oficial de protección de datos podrá desempeñar otras funciones y el responsable o encargado del tratamiento garantizará que estas no den lugar a conflicto de intereses.
7. El oficial de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la autoridad de protección de datos. El oficial podrá verificar los procedimientos y emitir recomendaciones en el ámbito de sus competencias.

Artículo 41. ***Funciones del oficial de protección de datos.***

1. El oficial de protección de datos tendrá como mínimo las siguientes funciones:

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones que les competen en virtud de la ley y otras disposiciones referentes a la protección de datos.

b) Supervisar el cumplimiento de lo dispuesto en la presente ley.

c) Supervisar la implementación y aplicación de un manual interno de políticas y procedimiento en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

d) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto, relativa a la protección de datos y supervisar su aplicación de conformidad con la presente ley.

e) Cooperar con la autoridad de protección de datos.

f) Actuar como punto de contacto de la autoridad de protección de datos, sobre cuestiones relativas al tratamiento, incluida

la consulta previa a la que se refiere el artículo 38, numeral 9, así como solicitar instrucciones, en su caso, sobre cualquier otro asunto.

g) Cuando el oficial de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos, lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

2. El oficial de protección de datos, desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

CAPÍTULO V

Mecanismos de autorregulación

Artículo 44. ***Códigos de conducta.***

1. La Autoridad de protección de datos, promoverá la elaboración de códigos de conducta, destinados a contribuir a la correcta aplicación de la presente ley, teniendo en cuenta las características específicas de las distintas actividades de tratamiento y las necesidades específicas de las microempresas, las pequeñas y medianas empresas.

2. Las asociaciones y otras entidades representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta, modificar o ampliar dichos códigos con objeto de especificar la aplicación de la presente ley, en lo que respecta a:

a) El tratamiento leal y transparente.

b) Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos.

c) La recogida de datos personales.

d) La seudonimización de datos personales.

e) La información proporcionada al público y a los titulares.

f) El ejercicio de los derechos de los titulares.

g) La información proporcionada a los menores y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o representantes legales del menor.

h) Las medidas, procedimientos y las acciones para garantizar la seguridad del tratamiento contenidas en esta ley.

i) La notificación de incidentes de seguridad de los datos personales a la autoridad de protección de datos y la comunicación de dichos incidentes a los titulares.

j) La transferencia de datos personales a terceros países u organizaciones internacionales.

k) Los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos, que permitan resolver las controversias entre los responsables y los titulares relativos al tratamiento, sin perjuicio del derecho presentar una queja ante la autoridad de protección de datos o acudir ante autoridad judicial.

3. Los responsables o encargados del tratamiento a los que se aplica la presente ley, así como también, a los que no se aplica, podrán adherirse también a códigos de conducta aprobados de conformidad con el numeral 5 del presente artículo, con el fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales.

Los mencionados responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas las relativas a los derechos de los titulares.

4. El código de conducta, contendrá mecanismos que permitan a la entidad supervisora, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados del tratamiento, que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de la autoridad de protección de datos.

5. Las asociaciones y otras entidades mencionadas en el numeral 2 del presente artículo, que pretendan elaborar un código de conducta, modificar o ampliar un código existente presentarán el proyecto de código, la modificación o ampliación a la autoridad de protección de datos.

La autoridad de protección de datos determinará si el proyecto de código, la modificación o ampliación es conforme con la presente ley y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

6. Si el proyecto de código, la modificación o ampliación es aprobado de conformidad con el numeral 5, la autoridad de protección de datos el código.

7. La autoridad de protección de datos llevará un registro de todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 43. ***Supervisión de códigos de conducta aprobados.***

1. Podrá supervisar el cumplimiento de un código de conducta, una entidad que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditada

para tal fin por la autoridad de protección de datos, sin perjuicio de las funciones y facultades de esta.

2. La autoridad de protección de datos fijará los criterios de acreditación de las entidades a las que se refiere el presente artículo.

3. Sin perjuicio de las funciones y las facultades de la autoridad de protección de datos, en virtud del numeral 1 del presente artículo, la entidad acreditada deberá, con sujeción a las garantías del debido proceso, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este.

Informará de dichas medidas y sus razones, a la autoridad de protección de datos.

4. La autoridad de protección de datos podrá revocar la acreditación de una entidad de conformidad con el numeral 1, si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicha entidad infringe la presente ley.

5. El presente artículo no se aplicará al tratamiento realizado por autoridades y entidades públicas.

Artículo 44. ***Deberes de las entidades supervisoras de códigos de conducta.***

Las entidades supervisoras de códigos de conducta deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

1. Demostrar, a satisfacción de la autoridad de protección de datos, su independencia y pericia en relación con el objeto del código.

2. Establecer procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación.

3. Establecer procedimientos y estructuras para tratar los reclamos relativos a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, para hacer que estos sean transparentes para los titulares y el público en general.

4. Demostrar, a satisfacción de la autoridad de protección de datos, que sus funciones y objetivos no dan lugar a conflicto de intereses.

Artículo 45. *Certificación*.

1. La Autoridad de protección de datos promoverá, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en la presente ley, en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas, las pequeñas y medianas empresas.

2. Podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados conforme al numeral 5 del presente artículo, con el objetivo de demostrar que los responsables o encargados no sujetos a la presente ley, según lo establecido en el artículo 3°, ofrecen garantías adecuadas en el contexto de transferencias internacionales de datos personales a terceros países u organizaciones internacionales, según lo dispuesto en el artículo 49, numeral 2, literal e).

Los responsables o encargados mencionados deberán asumir compromisos vinculantes y exigibles, por vía contractual, para aplicar las garantías adecuadas, incluidas aquellas relativas a los derechos de los titulares.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

4. La certificación a la que se refiere el presente artículo, no limitará las obligaciones del responsable o encargado del tratamiento en cuanto al cumplimiento de la presente ley y se entenderá sin perjuicio de las funciones y las facultades de la autoridad de protección de datos.

5. La certificación en virtud del presente artículo será expedida por las entidades de certificación o por la autoridad de protección de datos, sobre la base de los criterios aprobados por ésta.

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación, darán a la entidad de certificación o en su caso a la autoridad de protección de datos, toda la información y acceso a sus actividades de tratamiento que requieran para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado del tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes.

La certificación será retirada, cuando proceda, por las entidades de certificación, o en su caso por la autoridad de protección de datos, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la misma.

8. La autoridad de protección de datos llevará en un registro todos los mecanismos de certificación, sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Parágrafo primero. Serán entidades certificadoras aquellas que hayan sido acreditadas por un organismo del subsistema nacional de calidad,

el cual tenga la pericia necesaria para evaluar si los aspirantes a entidades certificadoras cuentan con un nivel adecuado de competencia en materia de protección de datos.

Parágrafo segundo. La autoridad de protección de datos hará públicos los requisitos y los criterios a los que se refiere el numeral 5 del presente artículo, en una forma fácilmente accesible.

Artículo 46. ***Deberes de las entidades certificadoras.***

Las entidades certificadoras deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

1. Demostrar ante la autoridad de protección de datos y/o los sujetos interesados en la certificación que se encuentran acreditadas por un organismo del subsistema nacional de calidad.
2. Respetar y cumplir los criterios de certificación aprobados por la autoridad de protección de datos.
3. Establecer procedimientos para la expedición, revisión periódica y retirada de certificaciones, sellos y marcas de protección de datos en los términos descritos en el numeral 7 del artículo 45.
4. Establecer procedimientos y estructuras para tratar los reclamos relativos al retiro de la certificación por el incumplimiento de los requisitos por parte de un responsable o encargado del tratamiento.
5. Informar a la autoridad de protección de datos sobre las razones para la retirada de una certificación a un responsable o encargado del tratamiento.

TÍTULO IV

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Artículo 47. ***Regla general de las transferencias.***

Solo se realizarán transferencias de datos personales si, a reserva de las demás disposiciones de la presente ley, el responsable o el encargado del tratamiento cumplen las condiciones establecidas en el presente título, incluidas las relativas a las transferencias ulteriores de datos personales. Todas las disposiciones del presente título se aplicarán, a fin de asegurar un nivel adecuado en materia de protección de datos personales.

Parágrafo. Se considera transferencia la salida de datos fuera del territorio nacional, bien sea por cesión o comunicación de datos, o por un tratamiento de datos personales por parte del encargado del tratamiento.

Artículo 48. ***Transferencias basadas en un nivel adecuado de protección.***

1. Se podrán realizar transferencias de datos personales a países u organismos internacionales que proporcionen niveles adecuados de protección de datos.
2. Se entiende que un tercer país, un territorio, uno o varios sectores específicos del tercer país, o una organización internacional ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Autoridad de Protección de Datos sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a los sujetos obligados. Para emitir una decisión de adecuación, la Autoridad de Protección de Datos deberá tener en cuenta los siguientes elementos:

a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales;

b) La legislación vigente, tanto general como sectorial, incluidas las limitaciones y garantías para el acceso de las autoridades públicas a los datos personales;

c) La existencia de garantías judiciales e institucionales para el respeto de los derechos de protección de datos personales;

d) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país u organización que reciba la información, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a las personas Titulares de los datos en el ejercicio de sus derechos, y de cooperar con la Autoridad de Protección de Datos.

3. La declaración de nivel adecuado establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. Cuando la información disponible, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado de conformidad con lo dispuesto por el presente artículo, la Autoridad de Protección de Datos, podrá derogar, modificar o suspender, en la medida necesaria y sin efecto retroactivo, la decisión adecuación.

Parágrafo primero. La autoridad de protección de datos habilitará canales de contacto para que el tercer país u organización internacional, pueda subsanar la situación que dé lugar a la decisión adoptada, de conformidad con el numeral 3.

