Bogotá D.C., 22 de agosto de 2023

Señor
JAIME LUIS LACOUTURE PEÑALOZA
Secretario General
Cámara de Representantes

REF: Radicación Proyecto de Ley Estatutaria

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 5ta 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.

Atentamente,

MARÍA FERNANDA CARRASCAL ROJAS Representante a la Cámara por Bogotá	**DUVALIER SÁNCHEZ ARANGO** Representante a la Cámara por Valle del Cauca - Alianza Verde
HÉCTOR DAVID CHAPARRO Representante a la Cámara por Boyacá Partido Liberal Colombiano	**JUAN CAMILO LONDOÑO BARRERA** Representante a la Cámara por Antioquia Partido Alianza Verde

 **Norman David Bañol Álvarez** Representante a la Cámara Circunscripción especial indígena MAIS	 **LEIDER ALEXANDRA VÁSQUEZ OCHOA** **Representante a la Cámara por Cundinamarca** **PACTO HISTÓRICO**
 **Erick Velasco Burbano** Representante a la Cámara por Nariño Pacto Histórico.	 **DAVID ALEJANDRO TORO RAMÍREZ** Representante a la Cámara por Antioquia Pacto Histórico
 **Diela Liliana Benavides Solarte** **Senadora de la República**	 **AGMETH JOSÉ ESCAF TIJERINO** Representante a la Cámara por el departamento del Atlántico Pacto Histórico

MARÍA DEL MAR PIZARRO GARCÍA Representante a la Cámara - Bogotá Coalición Pacto Histórico	**GERMÁN GÓMEZ** Representante a la Cámara Partido Comunes
SANTIAGO OSORIO MARIN Representante a la Cámara Coalición Alianza Verde - Pacto Histórico	**CARLOS FELIPE QUINTERO OVALLE** Representante a la Cámara Departamento del Cesar
ALEJANDRO GARCÍA RÍOS Representante a la Cámara Risaralda Partido Alianza Verde	**Germán Rogelio Rozo Anís** Representante a la Cámara Departamento de Arauca
JUAN CARLOS WILLS OSPINA Representante a la Cámara por Bogotá	**ANDRÉS DAVID CALLE AGUAS** Representante a la Cámara por Córdoba Partido Liberal Colombiano

PROYECTO DE LEY NÚMERO _____ DEL 2023

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

EL CONGRESO DE LA REPÚBLICA,

DECRETA:

TITULO 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 los artículos 15 y 20 de la Constitución Política.

Artículo 2. Ámbito de aplicación material.

1. La presente ley se aplica al tratamiento total o parcialmente automatizado, así como el tratamiento no automatizado de los datos personales registrados o destinados a ser incluidos en bases de datos.

2. La presente ley no se aplicará al tratamiento de datos personales cuando:

a) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del ordenamiento jurídico colombiano;

b) Efectuado por una persona natural en el ejercicio de actividades exclusivamente personales o domésticas;

c) Por parte de las autoridades competentes con fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos y financiación de terrorismo, la

ejecución de sanciones penales, así como la de protección frente a amenazas a la seguridad nacional pública y su prevención.

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales, mientras que su tratamiento no represente una vulneración a los derechos de protección de datos personales y otros derechos fundamentales y garantías constitucionales de los titulares.

e) A las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia

Parágrafo: El Gobierno Nacional, legislará sobre de protección de datos personales tratados para fines de prevención, investigación, detección o monitoreo de actos delictivos incluido el lavado de activos y financiación de terrorismo, la ejecución de sanciones penales.

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 en Colombia, independientemente de si estos son de carácter oneroso, o;

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

3. Cuando proceda la aplicación de la legislación nacional en virtud del Derecho Internacional público, la presente ley deberá aplicarse también a todo responsable no establecido en Colombia pero que actúa en virtud de una misión diplomática, embajada u oficina consular.

Artículo 4. Datos de personas fallecidas.

1. Los causahabientes 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.

2. Las personas o instituciones a las que la persona fallecida hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste y, en su caso su rectificación o supresión. La Superintendencia de Industria y Comercio en conjunto con la Registraduría del Estado Civil, señalarán los requisitos y condiciones para acreditar la validez y vigencia de estas autorizaciones.

3. En caso de fallecimiento de niños, niñas y adolescentes, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Instituto Colombiano de Bienestar Familiar o quien haga sus veces, que podrá actuar de oficio o a instancia de cualquier persona natural o jurídica interesada.

4. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de quienes ejercen como representantes legales, o por la Defensoría del Pueblo, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Parágrafo primero. Las personas a las que se refiere en numeral 1 del presente artículo, no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los causahabientes a acceder a los datos de carácter patrimonial del causante.

Parágrafo segundo. La autorización expresa de que trata el numeral segundo podrá realizarse de conformidad con lo establecido en la ley 1996 de 2019 en relación con las directivas anticipadas, o a través de cualquier otro acto por medio cual se exprese dicha autorización.

Artículo 5. Definiciones. A efectos de la presente ley se entenderá por:

1. «Anonimización»: procedimiento técnico que modifica de manera irreversible los datos personales con el fin que no pueda atribuirse a un titular;
2. «Autoridad de control»: entidad pública que tienen 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 de riesgo crediticio»: para todos los efectos de la presente ley se entenderá por Base de Datos de Riesgo Crediticio aquella en la que se almacena y procesa datos personales de carácter financiero, crediticio, comercial y/o de servicios en cuanto al nacimiento, ejecución y extinción de obligaciones dinerarias se refiere; cuya finalidad será el tratamiento de dicha información para crear un perfil de los titulares y calcular su capacidad de endeudamiento y el riesgo crediticio que de ello se desprende, lo anterior bajo los parámetros y plazos de conservación contenidos en la Ley 2157 de 2021 o la que en su momento esté en vigencia.
4. «Base de datos»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

5. «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.
6. «Cesión o comunicación de datos»: Tratamiento de datos que supone su revelación a una persona distinta del titular y/o encargado de tratamiento;
7. «Consentimiento del titular»: toda manifestación de voluntad libre, consciente, específica espontánea, informada e inequívoca 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;
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 el titular identificado o identificable. Se considerará titular identificable toda persona natural cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;
11. «Datos relativos a la salud»: datos personales 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, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, partidos políticos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, genéticos, a la vida sexual y los datos biométricos;
13. «Denuncia»: sólo para efectos de esta ley, se entenderá como la comunicación dirigida a la autoridad de control que busca el inicio de una investigación administrativa que pretenda proteger el interés general y el derecho colectivo de los titulares de los datos.

14. «Destinatario o tercero»: Persona natural o jurídica, pública o privada, al que se comuniquen datos personales, distinta del titular, responsable de tratamiento y encargado. 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 c) y e) de la presente ley;

15. «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;

16. «Encargado del tratamiento» o «Encargado»: Persona natural o jurídica, pública o privada, que trate datos personales por cuenta del responsable del tratamiento.

17. «fuentes»: Es la persona, entidad u organización que, en virtud de una relación comercial, de servicios o de cualquier otra índole y en calidad responsable, realiza tratamiento de datos de carácter financiero y que, en razón de autorización legal o previamente obtenida del titular, reporta dichos datos a un Operador de Información.

18. «Grupo empresarial: grupo constituido por una empresa que ejerce el control respecto a empresas subordinadas y que exista entre ellas unidad de propósito y dirección, en consecuencia, hay subordinación cuando una empresa depende de otra llamada matriz, que la controla.