Artículo 49. ***Transferencias mediante garantías adecuadas.***

1. A falta de declaración de nivel adecuado de protección, en los términos del artículo 48, el responsable o el encargado del tratamiento sólo podrá trasnferir datos personales a un

tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los titulares cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al numeral 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de la autoridad de protección de datos, por:

a) Un instrumento jurídicamente vinculante y exigible, bilateral o multilateral, entre Colombia y otros países u organizaciones internacionales, que habilite las transferencias desde entidades u organismos públicos establecidas en Colombia hacia entidades u organismos públicos establecidas en otros países.

b) Normas corporativas vinculantes de conformidad con el artículo 50 de la presente ley.

c) Cláusulas contractuales modelo. La autoridad de protección de datos, establecerá los criterios bajo los cuales se deben elaborar las cláusulas.

d) Un código de conducta aprobado con arreglo a la presente ley, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país, de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares.

e) Un mecanismo de certificación aprobado con arreglo al artículo 45, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares.

3. Siempre que exista declaración de nivel adecuado de protección, expedida por la autoridad de protección de datos, las garantías adecuadas contempladas en el numeral 1 podrán igualmente ser aportadas, en particular, mediante:

a) Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional.

b) Disposiciones que se incorporen en acuerdos administrativos entre las entidades u organismos públicos, que incluyan derechos efectivos y exigibles para los titulares.

Artículo 50. ***Normas corporativas vinculantes.***

1. La autoridad de protección de datos aprobará normas corporativas vinculantes, siempre que estas:

a) Sean jurídicamente vinculantes y se apliquen a todos los miembros que hacen parte del mismo grupo de empresas o de la unión de empresas dedicadas a una actividad económica conjunta.

b) Confieran expresamente a los titulares derechos exigibles previstos en los artículos 18 al 27 de la presente ley.

c) Cumplan los requisitos establecidos en el numeral 2 del presente artículo.

2. Las normas corporativas vinculantes mencionadas en el numeral 1 especificarán, como mínimo, los siguientes elementos:

a) La estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta.

b) Las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamiento y sus fines, el tipo de titulares afectados y el nombre de los países en cuestión.

c) Su carácter jurídicamente vinculante, tanto a nivel interno como externo.

d) La aplicación de los principios generales en materia de protección de datos establecidos en la presente ley.

e) Los derechos de los titulares en relación con el tratamiento y los medios para ejercerlos.

f) La forma en que se facilita a los titulares la información, sobre las normas corporativas vinculantes.

g) Las funciones del o los oficiales de protección de datos, designados de conformidad con el artículo 39, de cualquier otra persona o entidad encargada de la supervisión y del cumplimiento de las normas corporativas vinculantes, así como de la supervisión de la formación y de la tramitación de las reclamaciones.

h) Los procedimientos de reclamaciones.

i) Los mecanismos establecidos, para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas con el fin de proteger los derechos del titular.

j) Los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de protección de datos.

k) Los mecanismos para informar a la autoridad de protección de datos de cualquier requisito jurídico de aplicación en un tercer país a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías

establecidas en las normas corporativas vinculantes.

l) La formación en protección de datos pertinente, para el personal que tenga acceso permanente o habitual a datos personales.

3. La autoridad de protección de datos podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y la autoridad de control en relación con las normas corporativas vinculantes según lo dispuesto en el presente artículo.

Parágrafo primero. Las Normas Corporativas Vinculantes sólo podrán ser sometidas a la aprobación de la autoridad de protección de datos una vez hayan sido aprobadas por el órgano correspondiente según los estatutos de la sociedad o los acuerdos del grupo empresarial. Las normas que sean formalmente presentadas ante la autoridad de protección de datos sólo estarán vigentes a partir de la fecha en que ésta emita su certificación y a partir de ese momento, se podrán aplicar.

Parágrafo segundo. En los casos en que las normas no sean aprobadas, los ajustes requeridos por la autoridad de protección de datos, una vez realizados, deben contar con la aprobación del órgano social o contractual correspondiente, antes de ser sometidas, nuevamente, a aprobación.

Artículo 51. ***Excepciones para situaciones específicas.***

1. En ausencia de una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, una transferencia o conjunto de transferencias de datos personales a terceros países u organizaciones internacionales sólo podrá realizarse si se cumplen alguna de las siguientes condiciones:

a) El titular haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos de dichas transferencias debido a la ausencia de una declaración de nivel adecuado de protección y de garantías adecuadas.

b) La transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del titular.

c) La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del titular, entre el responsable del tratamiento y otra persona natural o jurídica.

d) La transferencia sea necesaria por razones importantes de interés público.

e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones judiciales o administrativas.

f) La transferencia sea necesaria para proteger los intereses vitales del titular o de otras personas, cuando el titular esté física o jurídicamente incapacitado para dar su consentimiento.

g) La transferencia se realice desde un registro público destinado a facilitar información y esté accesible para consulta por el público en general o cualquier persona con un interés legítimo, siempre que se cumplan las condiciones establecidas por la ley para dicha consulta en cada caso particular. En tal situación, la transferencia no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro público. Si la finalidad del registro es la consulta por parte de personas con un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

2. Cuando una transferencia no pueda basarse en una declaración de nivel adecuado de protección o de garantías adecuadas según lo establecido en la presente ley, y no se aplique ninguna de las excepciones para situaciones específicas mencionadas en el numeral primero del presente artículo, sólo podrá llevarse a cabo si se cumplen las siguientes condiciones:

a) No es repetitiva.

b) Afecta sólo a un número limitado de titulares.

c) Es necesaria para fines e intereses legítimos imperiosos perseguidos por el responsable del tratamiento, sobre los cuales no prevalecen los intereses, derechos y garantías del titular. El responsable del tratamiento informará al titular, de la transferencia y de los intereses legítimos imperiosos perseguidos.

d) El responsable del tratamiento ha evaluado los riesgos y basándose en esta evaluación ha ofrecido garantías apropiadas con respecto a la protección de datos personales

Adicionalmente, el responsable del tratamiento informará a la autoridad de protección de datos sobre la transferencia y a los titulares de los intereses legítimos imperiosos perseguidos con dicha transferencia.

3. El numeral 1, literales a), b) y c), y el numeral 2 no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus funciones.

4. En ausencia de una declaración de nivel adecuado de protección, una normativa con rango de ley, podrá por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional.

5. El responsable o el encargado del tratamiento documentará en los registros de las actividades del tratamiento, la evaluación y las garantías apropiadas a las que se refiere el numeral 2 del presente artículo.

Artículo 52. ***Cooperación internacional en el ámbito de la protección de datos personales.***

En relación con terceros países y organizaciones internacionales, la autoridad de protección de datos tomará medidas apropiadas para:

a) Crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales.

b) Prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y garantías fundamentales.

c) Asociar a partes interesadas en la materia, a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales.

d) Promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

TÍTULO V

AUTORIDAD DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS

Artículo 53. ***Autoridad de Protección de Datos***.

1. La Superintendencia de Industria y Comercio ejercerá la función de autoridad nacional de protección de datos personales, garantizando el efectivo cumplimiento de los principios, derechos, garantías y los procedimientos establecidos en la presente ley en aras de facilitar la libre circulación de datos.

2. Sin perjuicio de lo mencionado, cuando el tratamiento de datos personales dé lugar a un comportamiento delictivo, la Fiscalía General de la Nación será la encargada de la persecución penal de dichas conductas.

3. La autoridad de protección de datos, tendrá a su cargo las funciones de inspección, vigilancia y control, las cuales se desarrollarán en cumplimiento de las facultades otorgadas en la presente ley.

4. Para el ejercicio de sus funciones, deberán tenerse en cuenta las garantías constitucionales y principios generales que regulan el actuar de la autoridad de protección de datos, garantizando en todo momento el derecho al debido proceso y demás garantías procesales.

Artículo 54. ***Funciones de la Autoridad de Protección de Datos.***

La autoridad de protección de datos, ejercerá las siguientes funciones:

a) Responder a las consultas previas realizadas por los responsables del tratamiento de conformidad con los establecido en el artículo 38.

b) Emitir, por iniciativa propia o previa solicitud, instrucciones, guías y demás instrumentos que considere necesarios sobre cualquier asunto relacionado con la protección de los datos personales.

c) Emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 44 de la presente ley.

d) Aprobar criterios de certificación.

e) Aprobar las Cláusulas contractuales modelo contempladas en el artículo 49, numeral 2, literal c).

f) Aprobar normas corporativas vinculantes de conformidad con el artículo 50.

g) Autorizar las cláusulas contractuales de las que trata el artículo 49, numeral 3, literal a).

h) Autorizar los acuerdos administrativos entre las entidades u organismos públicos de conformidad con el artículo 49, numeral 3, literal b).

i) Impartir instrucciones a los responsables y encargados del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones.

j) Llevar a cabo visitas de inspección, de oficio o a solicitud de parte.

k) Llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 45 de la presente ley.

l) Requerir a los responsables y encargados del tratamiento sobre presuntas infracciones a la presente ley.

m) Obtener de los responsables y encargados del tratamiento el acceso a toda la información necesaria para el ejercicio de sus funciones, así como el acceso a todas las instalaciones, incluidos equipos y medios de tratamiento de datos, respetando el debido proceso y la confidencialidad que ello requiere de acuerdo con la normativa vigente.

n) Impartir instrucciones a los responsables y encargados del tratamiento cuando las operaciones de tratamiento infrinjan lo dispuesto en la presente ley.

o) Imponer multas de carácter personal o institucional a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido lo establecido en la presente ley.

p) Imponer una limitación temporal o definitiva del tratamiento, como resultado de una sanción o de una orden administrativa a los sujetos obligados, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido la presente ley.

q) Impartir instrucciones a los responsables y encargados del tratamiento que atiendan las solicitudes de ejercicio de los derechos de los titulares en virtud de los artículos 18 al 27 de la presente ley.

r) Impartir instrucciones al responsable del tratamiento para que comunique a los titulares, los incidentes de seguridad de los datos personales.

s) Impartir instrucciones para garantizar el pleno y efectivo ejercicio de los derechos de rectificación, supresión o limitación del tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales.

t) Impartir instrucciones al organismo de certificación para que retire o que no emita una certificación con arreglo al artículo 45, si no se cumplen o dejan de cumplirse los requisitos para ello.