19. «Incidente de seguridad»: toda violación de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados, almacenados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

20. «Limitación del tratamiento»: aplicación de medidas por parte del responsable de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse;

21. «Normas corporativas vinculantes»: son aquellas políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio colombiano para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países que no tengan un nivel adecuado de protección de datos de conformidad a los estándares fijados por la autoridad de control, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

22. «Neurodato»: conjunto de información obtenida a partir de la actividad cerebral y el sistema nervioso, que se utilizan para estudiar el cerebro, comprender su funcionamiento y desarrollar aplicaciones en el campo de la neurociencia y la neurotecnología.

23. «Operadores»: Es la persona, entidad u organización que, en calidad de encargado, administra y trata información financiera previamente suministrada por la Fuente de Información respecto de uno o varios titulares con el fin de ponerla en conocimiento de los usuarios finales.

24. «Organización internacional»: son entidades compuestas por sujetos de Derecho Internacional Público (Estados u otras Organizaciones internacionales), que se unen a través de un acuerdo o tratado fundacional y establecen una estructura orgánica permanente.

25. «Queja»: reclamación de interés particular dirigida a la autoridad de control que busca el amparo del derecho fundamental a la protección de los datos personales.

26. «Representante»: persona natural o jurídica designada por escrito o por mensajes de datos suficientes y verificables por parte del responsable o el encargado del tratamiento, de conformidad con el artículo 40, para que represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud de la presente ley;

27. «Responsable del tratamiento» o «responsable»: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros determine los fines, medios y plazos de conservación del tratamiento;

28. «Servicio de la sociedad de la información»: 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.

29. «Seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona natural identificada o identificable;

30. «Tecnología de rastreo»: herramientas utilizadas para recopilar información sobre los usuarios y su comportamiento en línea. Estas tecnologías permiten hacer un seguimiento y recopilación de datos sobre las actividades de los usuarios. Algunas de las tecnologías de rastreo más comunes incluyen cookies, etiquetas de página, píxel, entre otras.

31. «Tercer país»: país que no cuenta con declaración de conformidad por parte de la autoridad de control.

32. «Titular»: Persona natural cuyos datos personales son objeto de Tratamiento.

33. «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 datos personales a destinatarios y/o encargados ubicados fuera del territorio nacional u organizaciones internacionales.

34. «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.

35. «Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, 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;

36. «Usuarios»: Persona natural o jurídica que accede a información financiera de uno o varios titulares de datos personales suministrada por el operador, por la fuente o directamente por el titular, en calidad de responsable del tratamiento de la información.

CAPÍTULO II

PRINCIPIOS Y CONDICIONES RELATIVAS A LA PROTECCIÓN DE DATOS

Artículo 6. Principios relativos al tratamiento.

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

a) «Principio de Legalidad»: El tratamiento de los datos personales debe sujetarse a lo establecido en la presente 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 no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 85, numeral 1, 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 dilación indebida, 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 traten 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, de conformidad con el artículo 85, numeral 1, 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 en el literal anterior será complementario de los deberes de secreto profesional de conformidad con su normativa aplicable.

k) «Principio de seguridad»: Los responsables y/o encargados 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.

l) «Principio de proporcionalidad»: Es una herramienta metodológica que pretende aportar racionalidad, predictibilidad y legitimidad al tratamiento de datos personales. Este principio se traduce en realizar una ponderación atendiendo a tres criterios:

a) Idoneidad: La medida es capaz de alcanzar el objetivo propuesto

b) Necesidad: No exista otra medida más moderada e igual de eficaz para conseguir tal objetivo

c) Proporcionalidad en sentido estricto: Hay que ponderar el beneficio que el tratamiento, desde el punto de vista de la protección de datos, proporciona a la sociedad manteniendo un equilibrio con el impacto que representa sobre otros derechos fundamentales.

2. «Principio de responsabilidad demostrada» «accountability»: El responsable del tratamiento deberá dar cumplimiento a lo dispuesto en la presente ley y las disposiciones que la desarrollan, siendo capaz de demostrarlo.

3. «Principio de Neutralidad Tecnológica»: la presente ley se aplicará en el uso de tecnologías y herramientas para el tratamiento de datos personales. Su aplicación no se limita a una única forma de tratar la información, ni es excluyente de tecnologías existentes, ni perderá vigencia frente a las futuras.

Artículo 7. 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, a petición de este, de medidas precontractuales;

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

d) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural;

e) El tratamiento es necesario para el cumplimiento de una misión 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 sobre dichos intereses no prevalezcan los intereses o los derechos y garantías fundamentales del titular que requieran la protección de datos personales, teniendo en cuenta las expectativas razonables de los titulares respecto de su relación con el responsable, en particular cuando el titular sea un menor de edad.

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

2. La base jurídica que legitima el tratamiento indicado en el numeral 1, literales c) y e), y la finalidad del mismo debe estar fundamentada en normativa vigente.

3. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del titular o una disposición distinta a la presente ley que constituya una medida necesaria y proporcional en una sociedad democrática. El responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) Cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) El contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los titulares y el responsable del tratamiento;

c) La naturaleza de los datos personales, en concreto cuando se traten datos sensibles, de conformidad con el artículo 15, o datos personales relativos a delitos y condenas penales, de conformidad con el artículo 16;

d) Las posibles consecuencias para los titulares del tratamiento ulterior previsto;

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

4. Las leyes y sus reglamentaciones expedidas con posterioridad a la presente ley deberán 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.

Parágrafo: 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, como las relativas a otras situaciones específicas de tratamiento a tenor del Título VI. La normativa vigente cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

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 consintió de forma previa el tratamiento de sus datos personales.

2. Corresponderá al responsable del tratamiento la prueba de 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 y 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 libre, espontánea, específica, informada e inequívoca. 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 a 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 catorce 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 catorce años, fundado en el consentimiento, sólo será lícito si consta el consentimiento del representante legal, con el alcance que determinen 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 tomará todas las medidas razonables 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 catorce años es ejercida por más de una persona, se presume que el consentimiento de uno obedece a la voluntad de todos. En el supuesto 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. Condiciones para el tratamiento en la ejecución de un contrato.

1. Se recolectarán los datos necesarios para la ejecución del contrato, todos aquellos datos que no se requieran para la existencia y ejecución del mismo, necesitarán de otra base legitimadora para su tratamiento.

2. El plazo de conservación de los datos estará determinado por la duración del contrato, salvo que, en cumplimiento de un deber legal el responsable esté obligado a exceder ese plazo.

3. La contratación que se lleve a cabo por entidades públicas, también le serán aplicables los principios y demás obligaciones establecidas en la presente ley.

4. Una vez terminada la relación contractual por cualquier causa, incluida la nulidad, los datos de carácter personal se devolverán al titular, si éste los solicita dentro de los 30 días siguientes a la terminación del contrato o luego de la sentencia ejecutoriada que declara la nulidad. Con posterioridad a los 30 días, los datos podrán ser suprimidos por el responsable. No procederá la supresión de los datos cuando exista una disposición legal que exija su conservación, en cuyo caso, deberá procederse a la devolución de los mismos garantizando el responsable del tratamiento dicha conservación.

5. El responsable del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación contractual con el titular, excepto para la puesta a disposición por orden judicial, o por orden de la fiscalía general de la nación, o por la Superintendencia de Industria y Comercio, y cuando proceda, la Superintendencia Financiera de Colombia.