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

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

TÍTULO VI

DISPOSICIONES RELATIVAS A SITUACIONES ESPECÍFICAS DE TRATAMIENTO

CAPÍTULO I

Tratamientos de documentos públicos

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

1. El responsable y encargado del tratamiento implantarán las medidas técnicas y organizativas en atención al riesgo para evitar la circulación no autorizada de reproducciones digitales, copias o fotocopias de la cédula de ciudadanía, como documento que contiene datos de carácter personal, teniendo en cuenta, entre otros, los siguientes criterios:

a) Implementarán procedimientos de trazabilidad al interior de la organización, para evitar que se realicen copias no autorizadas de la cédula de ciudadanía entregada por los titulares. El titular podrá hacer uso de sellos, leyendas o firmas que determinen las condiciones de tiempo, modo, lugar y la finalidad con la que entrega la copia de su cédula de ciudadanía.

b) Si no existe una base jurídica que legitime el tratamiento de los datos sensibles contenidos en la cédula de ciudadanía, deberá evitarse su captura o implementar técnicas de anonimización sobre los datos sensibles.

c) Exclusivamente el personal autorizado podrá tener acceso a los lugares y/o activos de información donde se archiven las copias de la cédula de ciudadanía.

d) Aquellas copias de cédulas de ciudadanía que se hubiesen recabado exclusivamente para la realización de trabajos temporales deberán cumplir, entre otras, las medidas de seguridad de conformidad con el artículo 35 y ser borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su tratamiento.

e) Mientras la cédula de ciudadanía no se encuentre archivada en los dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser tratada por terceros no autorizados.

2. Si para efectos de identificación, el titular no facilitó su cédula de ciudadanía para las operaciones de tratamiento llevadas a cabo por el responsable, en caso de ejercicio de los derechos contemplados en esta ley, utilizará el método de identificación previsto al momento de la recolección de los datos personales del titular, y sólo en caso excepcional y motivado, podrá requerirles para que el titular se identifique.

3. Cuando sea necesaria la publicación de un acto administrativo que contenga datos personales del titular, incluyendo su cédula de ciudadanía, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de la cédula de ciudadanía, cédula de extranjería, pasaporte o documento equivalente o cualquier otro mecanismo de seudonimización.

Parágrafo. Lo contemplado en el presente artículo aplicará en igual medida para cédula de

extranjería, pasaporte o documento de identificación equivalente presentado por el titular.

CAPÍTULO II

Neurodatos

Artículo 56. ***Tratamiento de neurodatos.***

El responsable, o en su caso el encargado que traten neurodatos, deberán garantizar la protección de los derechos y garantías fundamentales relacionadas con la protección de los datos personales y la intimidad de las personas, por lo que se establecen las siguientes obligaciones:

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

Artículo 57. ***Tecnologías de rastreo.***

1. Es necesario obtener el consentimiento del titular para utilizar tecnologías de rastreo. Las opciones de aceptar o rechazar deben presentarse de manera destacada y equitativa, sin que rechazar sea más complicado que aceptar. No se considerará acción afirmativa utilizar los servicios sin manifestar la aceptación o el rechazo de las tecnologías de rastreo.
2. Las tecnologías de rastreo técnicamente necesarias o esenciales, que son indispensables para el funcionamiento adecuado y para proporcionar los servicios solicitados por el titular, están exentas del requisito de obtener el consentimiento.
3. Las tecnologías consideradas técnicamente necesarias cumplen con los siguientes criterios:

a) Son temporales y se eliminan al finalizar la sesión. Se utilizan para mantener la sesión del titular, establecer parámetros libremente elegidos por éste y permitir el acceso a ciertas funcionalidades.

b) Se utilizan para recordar los artículos agregados al carrito de compras, durante una sesión de compra en línea.

c) Se utilizan para mantener la sesión activa y autenticar al titular mientras navega por la plataforma.

d) Se utilizan para garantizar la seguridad de las interacciones detectando actividades potencialmente maliciosas o no autorizadas.

e) No podrán ser usadas para otras finalidades ni para elaborar perfiles de los titulares. En caso de que no cumplan esta función, se deberá informar al usuario y darle la opción de rechazarlas.

4. Las tecnologías de rastreo técnicamente necesarias no deben recopilar información personal más allá de lo estrictamente necesario para el funcionamiento del servicio y deben usarse exclusivamente con fines técnicos.

TÍTULO VII

INDEMNIZACIÓN Y RÉGIMEN SANCIONATORIO

CAPÍTULO I

Disposiciones generales y graduación de las sanciones

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

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

los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el numeral 2.

6. La autoridad de protección de datos será competente para conocer y decidir sobre la acción descrita en el presente artículo por el incumplimiento de las obligaciones de la presente ley, sin perjuicio del derecho que tiene el titular de acceder a la administración de justicia.

Artículo 59. ***Sujetos responsables*****.**

Están sujetos al régimen sancionador establecido en la presente ley:

1. Los responsables del tratamiento, así como los corresponsables en la medida que su participación en la operación de tratamiento fuera determinante en la infracción.
2. Los encargados del tratamiento.
3. Las entidades de certificación.
4. Las entidades acreditadas de supervisión de los códigos de conducta.

Parágrafo. No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este título.

Artículo 60. ***Condiciones generales para la imposición de sanciones.***

1. La autoridad de protección de datos, garantizará que la imposición de las sanciones con arreglo al presente título por las infracciones a los deberes y obligaciones contemplados en la presente ley, sean en cada caso individual efectivas, proporcionadas y correctivas. En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Administrativo y de lo Contencioso Administrativo.
2. Las sanciones se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 54. Al decidir la imposición de la sanción y su cuantía se graduarán atendiendo los siguientes criterios que resulten aplicables:

a) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta el alcance o propósito de la operación de tratamiento de que se trate, así como, el número de titulares afectados y el daño o peligro generado a los intereses jurídicos tutelados en la presente ley.

b) El alcance continuado de la infracción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

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

d) Los beneficios obtenidos por el infractor o terceros, en virtud de la comisión de la infracción.

e) El grado de responsabilidad del infractor, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud del artículo 35.

f) La reincidencia en la comisión de la infracción.

g) La resistencia, negativa u obstrucción a las labores de inspección o de vigilancia de la Autoridad de protección de datos.

h) La afectación a los derechos de los niñas, niños y adolescentes.

i) El incumplimiento de las instrucciones impartidas en virtud del artículo 54, cuando hayan sido ordenadas previamente contra el infractor en relación con el mismo asunto.

j) La renuencia o desacato a cumplir las instrucciones impartidas por la autoridad de protección de datos.

k) Si las infracciones fueron realizadas con el propósito de cometer alguna conducta tipificada como delito por la ley.

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

m) El grado de cooperación con la autoridad de protección de datos, con el fin de contener y mitigar los posibles efectos adversos de la infracción.

n) La posibilidad de que la conducta del titular hubiera podido inducir a la comisión de la infracción.

o) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

p) La forma en que la autoridad de protección de datos tuvo conocimiento de la infracción, en particular si el infractor notificó la infracción y, en tal caso, en qué medida.

q) La adhesión a códigos de conducta en virtud del artículo 42 o a mecanismos de certificación aprobados de conformidad con el artículo 45.

r) Disponer, cuando no fuere obligatorio, de un Oficial de protección de datos.

s) El reconocimiento o aceptación expresos que haga el infractor sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

t) El sometimiento por parte del infractor, con carácter voluntario, a mecanismos de resolución alternativa de conflictos,

en aquellos supuestos en los que existan controversias entre aquellos y cualquier titular o interesado.

u) Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso.

3. Si la autoridad de protección de datos detecta un posible incumplimiento de las disposiciones de la presente ley por parte de una entidad pública, remitirá la actuación a la Procuraduría General de la Nación para que la procuraduría delegada competente realice la investigación correspondiente.

4. El ejercicio por la autoridad de protección de datos de sus funciones en virtud del presente artículo estará sujeto a las garantías del debido proceso.

CAPÍTULO II

De las infracciones en materia de protección de datos

Artículo 61. ***Infracciones.***

Constituyen infracciones los actos y conductas que resulten contrarios a la aplicación de los principios y obligaciones de la presente ley.

CAPÍTULO III

De la imposición de sanciones

Artículo 62. ***Sanciones.***

La autoridad de protección de datos podrá imponer a los infractores las siguientes sanciones:

1. Multas de carácter personal e institucional hasta por el equivalente de cuatro mil (4.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción; o, hasta el cinco por ciento (5%) de los ingresos operacionales del infractor en el año fiscal inmediatamente anterior al de la imposición de la sanción.

2. Sanciones operativas y medidas correctivas.

a) Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán las medidas correctivas que se deberán adoptar.

b) Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la autoridad de protección de datos.

c) Cierre inmediato y definitivo de las operaciones relacionadas con el tratamiento ilícito de Datos Sensibles.

d) Las medidas correctivas serán establecidas por la autoridad de protección de datos, de acuerdo a las facultades otorgadas por el artículo 54, dependiendo de cada caso individual y serán independientes de la imposición de multas.

TÍTULO VIII

RÉGIMEN DE TRANSICIÓN

Artículo 63. ***Condiciones del consentimiento.***

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

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

a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento previo y expreso.

b) Que, habiéndo obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

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

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

1. Respecto de los tratamientos que existieran al momento de la entrada en vigencia de la presente ley se llevará a cabo de la siguiente manera:

a) En el plazo máximo de dieciocho meses desde su entrada en vigencia, deberán implantarse las medidas de seguridad en los tratamientos automatizados.

b) Respecto de los tratamientos no automatizados que existieran al momento de la entrada en vigencia de la presente ley, en el plazo máximo de un año.

2. Los tratamientos, tanto automatizadas como no automatizadas, creadas con posterioridad a la fecha de entrada en vigencia de la presente ley deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en esta ley.

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

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

Las solicitudes para el ejercicio de los derechos que hayan sido efectuadas con anterioridad a la

entrada en vigencia de la presente ley, su contestación se regirá por la Ley 1581 de 2012.

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

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

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

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

Artículo 67. ***Transferencias internacionales.***

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

Artículo 68. ***Régimen sancionatorio.***

1. El Régimen Sancionatorio contemplado en el Título VII entrará en aplicación a los 2 años de entrada en vigencia de la presente ley. La autoridad de protección de datos impondrá a los responsables y Encargados del Tratamiento las sanciones descritas en la Ley 1581 de 2012, señalando de forma paralela el equivalente de la infracción y su respectiva sanción en el Régimen Sancionatorio aprobado por la presente ley.
2. De conformidad con las facultades constitucionales que le han sido otorgadas a la Procuraduría General de la Nación, esta deberá asignar en el término de 18 meses con posterioridad a la entrada en vigencia de la presente ley, las funciones y competencias a una procuraduría delegada que será seleccionada o creada atendiendo a los criterios de especialidad por el incumplimiento a las disposiciones establecidas en la presente ley.

Artículo 69. ***Registro nacional de bases de datos (RNBD).***

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

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

Artículo 70. ***Entidades certificadoras***

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

Artículo 71. ***Vigencia y derogatorias***

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

De las y los Congresistas,

MARÍA FERNANDA CARRASCAL ROJAS
Representante a la Cámara por Bogotá

DUVALIER SÁNCHEZ ARANGO
Representante a la Cámara por Valle del Cauca - Alianza Verde

LUIS DAVID SUAREZ CHADID
Representante a la Cámara por Sucre
Partido Conservador

JUAN CAMILO LONDOÑO BARRERA
Representante a la Cámara por Antioquia
Partido Alianza Verde

ANA CAROLINA ESPITIA JEREZ
Senadora de la República

MARÍA DEL MAR PIZARRO GARCÍA
Representante a la Cámara por Bogotá
Partido Colombia Humana

SANTIAGO OSORIO MARIN
Representante a la Cámara
Coalición Alianza Verde - Pacto Histórico

ALEJANDRO GARCÍA RÍOS
Representante a la Cámara por Risaralda
Partido Alianza Verde

JHON FREDI VALENCIA CAICEDO
Representante a la Cámara
Citrep No. 11 Ptyo

CRISTÓBAL CAICEDO ANGULO
Representante a la Cámara por Valle del Cauca
- Pacto Histórico

HECTOR DAVID CHAPARRO
Representante a la Cámara
Partido Liberal

CRISTIAN DANILO AVENDAÑO FINO
Representante a la Cámara por Santander
Partido Alianza Verde

PABLO CATATUMBO TORRES VICTORIA
Senador de la República

EXPOSICIÓN DE MOTIVOS

PROYECTO DE LEY ESTATUTARIA NÚMERO 152 DE 2024

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

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

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

1. Objeto del Proyecto de Ley

La presente ley establece las normas relativas a la protección de las personas naturales en lo que respecta a la protección y tratamiento de sus datos personales y las normas relativas a la libre circulación de tales datos. Así mismo, protege los derechos y garantías fundamentales de las personas naturales y, en particular, su derecho fundamental a la protección de los datos personales, en los términos descritos en los artículos 15 y 20 de la Constitución Política.

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

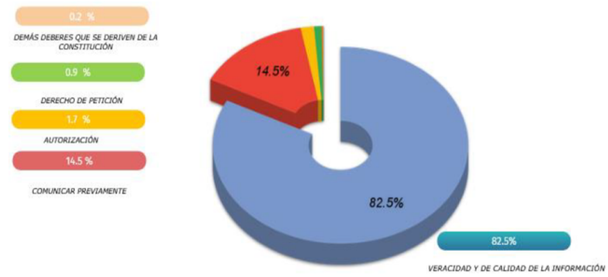
Tabla 2. Quejas presentadas durante (2013-2023 parcial)

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

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

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

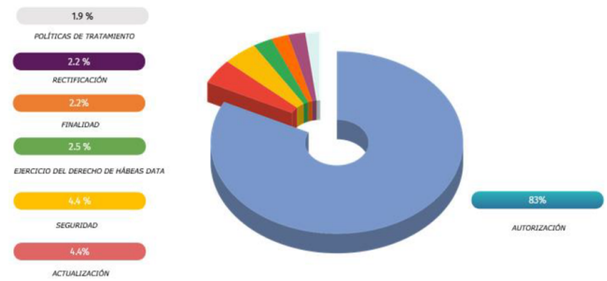
Imagen 1. Número de quejas



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

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

Imagen 2. Número de quejas



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

3. Antecedentes

Sea lo primero señalar que este proyecto de ley estatutaria fue radicada en la Legislatura 2023-2024 con el número de radicado Proyecto Ley 156 de 2023 Cámara. No obstante, no logró cumplir su trámite, pero fue un buen escenario para realizar espacios de diálogo ciudadano que conllevaron a las modificaciones realizadas al articulado propuesto y a incluir cada una de las recomendaciones dadas tanto por la Superintendencia de Industria y Comercio (SIC) como de otras entidades, academia, organizaciones de la sociedad civil y ciudadanos que participaron en la audiencia pública y espacios de trabajo desarrollados.

Esta iniciativa legislativa fue suscrita por: honorable Representante María Fernanda Carrascal Rojas, honorable Representante Duvalier Sánchez Arango, honorable Representante Héctor David Chaparro Chaparro, honorable Representante Juan Camilo Londoño Barrera, honorable Representante Juan Carlos Vargas Soler, honorable Representante John Jairo González Agudelo, honorable Representante James Hermenegildo Mosquera Torres, honorable Representante Norman David Bañol Álvarez, honorable Representante Leider Alexandra Vásquez Ochoa, honorable Representante Erick Adrián Velasco Burbano, honorable Representante David Alejandro Toro Ramírez,

honorable Representante Diela Liliana Benavides Solarte, honorable Representante Agmeth José Escaf Tijerino, honorable Representante María del Mar Pizarro García, honorable Representante Germán José Gómez López, honorable Representante Santiago Osorio Marín, honorable Representante Carlos Felipe Quintero Ovalle, honorable Representante Alejandro García Ríos, honorable Representante Germán Rogelio Rozo Anís, honorable Representante Juan Carlos Wills Ospina, honorable Representante Andrés David Calle Aguas y honorable Representante Karen Juliana López Salazar.

Para fortalecer esta iniciativa legislativa se realizaron diversos espacios de participación ciudadana que permitieron realizar ajustes y construir un articulado consensuado que atienda a las necesidad y exigencias de un mundo cada vez más conectado por medios virtuales y en el que la información es de gran valor.

Uno de los mayores espacios de participación, 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, 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 Aleida Legaltech Colombia, quienes han sido apoyo fundamental en la construcción de la iniciativa legislativa y en su ponencia.

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

4. Justificación de las Disposiciones del Proyecto de ley

4.1. Necesidad de actualizar la normatividad actual

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

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

Además, este proyecto de ley propone un enfoque acorde con el entorno digital actual, que se caracteriza por los avances tecnológicos y la creciente interconectividad. Basado en la gestión de riesgos para la protección de datos, busca que las organizaciones y entidades responsables del tratamiento de datos personales evalúen los posibles riesgos para la privacidad de los titulares y tomen medidas proporcionales para mitigarlos. De esta manera, se promueve una cultura de responsabilidad y se garantiza la implementación de medidas adecuadas para salvaguardar la información personal.

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

4.1.1. Del Objeto, ámbito de aplicación y definiciones

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

En lo que respecta al ámbito de aplicación este proyecto de ley centra su atención en el titular cuyos datos van a ser tratados, mientras que la normatividad actual coloca el foco en las personas jurídicas que los tratarán. Adicionalmente, se corrige la exclusión de las bases de datos reguladas por leyes específicas (Ley 1266 de 2008 y Ley 79 de 1993) que se encontraba en la Ley 1581 de 2012. De igual manera, se hace una distinción entre el ámbito de aplicación material y el 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.
- Autoridad de control.
- Base de datos de riesgo crediticio.
- Bloqueo de datos.
- Cesión o comunicación de datos.
- Datos biométricos.
- Datos genéticos.
- Datos relativos a la salud.
- Denuncia.
- Destinatario o tercero.
- Elaboración de perfiles.
- Encargado del tratamiento.
- Grupo empresarial.
- Incidente de seguridad.
- Limitación del tratamiento.
- Neurodatos.
- Organización internacional.
- Queja.
- Responsable del tratamiento.
- Servicio de la sociedad de la información.
- Seudonimización.
- Tecnología de rastreo.
- Transferencia internacional de datos personales.
- Tratamiento a gran escala.

4.1.2. Principios aplicables a la protección de datos

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

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

En ese sentido, se introducen los principios de lealtad, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad, proporcionalidad, responsabilidad demostrada y neutralidad tecnológica. Estos principios adicionales en el artículo 6° 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.

Finalmente, se enfatiza en la responsabilidad del responsable del tratamiento en demostrar el cumplimiento de la normativa. En resumen, el artículo 6° 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 los datos de las personas fallecidas.

Frente a esta importante materia, el proyecto de ley determina que los Datos de Carácter personal que identifican a una persona natural, cuando la persona fallece su estado civil se considera extinguido porque la muerte pone fin a su existencia legal, en consecuencia, ya no existe el concepto del dato como el de un dato personal. No obstante, en aras de garantizar la protección de la memoria del fallecido y el impacto que esto puede tener en la intimidad de los causahabientes, se disponen medidas para el tratamiento de esta información.