Artículo 11. Condiciones para el tratamiento cuando se esté ante el cumplimiento de un deber legal. Cuando la base jurídica que legitima el tratamiento es la ley, no se requerirá que

cada tratamiento se rige por una norma específica. Una ley o disposición normativa puede ser suficiente como base para varias operaciones de tratamiento aplicable al responsable.

Artículo 12. Condiciones para cuando el tratamiento es necesario para el interés vital del titular.

1. Se presume legítimo el tratamiento que ocurra en el contexto de una urgencia médica o emergencia sanitaria y/o eventos catastróficos.

2. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital del titular cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. El tratamiento busca facilitar que el titular reciba atención médica en situaciones que pongan en riesgo su vida y se encuentre incapacitado física o jurídicamente para autorizar dicho tratamiento. Esta base legitimadora será compatible con el interés público.

3. Cuando se trate de un menor de edad cuyo representante legal no se encuentre presente, el tratamiento se llevará a cabo de acuerdo a lo establecido en el numeral 2 del presente artículo. En cuanto sea posible, el responsable del tratamiento obtendrá el consentimiento de quien represente los intereses del menor.

Parágrafo primero: Entiéndase como urgencia médica, condiciones de salud que amenacen la vida del titular.

Parágrafo segundo: El tratamiento realizado en el marco de una emergencia sanitaria y/o eventos catastróficos sólo será legítimo, si la misma ha sido declarada en los términos establecidos en el artículo 69 de la Ley 1753 de 2015, o cualquier norma que la adicione, modifique o sustituya.

Parágrafo tercero: En ningún caso el tratamiento de datos basado en el interés vital del titular puede considerarse consentimiento informado y para ello debe consultarse la normativa que regula la relación médico-paciente.

Artículo 13. Condiciones para el tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de funciones públicas conferidas al responsable.

1. El responsable del tratamiento que actúe en ejercicio de una misión realizada en interés público o en el ejercicio de funciones públicas debe hacerlo en estricto cumplimiento de estas.

2. Cuando se habla de una misión realizada en interés público o en ejercicio de funciones públicas, las mismas pueden ser llevada a cabo por un responsable de naturaleza pública o privada, siempre y cuando, tengan la idoneidad para poder realizar el tratamiento.

3. El tratamiento ulterior de datos será legítimo si dicha finalidad está determinada y especificada en las disposiciones normativas de las que emana el interés público o las funciones públicas conferidas al responsable. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta las condiciones descritas en el artículo 7, numeral 3 de la presente ley.

Artículo 14. Condiciones para el tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero.

1. Una vez se haya examinado que el tratamiento no puede ser realizado en el supuesto de otra base legitimadora, el responsable podrá basar el tratamiento de datos personales en el interés legítimo siempre que se verifiquen las siguientes condiciones generales y específicas para dicho tratamiento:

a) Debe representar un interés real y actual, es decir, no debe ser especulativo.
b) Debe existir una relación pertinente y apropiada entre el titular y el responsable, como en situaciones en las que el titular es cliente o está al servicio del responsable.
c) No es aplicable al tratamiento realizado por las entidades públicas en ejercicio de sus funciones.
d) No puede ser invocado cuando se traten datos sensibles.
e) Cuando se trate de una transferencia internacional basándose en un interés legítimo imperioso, debe cumplir con los requisitos establecidos en el artículo 67 de la presente ley.

2. Dependiendo del estado de la técnica, recursos a disposición y las circunstancias del tratamiento, el interés legítimo puede convertirse en una de las bases legitimadoras mencionadas en el artículo 7, y se tomará aquella como preferente.

3. El interés legítimo siempre debe estar acompañado de un examen de ponderación, excepto cuando:

a) Se realiza tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.
b) El tratamiento está relacionado con la realización de determinadas operaciones mercantiles de conformidad con el artículo 87 de la presente Ley.
c) El tratamiento es necesario para la prevención del fraude.
d) Se transmiten datos personales dentro de un grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados.

4. El examen que se menciona en el numeral 3 del presente artículo, es una evaluación que se compone de tres diferentes fases preclusivas. El mismo tiene como objeto comprobar si el

tratamiento es lícito y este examen, debe quedar documentado, en cumplimiento del principio de responsabilidad demostrada "*Accountability"* y, de una forma clara y transparente, en virtud del principio de transparencia, dicho examen debe partir con la descripción del tratamiento. Las fases que componen el examen de interés legítimo son las siguientes:

a) Test de finalidad (" satisfacción *de intereses legítimos del responsable*"): teniendo en cuenta la finalidad o el propósito específico del tratamiento analizado, debe identificarse cuál es el beneficio concreto sobre el que se sustenta dicho tratamiento;
b) Test de necesidad (*"¿es necesario el tratamiento?"*): resulta imprescindible analizar si dicho tratamiento es necesario y proporcional para la consecución de los objetivos propuestos o si por el contrario concurren otras alternativas para satisfacer esos intereses;
c) Test de equilibrio (*"que sobre dichos intereses no prevalezcan los intereses o los derechos y garantías fundamentales del titular"*): si resultara que no existe otra alternativa o esta exigiera esfuerzos desproporcionados, procede realizar la prueba de sopesamiento. Dicha prueba consiste en analizar el impacto y/o el daño o perjuicio potencial del concreto tratamiento en los derechos y garantías de los titulares, para lo cual se tendrá en cuenta:
    i) Origen de los datos;
    ii) Categoría de los datos;
    iii) Si existe o no una relación previa con el titular;
    iv) Expectativa;
    v) Si afecta los intereses, derechos y garantías del titular;
    vi) Agentes implicados en el tratamiento;
    vii) Garantías adicionales para limitar su impacto en los derechos y garantías fundamentales.

5. El tratamiento puede basarse en un interés legítimo cuando el test de equilibrio sea a favor del responsable.

Artículo 15. 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, o la afiliación sindical, el tratamiento de datos genéticos, neurodatos, datos biométricos dirigidos a identificar de manera unívoca a una persona natural, datos relativos a la salud o datos relativos a sexo o características biológica, su identidad o expresión de género, la vida sexual o la orientación sexual de una persona natural.

2. El numeral 1 no será de aplicación cuando concurran 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 un convenio colectivo 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 a 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 sobre la base de la normativa, que debe ser proporcional al objetivo perseguido, respetando el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los derechos y garantías fundamentales del titular;

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, o 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 y 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, de conformidad con el artículo 85, numeral 1, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

3. Los datos personales a 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 16. Tratamiento de datos personales relativos a delitos y condenas penales. El tratamiento de datos personales relativos a delitos y condenas penales o medidas de seguridad conexas sobre la base del artículo 7, numeral 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas que establezcan la protección adecuada para los derechos y garantías de los titulares. Solo podrá llevarse un registro completo de antecedentes judiciales bajo el control del Ministerio de Defensa Nacional de conformidad con el artículo 94 del Decreto 19 de 2012 o cualquier norma que la adicione, modifique o sustituya.

Artículo 17. Tratamiento de datos relativos a infracciones y sanciones administrativas.

1. El tratamiento de datos relativos a infracciones y sanciones administrativas, 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 y sanciones administrativas 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 y sanciones administrativas solo 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.

Artículo 18. Tratamiento que no requiere identificación

1. Cuando un responsable trate datos personales que no requieren o ya no requieren la identificación de un titular para el cumplimiento de los fines previstos, éste no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al titular.

2. Cuando, en los casos a que se refiere el numeral 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al titular, no se aplicarán los artículos 24 al 32 de la presente ley, excepto cuando el titular, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

TITULO II

DEBER DE INFORMACIÓN Y DERECHOS DE LOS TITULARES

CAPÍTULO I

TRANSPARENCIA E INFORMACIÓN

Artículo 19. Transparencia e información al titular.

1. El responsable del tratamiento tomará las medidas pertinentes para facilitar al titular toda información indicada en los artículos 20 y 21, así como cualquier comunicación con arreglo a los artículos 24 al 34 y 50 relativa al tratamiento, 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 los artículos 24 al 34. En caso de que el responsable no esté en condiciones de identificar al titular, en virtud de lo establecido en el artículo 18 numeral 2, no se aplicarán los artículos 24 al 32 de la presente ley, 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 en virtud a los establecido en los artículos 24 al 34, en los términos del derecho de petición general de conformidad a la Ley 1755 del 2015 o cualquier norma que la adicione, modifique o sustituya.

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 a las que se refieren los artículos 24 al 34 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 control.

5. La información facilitada en virtud de los artículos 20 y 21 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 24 a 34 y 50 serán a título gratuito. Cuando las solicitudes sean carentes de fundamento legal, temeraria y/o excesivas, especialmente debido a su carácter reiterativo, el responsable del tratamiento podrá:

a) En el caso de ser una solicitud ya resuelta, remitirse a las respuestas anteriores;
b) Cobrar al titular los gastos administrativos por proporcionar la información, la comunicación o realizar la actuación solicitada;
c) Negarse a actuar respecto de la solicitud, por considerarse temeraria y reiterativa.

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 Control, cuando ésta así lo requiera, que la conducta del titular es carente de fundamento legal, temeraria y/o reiterativa.

6. Sin perjuicio de lo dispuesto en el artículo 18, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad del titular que radicó una solicitud a que se refieren

los artículos 24 a 34, podrá requerir a la misma información adicional necesaria para confirmar su identidad.

7. La información que deba facilitarse a los titulares en virtud de los artículos 20 y 21 podrá transmitirse 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 Superintendencia de Industria y Comercio establecerá las reglas, símbolos e imágenes mediante las cuales el responsable del tratamiento o el encargado podrán dar cumplimiento al deber de información.

Artículo 20. 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 tercer país u organización internacional y la existencia o ausencia de una declaración de conformidad de la Superintendencia de Industria y Comercio, o, en los casos de las transferencias indicadas en los artículos 64 o 65 o el artículo 67 numeral 1, inciso segundo, 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.

2. Además de la información mencionada en el numeral 1, el responsable del tratamiento facilitará al titular, en el momento en que se obtienen los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) La descripción y ejercicio de los derechos que le asisten al titular;

c) cuando el tratamiento esté basado en el artículo 7, numeral 1, literal a), o el artículo 15, numeral 2, literal a), 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;
d) El derecho a presentar una queja ante la Superintendencia de Industria y Comercio, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos;
e) 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;
f) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 34, numeral 1 y 4, 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.

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

Artículo 21. 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 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 conformidad de la Superintendencia de Industria y Comercio, o, en el caso de las transferencias indicadas en los artículos 64 o 65 o el artículo 67, numeral 1, inciso

segundo, 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.

2. Además de la información mencionada en el numeral 1, el responsable del tratamiento facilitará al titular, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) La descripción y ejercicio de los derechos que le asisten al titular.
c) Cuando el tratamiento esté basado en el artículo 7, numeral 1, literal a), o el artículo 15, numeral 2, literal a), 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;
d) El derecho a presentar una queja ante la Superintendencia de Industria y Comercio, cuando el titular considere que no se ha tramitado correctamente el ejercicio de derechos;
e) 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 que no facilitar tales datos;
f) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 34, numerales 1 y 4, 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.

3. El responsable del tratamiento facilitará la información indicada en los numerales 1 y 2:

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) Si los datos personales han de utilizarse para comunicación con el titular, a más tardar en el momento de la primera comunicación a dicho titular, o;
c) Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. 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.

5. 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 el artículo 85, numeral 1, 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, o
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 22. Aviso de privacidad o Capa básica.

1. Cuando los datos personales sean obtenidos del titular, el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 20 de 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 24 al 34 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 34 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 21 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 23. Disposiciones generales sobre ejercicio de los derechos.

1. Los derechos reconocidos en los artículos 24 al 34 de la presente ley, podrán ejercerse directamente o con el acompañamiento de los apoyos señalados en la ley 1996 de 2019 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 los artículos 19 numeral 3 inciso segundo, y el numeral 5 y el artículo 24 numeral 3 de 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 24. 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, derecho de acceso a los datos personales y 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, o a oponerse a dicho tratamiento;
f) El derecho a presentar una reclamación ante la Autoridad de control;
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, a que se refiere el artículo 34, numerales 1 y 4, 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 del artículo 64 de la presente ley.

3. El responsable del tratamiento facilitará al titular una copia de los datos personales objeto de tratamiento. El responsable podrá cobrar al titular los gastos administrativos por cualquier otra copia solicitada. Cuando el titular presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el numeral 3 no afectará negativamente a los derechos y garantías de otras personas naturales.

Artículo 25. Derecho de rectificación. El titular tendrá derecho a obtener sin dilación indebida 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 conciernan teniendo en cuenta los fines del tratamiento.

Artículo 26. Derecho de rectificación en medios de comunicación.

1. El derecho a la rectificación implica la corrección de la información que atente contra el principio de exactitud. Para que sea efectivo, debe tener un despliegue comunicativo similar al inicial y que el medio de comunicación reconozca su error.

2. El derecho se ejercitará mediante la presentación de la solicitud de rectificación al oficial de protección de datos o área designada para la protección de datos por el medio de comunicación o, de forma tal que permita tener constancias de su fecha y de su recepción. La rectificación deberá limitarse a la información que se desea rectificar.

3. Siempre que el derecho se ejercite de conformidad con lo establecido en el numeral anterior, el medio de comunicación deberá publicar o difundir íntegramente la rectificación en las condiciones descritas en el numeral 1, dentro de los tres días hábiles siguientes al de su recepción, prorrogables por única vez y por el mismo término, con relevancia semejante a aquella en que se publicó o difundió la información que se rectifica, sin comentarios ni apostillas.

Cuando no fuere posible atender la solicitud de rectificación dentro de los tres días hábiles, se informará al titular los motivos de la demora.

4. Podrán ejercitar el derecho de rectificación el titular afectado o sus representantes y, si hubiese fallecido aquél, sus familiares o herederos o los representantes de éstos.

5. Si en el término señalado en el numeral 3, no se hubiera publicado o divulgado la rectificación o se hubiese notificado expresamente por el medio de comunicación que aquella no será difundida, o se haya publicado o divulgado sin respetar lo dispuesto en los numeral 1 y 3, el titular afectado tendrá derecho a ejercer las acciones constitucionales que procedan y también el derecho de indemnización del que habla el artículo 89 de la presente ley.

6. Los responsables de redes sociales y plataformas de servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación del contenido que otros usuarios difundan y atente contra el principio de exactitud en Internet.

Artículo 27. Derecho de supresión («el derecho al olvido»).

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 sin dilación indebida los datos personales cuando concurra alguna de las siguientes circunstancias:

a) Los datos personales ya no sean 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 el artículo 7, numeral 1, literal a), o el artículo 15, numeral 2, literal a), y este no se fundamente en otra base legitimadora;

c) El titular se oponga al tratamiento con arreglo al artículo 33, numeral 1 y 2, y no prevalezcan otros motivos legítimos.

d) Los datos personales hayan sido tratados ilícitamente;

e) Los datos personales deban 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 el artículo 9, numeral 3.

g) La Autoridad de Control Competente determine que en el tratamiento ha incurrido en conductas contrarias a la Constitución o esta ley y las demás normas que la modifiquen o adicionen.