Este aspecto es innovador, puesto que este escenario no está previsto en la actual legislación colombiana, pues, se permite que los causahabientes, personas o instituciones que la persona fallecida hubiera designado expresamente para ello, puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso, con sujeción a las instrucciones del fallecido. No obstante, la determinación de los requisitos y condiciones para acreditar la validez y vigencia a estas autorizaciones queda supeditada a la Superintendencia de Industria y Comercio. Asimismo, se establecen especialidades en relación con los menores, personas discapacitadas y fallecidas respecto de las facultades que tienen los representantes legales para poder garantizar la protección de lo establecido en el artículo 15 de la Constitución Política, el control sobre los datos personales que de ellos se tratan y la autodeterminación informática.

Esta regulación es crucial para preservar su privacidad, dignidad y memoria, proteger a sus familiares, salvaguardar la privacidad de terceros y fomentar la transparencia y responsabilidad histórica. Garantizar este derecho evita un uso indebido de la información personal, permite a los familiares manejar asuntos legales y honrar la memoria de sus seres queridos, y protege la privacidad de aquellos relacionados con los fallecidos. Además, facilita investigaciones históricas y enriquece el conocimiento colectivo.

4.1.4. 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.

4.1.4.1. 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.

4.1.4.2. 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.

4.1.4.3. Con base en un interés vital

El tratamiento con base en el interés vital encuentra su fundamentación 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.

4.1.4.4. 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.

4.1.5. 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.

De otra parte, el tratamiento de los relativos a delitos y condenas penales, debe ser lícito y basarse en una de las bases legitimadoras establecidas en esta disposición y estar sujeto a la supervisión de una autoridad pública competente para garantizar la protección adecuada de los derechos y garantías de los titulares de los datos.

En cuanto a las infracciones administrativas, se debe llevar a cabo un tratamiento de datos por parte del organismo competente. Este tratamiento debe limitarse a los datos estrictamente necesarios con el objetivo de salvaguardar los derechos y libertades de los titulares, así como garantizar la seguridad jurídica en el proceso.

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. Tratamiento de datos en tecnologías avanzadas, neuroderechos y herramientas de seguimiento en línea

La acelerada innovación tecnológica de la última década ha generado la necesidad de analizar y ajustar los marcos normativos de los países con el fin de regular las nuevas tecnologías. En particular, las tecnologías pertenecientes a la llamada revolución industrial 4.0 se han vuelto cada vez más invasivas en términos de privacidad. La recopilación y el uso de grandes cantidades de datos personales se han convertido en elementos fundamentales para el funcionamiento de estas tecnologías como las Inteligencias Artificiales (IA), lo que ha llevado a la urgente necesidad de establecer regulaciones al respecto.

En este contexto, Colombia no puede quedarse rezagada en este ámbito. La protección de datos en el contexto de las inteligencias artificiales se ha vuelto una preocupación prioritaria, dado que el rápido avance tecnológico ha permitido la creación y aplicación de algoritmos y redes neuronales cada vez más sofisticadas y poderosas. Estas redes neuronales y algoritmos son capaces de analizar, interpretar y utilizar grandes volúmenes de datos personales de forma automatizada, lo que plantea desafíos significativos en términos de privacidad y seguridad.

4.2.1. Tratamiento de neurodatos

Los grandes avances en tecnología no solo traen retos para proteger la privacidad de redes neuronales artificiales, sino que también se hace necesario proteger la información de nuestro cerebro mediante la introducción de normativas que brinden una protección reforzada a los "neurodatos". Pero ¿Qué son los neurodatos? De acuerdo con la Unidad de Tecnología y Privacidad del Supervisor Europeo de Protección de Datos (SEPD) y la Agencia Española de Protección de Datos[1], pueden definirse *como la información que se recoge del cerebro y/o del sistema nervioso.*

Es importante considerar que los neurodatos suelen ser recopilados de personas identificadas. A veces, estas personas se identifican a sí mismas (por ejemplo, en aplicaciones de entretenimiento), mientras que otras veces, quienes gestionan los sensores de recolección de datos son quienes las identifican (como en aplicaciones de salud). Incluso si la persona no se identifica durante la recolección de neurodatos, aún puede ser identificada, ya que hay evidencia que demuestra que los neurodatos pueden identificar de manera única a las personas[2].

[1] Unidad de Tecnología y Privacidad del Supervisor Europeo de Protección de Datos (SEPD) Agencia Española de Protección de Datos, (2024). Neurodatos (Informe EDPS TechDispatch 2024-1). TechDispatch. https://www.edps.europa.eu/system/files/2024-06/techdispatch_neurodatos_es_0.pdf

[2] T. Nakamura, V. Goverdovsky and D. P. Mandic, "In-Ear EEG Biometrics for Feasible and Readily Collectable Real-World Person Authentication," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 648-661, March 2018, doi: 10.1109/TIFS.2017.2763124

Por lo tanto, los neurodatos de los seres humanos son datos personales.

La recopilación de los neurodatos suele hacerse a través de una gran variedad de métodos e instrumentos que interactúan con el cerebro y el sistema nervioso en general, ya sea de modo pasivo *–monitorizando la actividad cerebral–* o de modo activo *–alterando tal actividad-*.

El diario El País de España nos ilustra de la siguiente manera:

"Los grandes avances actuales en las ciencias del cerebro permiten la posibilidad de analizar, registrar, alterar y/o manipular la actividad del cerebro. Esto es lo que científicamente se conoce como 'neuromodulación'. Si además se incluyen los avances en sistemas y microcircuitos, surge la neurotecnología que, junto con la Inteligencia Artificial, ha demostrado que es posible acceder a parte de la información almacenada en el cerebro e incluso leer y escribir la actividad cerebral de las personas. Esto supone una revolución en el campo de la Neurociencia y abre un nuevo horizonte por desarrollar para las compañías e instituciones". (Calderón, R.A. 2021).

Entonces, esa barrera que se rompió con las neurotecnologías para obtener acceso a los neurodatos debe ser regulada de manera que se protejan nuestros derechos y libertades

Las garantías de los derechos a la intimidad y protección de datos en el tratamiento de los neurodatos son importantes por varias razones:

- Autonomía y libre albedrío: La neurotecnología puede tener el potencial de influir en la actividad cerebral y la toma de decisiones de las personas. Regular la privacidad y protección de datos garantiza que las personas conserven su capacidad de autonomía y libre albedrío, evitando cualquier forma de manipulación o interferencia no consentida.
- Integridad y privacidad mental: La actividad cerebral contiene información íntima y personal que revela aspectos de la vida privada y el pensamiento de una persona. Al regular la privacidad y protección de datos en el uso de la neurotecnología, se salvaguarda la integridad y privacidad mental de los individuos, protegiéndolos de posibles abusos o violaciones de su esfera personal.
- Consentimiento informado: La regulación de la privacidad y protección de datos garantiza que el uso de neurotecnologías esté respaldado por un consentimiento informado y explícito por parte de las personas involucradas. Esto implica que los individuos deben ser plenamente conscientes de los procedimientos de medición de la actividad cerebral, los riesgos potenciales y los derechos que les asisten.
- Discriminación y sesgos: El uso de neurotecnologías puede recopilar datos sensibles y revelar información que podría ser utilizada para generar sesgos o discriminación. La regulación adecuada puede establecer medidas para prevenir y abordar la discriminación basada en el pensamiento o cualquier otro factor obtenido a través de las neurotecnologías, protegiendo los derechos fundamentales de las personas.
- Acceso equitativo y desigualdad: La regulación en este ámbito puede contribuir a garantizar que las neurotecnologías estén disponibles y sean accesibles para toda la población, evitando la generación de disparidades en el acceso y uso de estas tecnologías. Esto ayuda a prevenir la creación de brechas y desigualdades sociales.

Por consecuencia en el artículo que se propone en el presente proyecto de ley se establece un marco legal que protege los derechos de las personas en el uso de sus neurodatos, garantizando su identidad personal, libre albedrío, privacidad mental, acceso equitativo y protección contra sesgos.

4.2.2. Tecnologías de rastreo

Asimismo, este proyecto de ley busca introducir en Colombia una regulación sobre tecnologías de rastreo como, por ejemplo, las *cookies*. En primer lugar, aseguraría una protección adecuada de la privacidad de los usuarios al establecer salvaguardias y restricciones claras para el manejo de información personal recopilada a través de estas tecnologías. Esto permitiría prevenir abusos y garantizar el control sobre los datos sensibles revelados mediante el seguimiento de hábitos de navegación y preferencias.

En segundo lugar, la regulación específica requeriría el consentimiento informado de los usuarios antes de utilizar tecnologías de rastreo, lo cual sería esencial para otorgarles el poder de decisión sobre el uso de sus datos personales. Además, se promovería la transparencia y responsabilidad por parte de las organizaciones al exigirles brindar información clara sobre sus prácticas, estableciendo así una relación de confianza entre usuarios y empresas.

Finalmente, la regulación alineará a Colombia con los estándares internacionales de protección de datos. Esto facilita la interoperabilidad y el intercambio de datos con otros países, promoviendo la coherencia en la protección de la privacidad en el entorno digital y brindando a los ciudadanos colombianos una mayor garantía de sus derechos en un contexto globalmente conectado.

4.3. 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.

Una contribución importante del proyecto de ley es que define el aviso de privacidad como información de primera capa, que consiste en proporcionar al titular la información básica sobre el tratamiento de sus datos y permitir el acceso fácil e inmediato al resto de la información a través de una dirección electrónica u otro medio. La información básica incluirá la identidad del responsable del tratamiento y su representante legal, la finalidad del tratamiento y los derechos que pueden ejercer los titulares. Lo anterior, con el fin de aligerar las cargas administrativas que recaen sobre los ciudadanos. Sin embargo, este derecho no sería absoluto y se establece que el responsable del tratamiento puede cobrar al titular los gastos administrativos por proporcionar información o realizar acciones solicitadas si las solicitudes son carentes de fundamento legal, temerarias y/o excesivas. También se menciona la posibilidad de negarse a actuar respecto a solicitudes consideradas temerarias y reiterativas.

Finalmente, la nueva disposición permite al responsable del tratamiento solicitar información adicional al titular para confirmar su identidad en caso de tener dudas razonables al respecto. Así como 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.

4.4. 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 el Capítulo II de 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.

4.4.1. 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, y además se

especifica una serie de información que el titular tiene derecho a conocer relacionada con el tratamiento de sus datos personales, así como a solicitar una copia de los datos personales objeto de tratamiento, y el responsable del tratamiento podrá cobrar gastos administrativos por copias adicionales. 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. Además, este derecho no se encuentra recogido en un único artículo, lo que dificulta aún más que el interesado conozca y ejerza su derecho.

4.4.1.1. 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.

La Ley 1581 del 2012 no proporciona disposiciones específicas sobre el derecho de rectificación en medios de comunicación. Es importante destacar el derecho de rectificación en este ámbito ya qué el acceso a una rectificación justa y oportuna es fundamental cuando se trata de información publicada en medios, porque permite a los individuos corregir datos inexactos o erróneos que puedan afectar su reputación y privacidad. La rectificación garantiza que las personas tengan la oportunidad de refutar información incorrecta y asegura que los medios de comunicación sean responsables en la difusión de información precisa y veraz. Este derecho protege la reputación y privacidad de los individuos, promoviendo así un equilibrio entre la libertad de expresión y el derecho a la rectificación en el ámbito de los medios de comunicación.

4.4.1.2. Derecho de supresión

Aunque la Ley 1581 de 2012 reconoce el derecho de supresión de datos personales, existen vacíos y falta de claridad en cuanto a los casos en los que se puede ejercer este derecho y la forma de hacerlo. Asimismo, no aborda adecuadamente la problemática del derecho al olvido en el entorno digital y las redes sociales.

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 artículo 27 de este 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.

Además, el artículo establece la obligación del responsable del tratamiento de adoptar medidas razonables para informar a los destinatarios o terceros que estén tratando los datos personales sobre la solicitud de supresión realizada por el titular. Esto busca garantizar que, una vez suprimidos los datos, no se sigan difundiendo o utilizando de manera

indebida. Estas medidas técnicas y de divulgación contribuyen a asegurar la efectividad del derecho de supresión y a proteger la privacidad de los titulares.

No obstante, se establecen excepciones al derecho de supresión en casos en los que existan derechos o intereses legítimos que prevalezcan sobre este derecho, como el ejercicio de la libertad de expresión e información, el cumplimiento de obligaciones legales o el interés público en áreas como la salud pública, la investigación científica o las estadísticas. Estas excepciones buscan encontrar un equilibrio entre el derecho al olvido y otros derechos fundamentales, evitando que su ejercicio obstaculice el cumplimiento de objetivos legítimos y el desarrollo de la sociedad en general.

En Colombia el derecho al olvido no cuenta con una regulación como tal que lo defina y establezca las condiciones para acceder a él, por eso la inclusión del artículo 28 del presente proyecto de ley que establece el derecho al olvido en búsquedas de Internet, en el Régimen de Protección de Datos de Colombia sería fundamental para garantizar el control y la privacidad de los titulares sobre su información personal en el entorno digital. En la era de la información en línea, es crucial que los individuos tengan la capacidad de gestionar la visibilidad de su información personal y proteger su reputación.

El Régimen de Protección de Datos de Colombia fortalecería la protección de la privacidad y el control de los titulares sobre su información personal en el contexto de las búsquedas en Internet. Permite a los titulares solicitar la eliminación de enlaces que contengan información inadecuada o irrelevante, considerando factores relevantes como el tiempo transcurrido y el interés público. Al mismo tiempo, garantiza que el acceso a la información no se vea limitado a través de otros criterios de búsqueda. En conjunto, estas disposiciones promueven el derecho a la privacidad y la gestión adecuada de la información personal en el entorno digital en constante evolución.

Según Ramírez (2023) de acuerdo al estudio Digital 2023 realizado por Hootsuite y We Are Social, en Colombia son aproximadamente 38.45 millones de personas que usan redes sociales, lo que representa un 74% de la población, aunque las cifras representan un decrecimiento del 3.35% del año anterior sigue siendo un número elevado.Es por eso que no hay que dejar por fuera el derecho al olvido en las redes sociales, pues en tiempos que las personas comienzan a tener más conciencia sobre su privacidad y la protección de sus datos personales, muchos buscan apagar algunas redes sociales y se hace necesario garantizar el derecho al olvido en estas redes.

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.

4.4.1.3. 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.

4.4.2. 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.

4.4.3. 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 el artículo 33 que se presenta 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 del artículo 34 en el presente 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 artículo 34 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.

4.4.4. Derecho a la queja

Esta disposición en el artículo 35 del 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, el artículo 36 establece 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.

4.5. Del responsable del tratamiento

4.5.1. 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.

4.6. 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.

4.6.1. Los problemas de seguridad en el manejo de datos

El Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales (2021), analizó las medidas de seguridad implantadas para tratar datos personales en 31.169 empresas (entre empresas y entidades públicas) del país. Este estudio refleja que tan solo el 50.7 % de las empresas que hacen parte del estudio, han implementado medidas apropiadas y efectivas para garantizar la seguridad de los datos personales, el 58 % de las organizaciones no han implementado medidas especiales para

proteger datos sensibles, y en promedio el nivel de incumplimiento de los ítems evaluados por la Superintendencia de Industria y Comercio es de 59.41%. Esto muestra una falta de preparación por parte de los sujetos obligados para garantizar la seguridad de los datos personales, una debilidad de la actual Ley 1581 de 2012 y sus normas reglamentarias para garantizar el cumplimiento de esta obligación y por ende una ausencia de capacidades por parte de las organizaciones para la gestión del riesgo en materia de Seguridad.

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

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

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

En este sentido, la Seguridad se convierte en una condición sine 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.

4.6.2. Adaptaciones requeridas

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

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

Se observa así que, el proyecto de ley introduce el concepto de Resiliencia como característica del desempeño de los servicios de tratamiento de información que puede ayudar a mejorar la seguridad (INSST, 2018). La resiliencia se manifiesta en la capacidad de anticiparse, responder y recuperarse de manera efectiva ante los desafíos y adversidades, permitiendo que el sistema de información se

mantenga robusto y operativo en todo momento, sin importar las circunstancias, característica necesaria en tiempos donde los ataques cibernéticos hacen parte del paisaje cotidiano.

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

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

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

4.7. 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, mostrandolas 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 declaración de conformidad, 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 "Conforme". En ausencia de dicha declaración, 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. En cuanto a este instrumento, pasa a ser parte integrante del nuevo cuerpo normativo en los términos ya establecidos por el Decreto número 255 de 2022.

Así mismo, esta nueva propuesta legislativa pretende dilucidar los conceptos de transferencia y transmisión establecidos en los artículos 24 y 25 del Decreto Reglamentario 1377 de 2013. Siendo la transferencia entendida como una "Cesión"[3] en *strictu sensu*, como se conoce a nivel internacional,

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

y la transmisión[4] 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 no se considera 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.

4.8. Tratamiento en el ejercicio de la libertad de expresión e información

Sin incurrir en un exceso de regulación, la normativa nacional tiene la responsabilidad de conciliar las normas que protegen tanto la libertad de expresión e información como la protección de los datos personales, por lo que su inclusión en el marco de este proyecto de ley es esencial. La libertad de expresión es un derecho fundamental reconocido en el artículo 20 de la Constitución Política de Colombia. Como tal, su preservación y cualquier intento de limitar su ejercicio debe ser considerado inconstitucional.

Según lo establecido por la Corte Constitucional en la Sentencia T-277 de 2015: *"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"*.

Es importante encontrar un equilibrio adecuado que permita garantizar la libertad de expresión e información, al mismo tiempo que se protegen los datos personales de los individuos. Esto implica considerar las disposiciones legales y constitucionales que amparan la libertad de expresión y el derecho a la información, así como de establecer medidas de protección en el tratamiento de datos personales que sean compatibles con estas garantías y libertades fundamentales y que, su aplicación no represente una restricción al pleno ejercicio de estos derechos o control sobre el contenido de la información que configure una forma de censura.

Este proyecto de ley proporciona lineamientos claros que tienen como eje central la protección de los datos personales en el ejercicio de la libertad de expresión y de información, respetando la exclusión del ámbito de aplicación de la presente propuesta legislativa a las bases de datos y archivos de información periodística y otros contenidos editoriales. Las medidas propuestas en el proyecto de ley solo consideran principios aplicados a la protección de datos con respecto al manejo de la información de los titulares, como lo son la minimización de los datos y la veracidad de los mismos, que son medidas básicas de protección que no implican ningún tipo de limitación al ejercicio pleno del derecho a la libertad de expresión e información.

4.9. Tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística

El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica, o fines estadísticos es una realidad que ha sido abordada por este proyecto de ley. Estos tipos de tratamiento fueron regulados como excepciones al tratamiento de datos sensibles

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

y a la necesidad de obtener el consentimiento para llevarlos a cabo.

El artículo 6° de la Ley 1581 de 2012 en lo que respecta al tratamiento de datos sensibles, prohíbe el tratamiento de esta tipología de datos, excepto cuando *"[...] el Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares".*

Por otro lado, el artículo 10 establece aquellos casos en los que no será necesaria la autorización del titular para el tratamiento de datos personales, centrándonos en este caso en el *"Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos."*

Sí bien este proyecto de ley reconoce estas excepciones al tratamiento de datos sensibles, es importante que existan disposiciones específicas que aborden las peculiaridades y salvaguardias necesarias para proteger la privacidad y los derechos de las personas involucradas en estos tipos de tratamiento.

El tratamiento de estos datos personales debe ser llevado a cabo con las garantías adecuadas para proteger los derechos y libertades del individuo. Estas garantías deben asegurar que se implementen medidas técnicas y organizativas que cumplan, especialmente, con el principio de minimización de datos. Cuando se realice un tratamiento posterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica, o fines estadísticos, es necesario que el responsable del tratamiento evalúe la viabilidad de alcanzar esos fines mediante un tratamiento de datos que no permita identificar a los individuos involucrados, o que ya no permita identificarlos, aplicando medidas como la anonimización de datos.