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 misión 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 15, numeral 2, literales h) e i), y numeral 3;

d) Con fines de archivo en interés público, investigación científica, o estadística, de conformidad con el artículo 85, numeral 1, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o;

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

Artículo 28. Derecho al olvido en búsquedas de Internet.

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieren tras una búsqueda efectuada, a partir de su nombre, en los enlaces publicados que contengan información relativa a esa persona cuando fueran inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invoque el titular, y evidencie la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Parágrafo 1: Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediera por la misma a su borrado previo o simultáneo.

Parágrafo 2: El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 29. Derecho al olvido en servicios de redes sociales y servicios equivalentes.

1. Toda persona tiene derecho a que sean suprimidos los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le concierne y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fueran inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invoque el titular evidencian la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este numeral, los datos que hubiesen sido facilitados por personas naturales en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercite por un titular respecto de datos que hubiesen sido facilitados al servicio, por éste o por terceros, durante su minoría de edad, el prestador deberá

proceder sin dilación a su supresión sin necesidad de que concurran las circunstancias mencionadas en el numeral 2.

Artículo 30. 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 condiciones siguientes:

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 reclamaciones administrativas o judiciales;

d) El titular se haya opuesto al tratamiento en virtud del artículo 33, numeral 1, 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 31. 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 al artículo 25, artículo 27 numeral 1, y al artículo 30 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 32. Derecho a la portabilidad de los datos.

1. El titular tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y 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 con arreglo al artículo 7, numeral 1, literal a), o el artículo 15, numeral 2, literal a), o en un contrato con arreglo al artículo 7, numeral 1, literal b) , y

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 del artículo 27. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

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

5. El Derecho a la portabilidad de los datos únicamente se debe aplicar cuando la base legitimadora es el consentimiento y/o el contrato.

Artículo 33. 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 el artículo 7, numeral 1, literales e) o f), 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 dichos fines.

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 de conformidad con el artículo 85 numeral 1, 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 misión realizada por razones de interés público.

Artículo 34. 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, o;
- **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, a expresar su punto de vista, a recibir una explicación de la decisión y a impugnar la decisión.

4. Las decisiones a que se refiere el numeral 2, no se basarán en datos sensibles contemplados en el artículo 15, numeral 1, salvo que se aplique lo consagrado en el artículo 15, numeral 2, literal a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos, garantías e intereses del titular.

Artículo 35. Derecho a presentar una queja ante la Autoridad de Control.

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 control competente.

2. La queja se formulará mediante solicitud dirigida a la Autoridad de Control y deberá contener, por lo menos:

a) La identificación del titular y/o su representante legal junto con los documentos que acrediten tal calidad;

b) El objeto de la queja, es decir, lo que se persigue con ella;

c) La descripción clara de los hechos que fundamentan el reclamo;

d) La dirección de notificación;

e) Los documentos que soporten la acreditación del requisito de procedibilidad establecido en el numeral 3 del presente artículo, y;

f) Los demás documentos que se quiera hacer valer en el trámite administrativo.

3. El titular o quien represente sus intereses solo podrá elevar queja ante la Autoridad de Control 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 de la información.

4. La Autoridad de Control tendrá la obligación de examinar integralmente la petición, y en ningún caso, podrá estimarla como incompleta por falta de requisitos o documentos que no se encuentren dentro del marco jurídico vigente, que no sean necesarios para resolverla o que se encuentren dentro de sus archivos.

Si el reclamo resulta incompleto, se requerirá al titular dentro de los diez (10) días siguientes a la fecha de radicación de la queja para que la complete, otorgándole al solicitante el término de un (1) mes para ello. Transcurrido el término de un (1) mes desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido de su queja, salvo que antes del vencimiento de dicho plazo éste solicite prórroga hasta por un término igual.

5. La autoridad de control ante la que se haya presentado la queja informará a solicitud del reclamante sobre el curso del trámite administrativo y en cualquier caso sobre las etapas que la normativa procesal así determine como obligatorias.

Artículo 36. Derecho a presentar una denuncia ante la Autoridad de Control.

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 Control, persiguiendo la protección del interés general 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 control 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 Control 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 esta ley.

TITULO III

RESPONSABLE DEL TRATAMIENTO Y ENCARGADO DEL TRATAMIENTO

CAPÍTULO I

OBLIGACIONES GENERALES

Artículo 37. Obligaciones del responsable del tratamiento.

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y garantías fundamentales de los titulares, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la presente Ley. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el numeral 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados en virtud del artículo 58 o a un mecanismo de certificación aprobado en virtud del artículo 60 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

4. El responsable del tratamiento deberá actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas técnicas y organizativas apropiadas para que la información suministrada a este, se mantenga actualizada.

5.El responsable del tratamiento garantizará el pleno ejercicio de los derechos que le conciernen a los titulares de la información en los términos previstos en esta ley y en las demás normas que la modifiquen o adicionen.

6. El responsable del tratamiento deberá dar cumplimiento al deber de información contenido en los artículos 20 y 21 de la presente ley

7. El responsable del tratamiento notificará a la Superintendencia de Industria y Comercio cuando se presenten incidentes de seguridad de conformidad con el artículo 49 de la presente ley.

8. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio como autoridad nacional de protección de datos.

9. El responsable del tratamiento deberá, de forma periódica y continua, 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.

Parágrafo: Los Responsables del Tratamiento deberán cumplir los deberes consignados en el presente artículo, sin perjuicio de las demás disposiciones previstas en la presente ley.

Artículo 38. 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 actuar del 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 39. 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 responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por la presente Ley, en particular en cuanto al ejercicio de los derechos de los titulares y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 20 y 21.

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, y en contra de, cada uno de los responsables.

Artículo 40. Representantes de responsables o encargados del tratamiento con domicilio fuera del territorio Nacional.

1. Cuando sea de aplicación el artículo 3 numeral 2, el responsable o el encargado del tratamiento designará por escrito un representante legal y/o sucursal en Colombia.

2. La obligación establecida en el numeral 1 del presente artículo no será aplicable:

a) Al tratamiento de datos que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 15 numeral 1, o de datos personales relativos a delitos y condenas penales a que se refiere el artículo 16, y que sea improbable que entrañe un riesgo para los derechos y garantías de las personas naturales, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o;

b) A las autoridades u organismos públicos.

3. El responsable o el encargado del tratamiento encomendará al representante las facultades necesarias a fin de garantizar el cumplimiento de lo dispuesto en la presente ley.

4. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 41. Encargado del tratamiento.

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable, éste elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la presente ley y garantice la protección de los derechos del titular.

2. 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.

3. El tratamiento por el encargado se regirá por un contrato con arreglo a las leyes civiles, 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 con el artículo 47;

d) Respetará las condiciones indicadas en los numerales 2 y 5 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 los artículos 47 al 52, 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.

4. 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.

5. 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 a que se refiere el numeral 3, 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.

6. La adhesión del encargado y/o subencargado del tratamiento a un código de conducta aprobado como lo indica el artículo 58 o a un mecanismo de certificación aprobado como lo indica el artículo 60 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los numerales 1 y 5 del presente artículo.

7. Sin perjuicio que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato a que se refieren los numerales 3 y 5 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los numerales 8 y 9 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable, encargado o subencargado de conformidad con los artículos 60 y 61.

8. La Superintendencia de Industria y Comercio podrá fijar cláusulas contractuales tipo para los contratos a que se refieren los numerales 3 y 5 del presente artículo.

9. El contrato a que se refieren los numerales 3 y 5 deberá constar por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 89, 91 y 96, 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.

Parágrafo. 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 3 y 5 del presente artículo, adquieran la calidad de subencargados.

Artículo 42. Tratamiento bajo el control del responsable o del encargado del tratamiento. 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 43. 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 terceros países u organizaciones internacionales;
e) Los encargados que intervienen en el tratamiento;
f) De ser procedente, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 67 numeral 1, inciso segundo, 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 a que se refiere el artículo 47, numeral 1 o la remisión al documento que las contenga.

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 un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 67 numeral 1, inciso segundo, la documentación de garantías adecuadas;
e) Una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 43, numeral 1 o la remisión al documento que las contenga.

Artículo 44. Disposición del Registro de las actividades de tratamiento.

Los registros a que se refiere el artículo 43 constarán por escrito, inclusive en formato electrónico. El responsable o el encargado del tratamiento pondrán el registro a disposición de la Autoridad de Control competente cuando lo requiera.

Artículo 45. 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 las autoridades de control competentes en materia 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 deberá procederse 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 modo 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 Superintendencia de Industria y Comercio, dentro del ámbito de sus respectivas 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.

Artículo 46. Cooperación con la autoridad de control

El responsable y el encargado del tratamiento, o en su caso sus representantes, cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

CAPÍTULO II

SEGURIDAD DE LOS DATOS

Artículo 47. 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 o 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 58 o a un mecanismo de certificación aprobado de conformidad con el artículo 60, así como, la adopción de directrices dadas por la Superintendencia de industria y Comercio 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 48. Medidas de seguridad en el ámbito del sector público.

1. El Modelo de Gobernanza de la Seguridad Digital incluirá las medidas técnicas y organizativas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 47 de la presente ley.

2. Los responsables o encargados a los que se refiere los artículos 39 y 40 de la Ley 489 de 1998, Rama judicial, Rama legislativa, Órganos de Control, Organización electoral, Fundaciones de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas, deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan al Modelo de Gobernanza de Seguridad Digital, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos y sujetas al derecho privado.

Parágrafo Primero: La implementación del Modelo de Gobernanza de Seguridad Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política, y demás normas concordantes.

Parágrafo Segundo: En los casos en los que un tercero preste un servicio por medio de contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Modelo de Gobernanza de la Seguridad Digital.

Parágrafo Tercero: El Modelo de Gobernanza de la Seguridad Digital también tendrá en cuenta el tratamiento manual de datos.

Artículo 49. Notificación de un Incidente de seguridad de los datos personales a la autoridad de control.

1. En caso de Incidente de seguridad de los datos personales, el responsable del tratamiento lo notificará a la Superintendencia de Industria y Comercio de conformidad con el artículo 73 sin dilación indebida 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 Superintendencia de Industria y Comercio 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 dilación indebida al responsable del tratamiento los incidentes de seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el numeral 1 deberá, como mínimo:

a) Describir la naturaleza de la Incidente de seguridad de los datos personales y, cuando sea posible, el número aproximado y 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 dilación indebida.

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 control verificar el cumplimiento de lo dispuesto en el presente artículo.

6. Los datos personales contenidos en la notificación de una Incidente de seguridad y que fueron comunicados a la Superintendencia de Industria y Comercio, 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 y adoptando medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

Artículo 50. 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 dilación indebida.

2. La comunicación al titular contemplada en el numeral 1 del presente artículo deebrá 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 49, 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 condiciones siguientes:

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 garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y garantías del titular a que se refiere el numeral 1;

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 por la que se informe de manera igualmente efectiva a los titulares.

5. Cuando el responsable no haya comunicado al titular el Incidente de seguridad de los datos personales, la Superintendencia de Industria y Comercio, 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 51. Evaluación de impacto relativa a la protección de datos.

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 recabará el 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 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 modo similar;

b) Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 15 numeral 1, o de los datos personales relativos a delitos y condenas penales a que se refiere el artículo 16, u

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

4. La Superintendencia de Industria y Comercio 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 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 que se refiere el numeral 1, y

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 que se refiere el artículo 58 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 conformidad con el artículo 7 numeral 1, literales c) o e), tenga su base jurídica en una ley o normativa especial que se aplique al responsable del tratamiento, donde se regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los numerales 1 a 6 no serán de aplicación excepto si una ley o norma especial posterior así lo ordena.

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

Artículo 52. Consulta previa.

1. El responsable del tratamiento consultará ante la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio antes de llevar a cabo un tratamiento cuando, de la evaluación de impacto de que trata del artículo 51, se concluya que dicho tratamiento supondría un alto riesgo para los derechos y garantías de los titulares.

2. Cuando la Delegatura para la Protección de Datos Personales considere que el tratamiento previsto en el numeral 1 suponga un alto riesgo para los derechos y garantías de los titulares,

asesorará por escrito al responsable, y en su caso al encargado, entre otras cosas respecto de las medidas técnicas y organizativas que se deberán adoptar previo al tratamiento de los datos.

La Delegatura para la Protección de Datos Personales deberá, en un plazo de 3 meses contados a partir de la fecha en que el responsable, o en su caso el encargado, acude ante ella, emitir un concepto. Este plazo podrá prorrogarse, en función de la complejidad del tratamiento, por única vez, por un periodo igual a la inicial, informando al responsable y, en su caso, al encargado del tratamiento de tal prórroga, indicando los motivos de la dilación.

3. El escrito que el responsable del tratamiento allegue a la Superintendencia de Industria y Comercio deberá contener como mínimo la siguiente información:

a) En caso de ser procedente, las responsabilidades respectivas del responsable, y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) Los fines y medios del tratamiento previsto;

c) Las medidas establecidas para proteger los derechos y garantías de los titulares de conformidad con la presente Ley;

d) En su caso, los datos de contacto del oficial de protección de datos;

e) La evaluación de impacto relativa a la protección de datos establecida en el artículo 51 de esta ley;

f) Cualquier otra información que solicite la autoridad nacional de protección de datos.

Parágrafo: Cuando la Superintendencia de Industria y Comercio deba requerir información y/o documentación adicional, los términos establecidos en el numeral 2 del presente artículo se suspenderán hasta que la información y/o documentación se haya obtenido o hasta que el plazo otorgado para suministrarlos, se haya cumplido.

CAPÍTULO VI

OFICIAL DE PROTECCIÓN DE DATOS

Artículo 53. 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 una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

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, o;

c) Las actividades principales del responsable o del encargado que consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 15 y de datos a los que se refieren los artículos 16 y 17.

2. Además el responsable y el encargado del tratamiento designarán un Oficial de protección de datos personales, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales;

b) Los centros docentes, instituciones de educación, que ofrezcan enseñanzas en cualquiera de los niveles de preescolar, básica y media, no formal e informal, así como en la educación superior establecidos en las Normas Generales de la Educación, así como las Universidades públicas y privadas;

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala;

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio;

e) Las instituciones que integran el Sistema General de Seguridad Social, están obligadas al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual;

f) Los establecimientos financieros de crédito y operadores de información;

g) Las entidades aseguradoras y reaseguradoras;

h) Las sociedades que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego;

i) Los distribuidores y comercializadores de servicio público de suministro;

j) Los responsables de bases de datos para la gestión y prevención del fraude, reguladas por la legislación de prevención del lavado de activos y de la financiación del terrorismo;

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los titulares o realicen actividades que impliquen la elaboración de perfiles de los mismos;

l) Las empresas de seguridad privada;

m) Las federaciones deportivas cuando traten datos de menores de edad.