Este proyecto de ley asegura la protección de los derechos de los titulares, así como establecer especificaciones y excepciones en relación con los requisitos de información y los derechos de rectificación, supresión, olvido, limitación del tratamiento, portabilidad de los datos y oposición. Es necesario establecer condiciones y garantías que incluyan procedimientos específicos para que los titulares puedan ejercer sus derechos, siempre que sea apropiado en función de los objetivos perseguidos por el tratamiento específico, en concordancia con las medidas técnicas y organizativas para minimizar el tratamiento de datos personales, respetando los principios de proporcionalidad y necesidad. En el caso del tratamiento de datos personales con fines científicos, también se deben cumplir otras normativas relevantes, como aquellas relacionadas con los ensayos clínicos u otras regulaciones específicas aplicables.

El tratamiento de datos con fines de archivo en interés público se refiere a la conservación y preservación de información relevante para la sociedad en general, como documentos históricos o culturales. Las autoridades públicas, así como los organismos públicos o privados encargados de llevar registros de interés público, deben ser responsables de adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros que sean de valor duradero para el interés público general, y deben facilitar el acceso a dichos registros. Se debe determinar la autorización para, en relación con el tratamiento ulterior de datos personales con fines de archivo, por ejemplo, ofrecer información específica relacionada con el comportamiento político en regímenes anteriores, crímenes contra la humanidad o crímenes de guerra. La autorización para el tratamiento ulterior de estos datos debe estar sujeta a una evaluación cuidadosa y considerar el interés público, los derechos de los individuos y los principios éticos y legales aplicables.

Asimismo, este proyecto de ley se aplica al tratamiento de datos personales realizado con fines de investigación científica. Se entiende que este tratamiento abarca un amplio espectro, que incluye el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, dentro de los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir con las especificidades del tratamiento de datos personales con fines de investigación científica, se deben aplicar condiciones concretas. Esto se refiere especialmente a la publicación o comunicación de datos personales en el contexto de la investigación científica. Se deben establecer salvaguardias adecuadas para garantizar la protección de la privacidad de los individuos involucrados en la investigación. Si el resultado de la investigación científica, especialmente en el ámbito de la salud, justifica la adopción de otras medidas en beneficio del titular, las disposiciones generales de este proyecto de ley deben aplicarse teniendo en cuenta dichas medidas.

El presente proyecto de ley debe aplicarse asimismo al tratamiento de datos personales que se realiza con fines de investigación histórica. Esto incluye la investigación histórica y la investigación para fines genealógicos.

Esta propuesta legislativa también se aplica al tratamiento de datos personales con fines estadísticos. Se deben implementar medidas adecuadas para proteger los derechos y las libertades de los titulares, y garantizar la confidencialidad estadística, todo ello dentro de los límites establecidos por el presente proyecto de ley. Se considera que tienen fines estadísticos cualquier operación que involucre la recopilación y el tratamiento de datos personales necesarios para llevar a cabo encuestas estadísticas o para generar resultados estadísticos. Estos resultados estadísticos también pueden ser utilizados con diversos propósitos, incluyendo la investigación científica. Es importante destacar que el fin estadístico implica que el resultado del tratamiento de datos con fines estadísticos no sea información personal identificable, sino datos

agregados. Además, tanto este resultado estadístico como los datos personales no deben ser utilizados para respaldar medidas o decisiones específicas en relación con personas naturales concretas.

4.10. Indemnización y régimen sancionatorio

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

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

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

De acuerdo con la información de la Dijin, la suplantación de identidad creció 409% en el 2020, debido a la pandemia del Covid-19 (Certicámara/ Dijin, 2020)[5]. 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 expresó, como de una institucionalidad que permita un control y ámbito de garantía efectivo del derecho a la protección de datos personales. Como resultado, en el artículo 22 de la precitada norma quedó establecida la potestad sancionatoria de la Autoridad de Protección de Datos Personales, estableciendo que aquello no reglado, seguiría lo pertinente al procedimiento sancionatorio establecido en el Código Contencioso Administrativo.

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

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

Esto no es más que la materialización del ius 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,

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

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.

4.11. Régimen de transición

El presente proyecto de ley cuenta con un régimen transitorio para garantizar una implementación ordenada y justa entre el antiguo marco legal y el nuevo.

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.

En algunos casos, ciertas situaciones pueden requerir un tratamiento especial debido a su naturaleza del tratamiento, permitiendo que se contemplen excepciones o reglas especiales para estas circunstancias específicas, asegurando una transición justa y equitativa.

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.

4.12. Otras disposiciones.

4.12.1. Autoridades de control

En el proyecto de ley se habla de los *"Poderes de la Autoridad Nacional de Protección de Datos Personales"* que clasifica las funciones de la Superintendencia de Industria y comercio en poderes consultivos, investigativos, correctivos y sancionatorios. Cada poder está relacionado con las diferentes facetas que debe poseer la Superintendencia de Industria y Comercio, por lo que, como órgano de consulta tiene la facultad de brindar orientación y asesoramiento a los sujetos obligados en los diferentes mecanismos de autorregulación; como órgano de investigación, debe tener la capacidad de recopilar información relevante en el marco de inspecciones, revisiones de certificaciones e indagaciones de presuntas infracciones al nuevo cuerpo normativo; y 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.

4.12.2. Tratamiento de documentos públicos

Es menester hacer una distinción entre información pública y el Dato Público. La primera se encuentra definida en la Ley de Transparencia y acceso a la información pública *como aquella que generan, obtienen, adquieren o controlan los sujetos obligados en función del servicio público que prestan*. Mientras que la Ley 1266 de 2008 define el dato público como aquel que *no está sujeto a reserva y que pueden estar contenidos en diversos documentos públicos, Sentencias judiciales o los relativos al estado civil de las personas*. Para efectos de un mejor entendimiento, la información pública puede contener datos que no necesariamente se consideren personales, en contraste con el dato público que es considerado una categoría de dato personal en los términos establecidos en la Ley 1266 de 2008.

4.12.3. Videovigilancia

El presente proyecto de ley recoge las disposiciones que se aplicarán a tratamientos de videovigilancia cuya licitud proviene de un interés público. Introduciendo en la normativa de protección de datos cuestiones tales como que las personas naturales o jurídicas, tanto públicas como privadas, que lleven a cabo el tratamiento de imágenes a través de sistemas de videovigilancia además de cumplir con el presente proyecto de ley, se limita a través de prohibición la captación imágenes de la vía pública salvo cuando sea necesario.

Los datos recopilados deben ser eliminados en un plazo máximo de 30 días desde su captación,

a menos que sea necesario conservarlos para demostrar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deben ponerse a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tenga conocimiento de la existencia de la grabación.

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 éstos 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."*

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

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

A su vez, el considerando 25 puntualiza que:

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

5.2. Marco jurídico nacional

5.2.1. Fundamento Constitucional

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

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

6. Fundamento Normativo

a) Ley 1581 de 2012:

Como se repetirá a lo largo del presente documento, la Ley 1581 de 2012 constituye el eje a partir del cual el ordenamiento jurídico colombiano ha establecido los elementos fundamentales para proteger los datos personales, de acuerdo al estado tecnológico y estándares internacionales existentes para la época. Entre sus características esenciales se encuentran:

- Prohíbe el tratamiento de datos de menores, requiriéndose para ello la intervención del representante legal.
- Establece que el responsable del tratamiento de datos personales debe obtener la autorización, previa, expresa e informada, del titular antes de procesar sus datos. La autorización puede ser otorgada por escrito, de forma oral o a través de conductas inequívocas.
- Establece que el responsable del tratamiento de datos personales debe solicitar autorización al titular al momento de recolectar los datos, proporcionándole información clara sobre los datos a recolectar y las finalidades específicas del tratamiento.
- Preceptúa excepciones en las cuales la autorización del titular no es necesaria:

• Cuando se trata de información requerida por una entidad pública o administrativa.

• Cuanto se trata de datos de naturaleza pública.

• Cuando hay casos de urgencia médica o sanitaria.

• Cuando se trata de tratamiento de información autorizado por ley para fines históricos, estadísticos o científicos, y datos relacionados con el Registro Civil de las personas.

- Consagra el Principio de Acceso y Circulación Restringida en virtud del cual el tratamiento de datos personales tiene los límites que se derivan de la naturaleza de los datos, las disposiciones de la ley y la Constitución. De esta forma el tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley.
- No preceptúa disposiciones específicas sobre el derecho de rectificación en medios de comunicación.
- Establece el derecho de supresión de datos personales.
- 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.
- Enumera los deberes relativos a los responsables del tratamiento de datos personales y establece las obligaciones del encargado del tratamiento.
- Contempla la seguridad como un principio fundamental.
- Prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Estableciendo como excepciones cuando se trate de:

- Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

- Reconoce como autoridad de control a la Superintendencia de Industria y Comercio a través de su Delegatura para la Protección de Datos Personales.
- Prohíbe el tratamiento de datos sensibles excepto cuando este tenga una finalidad histórica, estadística o científica, evento en el cual deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.
- Establece aquellos casos en los que no será necesaria la autorización del titular para el tratamiento de datos personales.
- Define qué se considera como dato de carácter personal: "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables". Los datos de contacto de las personas jurídicas están fuera del ámbito de aplicación de la ley.
- Establece la potestad sancionatoria de la Autoridad de Protección de Datos Personales.

b) Decreto número 1377 de 2013:

Reglamenta la Ley 1581 de 2012 y contiene los siguientes elementos principales:

- En su artículo 2° puntualiza un tipo de tratamiento excluido de la aplicación del Régimen General de Protección de Datos: los datos mantenidos en ámbitos meramente personales o domésticos; entendiendo por ámbito personal o doméstico aquellas actividades inscritas en el marco de la vida privada o familiar de las personas naturales.
- El artículo 3° preceptúa conceptos entre los cuales puntualiza la transferencia y transmisión de datos así:

"[...] 4. Transferencia: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

5. Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable [...]"