Artículo 54. Calidades del Oficial de protección de datos.

1. Un grupo empresarial podrá nombrar un único Oficial de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

2. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único Oficial de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

3. 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 un Oficial de protección de datos.

4. El Oficial de protección de datos será designado según su profesión y, en particular, por sus conocimientos especializados en Derecho y la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones indicadas en el artículo 57.

5. 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.

6. El responsable o el encargado del tratamiento publicará los datos de contacto del Oficial de protección de datos y los comunicarán a la Delegatura para la Protección de Datos Personales 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.

7. La Delegatura para la Protección de Datos Personales mantendrá, en el ámbito de sus respectivas competencias, una lista actualizada de oficiales de protección de datos que será accesible por medios electrónicos.

8. 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 o garantías de los titulares.

Artículo 55. Cualificación del oficial de protección de datos.

El cumplimiento de los requisitos establecidos en el artículo 54 numeral 4 de la presente ley para la designación del oficial de protección de datos, sea persona natural o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en Derecho y la práctica en materia de protección de datos.

Artículo 56. 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 relativas a 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 del artículo 57, facilitando los recursos necesarios para el desempeño de dichas funciones y 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 por lo que respecta a todas las cuestiones relativas 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 Delegatura para la Protección de Datos Personales. El Oficial podrá verificar los procedimientos y emitir recomendaciones en el ámbito de sus competencias.

Artículo 57. 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 incumben en virtud de la presente 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 las políticas 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 el artículo 51;

e) Cooperar con la Autoridad de Control;

f) Actuar como punto de contacto de la Autoridad de Control para la protección de datos personales sobre cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 52, así como a solicitar instrucciones, en su caso, sobre cualquier otro asunto;

h) 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

CÓDIGOS DE CONDUCTA Y CERTIFICACIÓN

Artículo 58. Códigos de conducta

1. La Autoridad de control competente 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 los distintos sectores de tratamiento y las necesidades específicas de las microempresas, las pequeñas y medianas empresas.

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o 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 y procedimientos a que se refieren los artículos 37 y 38 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 47;

i) La notificación de incidentes de seguridad de los datos personales a la Superintendencia de Industria y Comercio y la comunicación de dichos incidentes a los titulares;

j) La transferencia de datos personales a terceros países u organizaciones internacionales, o;

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 de los titulares en virtud del artículo 35.

3. Los responsables o encargados del tratamiento a los que se aplica la presente ley, así como también, a los que no se aplica en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el numeral 5 del presente artículo con fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales de conformidad con el artículo 64 numeral 2, literal d).

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 a que se refiere el numeral 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en artículo 59 numeral 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de la Superintendencia de Industria y Comercio con arreglo a los artículos 69 y 74.

5. Las asociaciones y otros organismos mencionados en el numeral 2 del presente artículo que pretendan elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la Superintendencia de Industria y Comercio con arreglo al artículo 73.

La Superintendencia de Industria y Comercio determinará si el proyecto de código o 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 o la modificación o ampliación es aprobado de conformidad con el numeral 5, la Superintendencia de Industria y Comercio publicará el código.

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

Artículo 59. Supervisión de códigos de conducta aprobados.

1. Sin perjuicio de las funciones y los poderes de la Superintendencia de Industria y Comercio en virtud de los artículos 69 y 74, un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la Superintendencia de Industria y Comercio podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 58.

2. El organismo podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:

a) Ha demostrado, a satisfacción de la Superintendencia de Industria y Comercio, su independencia y pericia en relación con el objeto del código;

b) Ha establecido 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;

c) Ha establecido procedimientos y estructuras para tratar las reclamaciones relativas 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, y para hacer que estos sean transparentes para los titulares y el público en general, y;

d) Ha demostrado, a satisfacción de la Superintendencia de Industria y Comercio, que sus funciones y objetivos no dan lugar a conflicto de intereses.

3. La Superintendencia de Industria y Comercio fijará los criterios de acreditación de los organismos a que se refiere el presente artículo.

4. Sin perjuicio de las funciones y las facultades de la Superintendencia de Industria y Comercio y de lo dispuesto en el Título VII, en virtud del numeral 1 del presente artículo, el organismo acreditado deberá, con sujeción a garantías adecuadas, 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 de las razones de las mismas a la Superintendencia de Industria y Comercio.

5. La Superintendencia de Industria y Comercio podrá revocar la acreditación de un organismo 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 dicho organismo infringe la presente Ley.

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

Artículo 60. Certificación.

1. La Autoridad de Control competente 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. Además del cumplimiento de los responsables o encargados del tratamiento sujetos a la presente ley, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el numeral 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos a la presente ley en virtud de los establecido en el artículo 3, en el marco de transferencias de datos personales a terceros países u organizaciones internacionales en virtud del artículo 64, apartado 2, literal e).

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.

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

4. La certificación a que se refiere el presente artículo no limitará la responsabilidad 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 Superintendencia de Industria y Comercio de conformidad con los artículos 69 y 74.

5. La certificación en virtud del presente artículo será expedida por las entidades de certificación a que se refiere el artículo 61 o por la Superintendencia de Industria y Comercio, sobre la base de los criterios aprobados por esta, de conformidad con el artículo 75, literal e).

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación darán a la entidad de certificación mencionada en el artículo 61, o en su caso a la Superintendencia de Industria y Comercio, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado de 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 a que se refiere el artículo 61, o en su caso por la Superintendencia de Industria y Comercio, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

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

Artículo 61. Entidad de certificación.

1. Sin perjuicio de las funciones y poderes de la Superintendencia de Industria y Comercio en virtud de los 69 y 74, las entidades de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones, una vez informada la Delegatura para la Protección de Datos Personales, a fin de que esta pueda ejercer, si así se requiere, sus facultades en virtud del artículo 77. La Superintendencia de Industria y Comercio garantizará que dichas entidades de certificación sean acreditadas por ella o por el organismo competente que conforma el Subsistema Nacional de la Calidad, bajo las siguientes condiciones:

a) Previa solicitud, la Superintendencia de Industria y Comercio o el organismo competente que conforma el Subsistema Nacional de la Calidad con arreglo a la norma EN ISO/IEC 17065/2012, acreditará a las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio para ser entidades de certificación;

b) Las entidades deben contar con la capacidad y elementos técnicos necesarios para la emisión de certificados sobre el nivel adecuado de pericia en materia de protección de datos.

c) Deben contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación.

d) Deben demostrar, a satisfacción de la Superintendencia de Industria y Comercio o el organismo competente que conforma el Subsistema Nacional de la Calidad, su independencia y su pericia en relación con el objeto de la certificación;

e) Deben comprometerse a respetar los criterios mencionados en artículo 60 numeral 5, y aprobados por la Superintendencia de Industria y Comercio de conformidad con el artículo 75 literal e);

f) Deben establecer procedimientos para la emisión, la revisión periódica y la revocatoria de certificaciones, sellos y marcas de protección de datos;

g) Deben establecer procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacerlo de forma transparente para los titulares y el público en general, y

h) Deben demostrar, a satisfacción de la Superintendencia de Industria y Comercio o el organismo competente que conforma el Subsistema Nacional, que sus funciones y cometidos no dan lugar a conflicto de intereses.