- En el Capítulo 2 del decreto se agrupan nociones frente al elemento Autorización bajos los principios que delinean el deber ser en el tratamiento de datos personales. De esta forma:

- El artículo 4° desarrolla la forma cómo debe operar la recolección de los datos de los titulares.
- El artículo 7° regula el modo de obtener la autorización en virtud del artículo 9° de la ley. De esta forma permite el tratamiento automatizado de la autorización para el tratamiento siempre y cuando se manifieste por escrito, de forma verbal o por medio de una conducta del titular que permite inferir de forma razonable su consentimiento en el tratamiento de la información. El decreto aclara que no se puede llegar a esta inferencia por vía del silencio del titular.
- El artículo 9° desarrolla la facultad del titular de revocar la autorización y por esta vía suprimir sus datos, siendo obligatorio para el responsable y/o encargado la disposición de mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión. Realizada la reclamación por parte del titular, el encargado cuenta con 15 días hábiles para proceder a la supresión so pena de ser sancionado.

- El Capítulo 3 aborda las políticas de tratamiento como documento orientador para el establecimiento de un macrosistema de aseguramiento de la información en las organizaciones, advirtiendo la necesidad de confeccionar el aviso de privacidad como herramienta para la difusión de las políticas a los titulares de los datos:

- El artículo 16 establece la obligación de conservar el modelo de aviso de privacidad.
- El artículo 19 preceptúa que, por medio de instrucciones en materia de seguridad de la información, la Superintendencia de Industria y Comercio impartirá directrices que constarán en circulares y/o resoluciones.

- El artículo 23 hace obligatoria la adopción de la función de responsable de los datos personales.
- El Capítulo 4 regula la transmisión y transferencia internacional de datos:
- El artículo 24 plantea expresamente la transmisión internacional de datos sin que sea necesario informar al titular de tal circunstancia ni contar con su autorización si entre el responsable y el encargado media un contrato.
- El artículo 25 señala que el contrato entre responsable y encargado deberá especificar las circunstancias especiales y las principales características del instrumento regulador de la relación entre el dueño de la base de datos y quien la gestiona.
- El último capítulo desarrolla el postulado de responsabilidad demostrada, que constituye el deber empresarial en el tratamiento de datos personales, siendo una demostración que se analizará a solicitud de la delegatura de protección de datos:
- El artículo 26 prescribe que la Superintendencia podrá requerir a las empresas para que suministren una descripción de sus procedimientos y evidencia de las medidas adoptadas para el aseguramiento de la información.
- El artículo 27 señala que la Superintendencia impartirá las directrices tomando como parámetros de revisión:

"[...]1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto.

2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.

3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento [...]"

c) Decreto número 767 de 2022:

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

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

6.1. Fundamento jurisprudencial:

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

Por su parte, la Sentencia **SU-082 de 1995** puntualizó los elementos que componen el Habeas Data, en los siguientes términos:

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

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

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

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

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

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

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

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

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

refiere a la seguridad y a la confidencialidad de los datos sujetos a tratamiento […].”

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

“[…]. Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no 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

7.1. 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.

7.2. 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.

7.3. 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.

7.4. Ley de Protección de Datos Personales de Brasil (LGPD):

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

7.5. 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.

7.6. Ley de Protección de Datos Personales en Argentina:

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

7.5. Ley de Protección de Datos Personales en Chile:

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

7.6. 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.

7.7. Ley de Protección de Datos Personales en Uruguay:

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

7.8. 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.

7.9. 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 dictan disposiciones para el Régimen General de Protección de Datos Personales",* para que sea tramitado, y con el apoyo de las y los Congresistas sea discutido y aprobado

De las y los Congresistas,

MARÍA FERNANDA CARRASCAL ROJAS
Representante a la Cámara por Bogotá

DUVALIER SÁNCHEZ ARANGO
Representante a la Cámara por Valle del Cauca - Alianza Verde

LUIS DAVID SUAREZ CHADID
Representante a la Cámara por Sucre
Partido Conservador

JUAN CAMILO LONDOÑO BARRERA
Representante a la Cámara por Antioquia
Partido Alianza Verde

ANA CAROLINA ESPITIA JEREZ
Senadora de la República

MARÍA DEL MAR PIZARRO GARCÍA
Representante a la Cámara por Bogotá
Partido Colombia Humana

SANTIAGO OSORIO MARIN
Representante a la Cámara
Coalición Alianza Verde - Pacto Histórico

ALEJANDRO GARCÍA RÍOS
Representante a la Cámara por Risaralda
Partido Alianza Verde

JHON FREDI VALENCIA CAICEDO
Representante a la Cámara
Citrep No. 11 Ptyo

CRISTÓBAL CAICEDO ANGULO
Representante a la Cámara por Valle del Cauca - Pacto Histórico

HÉCTOR DAVID CHAPARRO
Representante a la Cámara
Partido Liberal

CRISTIAN DANILO AVENDAÑO FINO
Representante a la Cámara por Santander
Partido Alianza Verde

PABLO CATATUMBO TORRES VICTORIA
Senador de la República

11. Referencias

- Superintendencia Financiera. Respuesta Derecho de Petición UTL Mafe Carrascal. Bogotá, D. C.
- Superintendencia de Industria y Comercio. Respuesta Derecho de Petición UTL Mafe Carrascal. Bogotá, D. C.
- (Defensoría del Pueblo, 2011, como se cita en Corte Constitucional, Sala plena, Sentencia del 6 de octubre de 2011, exp. PE 032)
- Política Nacional para la Transformación Digital e Inteligencia Artificial. (2019). CONPES 3975. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf
- Español, A. G., Uribe, E. T., Ayerbe, P. G., Mujica, M. P. (2021). Marco Etico para la Inteligencia Artificial. Recuperado de: https://inteligenciaartificial.gov.co/static/img/MARCO_ETICO.pdf
- INFOBAE (2022). Se dispararon las quejas por protección de datos: SIC. Recuperado de: https://www.infobae.com/america/

colombia/2022/01/29/se-dispararon-las-quejas-por-proteccion-de-datos-sic/

- CALDERÓN, R.A. (2021). ¿Cómo defender nuestra privacidad e identidad cerebral frente a los riesgos de la neurotecnología? Recuperado de: https://cincodias.elpais.com/cincodias/2021/01/27/legal/1611779453_654051.html
- RAMÍREZ, M, J. (2023). Uso de las redes sociales en Colombia: 90.5% utiliza Facebook. M4RKETING ECOMMERCE CO. Disponible en: https://marketing4ecommerce.co/uso-de-redes-sociales-en-colombia-90-5-utiliza-facebook/

Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. (2017).

- Grupo de Trabajo Sobre Protección de Datos del Artículo 29. Página 6. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf
- Salazar Castellanos, D. (25 de enero de 2023). ¿Por qué hay una ola de ciberataques en Colombia y el país está tan vulnerable? Bloomberg Linea. https://www.bloomberglinea.com/2023/01/25/por-que-hay-una-ola-de-ciberataques-en-colombia-y-el-pais-aun-es-tan-vulnerable/
- Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos Personales. (15 de marzo de 2022). Estudio de medidas de seguridad en el tratamiento de datos personales. https://www.sic.gov.co/sites/default/files/files/2022/Estudio%20de%20seguridad%202022%2015III2022.pdf
- Lesmes Díaz, L. (10 de abril de 2023). Colombia recibió 20.000 millones de ciberataques en 2022. El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-colombia-datos-sobre-ciberataques-en-el-pais-757651
- Pachón, C. (22 de diciembre de 2022). Los Ciberataques más famosos del 2021 en Colombia y el mundo. NSIT – Information technology. https://www.nsit.com.co/los-ciberataques-mas-famosos-del-2021-en-colombia-y-el-mundo/
- Superintendencia de Industria y Comercio. (2015). Guía para la Implementación del Principio de Responsabilidad Demostrada (accountability). SIC. https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
- Instituto Nacional de Seguridad y Salud en el Trabajo (INSST). (2018). Ingeniería de la resiliencia: conceptos básicos del nuevo paradigma en seguridad. INSST. https://www.insst.es/documents/94886/564690/ntp-1.132w.pdf/1791350b-969f-4ded-885a-8eaa46b8e987
- Superintendencia de Industria y Comercio. guía para la implementación del principio de responsabilidad DEMOSTRADA en las transferencias internacionales de datos personales. (2019). SIC. P. 8. - https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales.pdf
- Reglamento General de Protección de Datos, 2016, Considerando 146. Obtenido de: https://gdpr-text.com/es/read/recital-146/#:~:text=(146)%20El%20responsable%20o%20el,en%20infracción%20del%20presente%20Reglamento.
- Asuntos legales (2020) Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. Obtenido de: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651
- Corte Constitucional. (1992). Sentencia T-414 de 1992, Sala Primera de Revisión. M.P. Ciro Angarita Barón. Bogotá.
- Corte Constitucional. (1995). Sentencia SU-082 de 1995, Sala Primera de Revisión. M.P. Jorge Arango Mejía. Bogotá.
- Corte Constitucional. (2002). Sentencia T-729 de 2002, Sala Séptima de Revisión. M.P. Eduardo Montealegre Lynett. Bogotá.
- Corte Constitucional. (2011). Sentencia C-748 de 2011, Sala Plena. M.P. Jorge Ignacio Pretelt Chaljub. Bogotá.
- Corte Constitucional. (2015). Sentencia T-277 de 2015, Sala Primera de Revisión. M.P. María Victoria Calle Correa. Bogotá.
- Corte Constitucional. (2021). Sentencia SU -139 de 2021, Sala Plena. M.P. Jorge Enrique Ibáñez Najar. Bogotá.
- OEA. (2021). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Oas.org. Recuperado el 17 de julio de 2023, de https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf
- Rojas-Bejarano, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.