2. La acreditación de las entidades de certificación a que se refieren el numeral 1 del presente artículo se realizará sobre la base de los criterios aprobados por la Superintendencia de Industria y Comercio a través de la Delegatura para la Protección de Datos Personales de conformidad con el artículo 75 literal d) y e). En caso de acreditación de conformidad con el numeral 1, literal a), del presente artículo, estos requisitos se complementarán con las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.

3. Las entidades de certificación a que se refiere el numeral 1 serán responsables de la correcta evaluación a efectos de certificación o revocatoria de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento de la presente ley. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando la entidad de certificación cumpla los requisitos establecidos en el presente artículo.

4. Las entidades de certificación a que se refiere el numeral 1 comunicarán a la Superintendencia de Industria y Comercio a través de la Delegatura para la Protección de Datos Personales los motivos de la emisión de la certificación solicitada o de su revocatoria.

5. La Superintendencia de Industria y Comercio a través de la Delegatura para la Protección de Datos Personales hará públicos los requisitos a que se refiere el numeral 1 del presente artículo y los criterios a que se refiere artículo 60 numeral 5, en una forma fácilmente accesible. La Superintendencia de Industria y Comercio 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.

6. No obstante lo dispuesto en el Título VII, la Superintendencia de Industria y Comercio podrá revocar la acreditación a una entidad de certificación en virtud del numeral 1 del presente artículo, 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.

TITULO IV

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Artículo 62. Principio 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.

Artículo 63. Transferencias basadas en una declaración de conformidad

1. Podrá realizarse una transferencia de datos personales a un destinatario y/o encargado fuera del territorio nacional u organización internacional cuando la Superintendencia de Industria y Comercio a través de su Delegatura para la Protección de Datos Personales haya decidido que el tercer país, territorio o uno o varios sectores específicos de ese país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Superintendencia de Industria y Comercio tendrá en cuenta, en particular, los siguientes elementos:

a) El Estado de Derecho, el respeto de los derechos humanos y las garantías fundamentales, la legislación pertinente, tanto general como especial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias internacionales, la jurisprudencia, así como el reconocimiento a los titulares cuyos datos personales estén siendo transferidos, de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivas;

b) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el país o a las cuales esté sujeta una organización internacional, 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 los titulares en el ejercicio de sus derechos, y de cooperar con la Superintendencia de Industria y Comercio, y;

c) Los compromisos internacionales asumidos por el país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Superintendencia de Industria y Comercio, tras haber evaluado si existe un nivel adecuado de protección, podrá decidir, mediante una declaración de conformidad, que un tercer país, un territorio o uno o varios sectores específicos del tercer país, o una organización internacional garantizan un nivel de protección adecuado de conformidad con lo dispuesto en el numeral 2 del presente artículo. La declaración de conformidad 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. La misma especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el numeral 2, literal b), del presente artículo.

4. La Superintendencia de Industria y Comercio revisará periódicamente los acontecimientos en países y organizaciones internacionales que puedan afectar a la efectiva aplicación de las declaraciones de conformidad adoptadas con arreglo al numeral 3 del presente artículo.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el numeral 3 del presente artículo, muestra 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 el numeral 2, la Superintendencia de Industria y Comercio, mediante acto

administrativo revocará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la declaración de conformidad a que se refiere el numeral 3 del presente artículo.

6. La Superintendencia de Industria y Comercio habilitará canales de revisión para el tercer país u organización internacional en aras de subsanar la situación que dé lugar a la decisión adoptada de conformidad con el numeral 5.

7. Toda decisión, en virtud del numeral 5 del presente artículo, se entenderá sin perjuicio de las transferencias de datos personales a un tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, u organización internacional de que se trate en virtud de los artículos 64 a 67.

8. La Superintendencia de Industria y Comercio publicará en su página web o cualquier otro medio de difusión que considere apropiado una lista de países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantice, o ya no, un nivel de protección adecuado.

Artículo 64. Transferencias mediante garantías adecuadas

1. A falta de declaración de conformidad en los términos del artículo 63, el responsable o el encargado del tratamiento sólo podrá transmitir 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 requiere ninguna autorización expresa de la Superintendencia de Industria y Comercio, por:

a) Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) Normas corporativas vinculantes de conformidad con el artículo 65;

c) Cláusulas tipo de protección de datos adoptadas por la Superintendencia de Industria y comercio.

d) Un código de conducta aprobado con arreglo al artículo 58, 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, o

e) Un mecanismo de certificación aprobado con arreglo al artículo 60, 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 conformidad expedida por la Superintendencia de Industria y Comercio, 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, o

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

Artículo 65. Normas corporativas vinculantes.

1. La Superintendencia de Industria y Comercio 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 esta ley;

c) Cumplan los requisitos establecidos en la presente ley.

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 tratamientos 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, en particular en lo que respecta a las disposiciones contempladas en las literales d) y e) del presente numeral, además de los artículos 20 y 21;

g) Las funciones de todo oficial de protección de datos designado de conformidad con el artículo 53, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las

normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

h) Los procedimientos de reclamación;

i) Los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta 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 para 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 Superintendencia de Industria y Comercio;

k) Los mecanismos para informar a la Superintendencia de Industria y Comercio 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, y

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

3. La Superintendencia de Industria y Comercio podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes en virtud de lo dispuesto en el presente artículo.

Parágrafo primero: Las Normas Corporativas Vinculantes solo podrán ser sometidas a la aprobación de la Superintendencia de Industria y Comercio, como autoridad nacional 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 Superintendencia de Industria y Comercio solo estarán vigentes a partir de la fecha en que esta emita su certificación y es, a partir de ese momento, que pueden iniciar a aplicarse.

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

Artículo 66. Transferencias o comunicaciones no autorizadas por la Ley.

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país requirente y Colombia, sin perjuicio de otros motivos para la transferencia al amparo del presente Título.

Artículo 67. Excepciones para situaciones específicas.

1. En ausencia de una declaración de conformidad según lo establecido en el artículo 63 numeral 3, o de garantías adecuadas de conformidad con artículo 64, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

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 conformidad 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 que tenga por objeto facilitar información y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 63 o 64 , incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el numeral primero del presente artículo, solo se podrá llevarse a cabo si no es repetitiva, afecta solo a un número limitado de

titulares, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y garantías del titular, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos de conformidad con el artículo 14 numerales 4 y 5 de la presente ley y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la Superintendencia de Industria y Comercio de la transferencia.

Además de la información a que hacen referencia los artículos 20 y 21, el responsable del tratamiento informará al titular de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el numeral 1 literal g) del presente artículo, no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el numeral 1, el párrafo primero, literales a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. En ausencia de una declaración por la que se constate la conformidad de la protección de los datos, la Superintendencia de Industria y Comercio, 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 indicados en el artículo 43 de la presente Ley, la evaluación y las garantías apropiadas a que se refiere el numeral 1, inciso segundo, del presente artículo.

Artículo 68. Cooperación internacional en el ámbito de la protección de datos personales

En relación con terceros países y organizaciones internacionales, la Superintendencia de Industria y Comercio 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.

TITULO V

AUTORIDADES DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Artículo 69. Autoridad Nacional de Protección de Datos.

1. La Superintendencia de Industria y Comercio ejercerá la función de autoridad nacional de control en materia 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. Los jueces en sede de tutela sustituirán la competencia de la Superintendencia de Industria y Comercio, para efectos de proteger los derechos fundamentales asociados a la protección de datos personales, teniendo en cuenta lo dispuesto en el artículo 86 de la Constitución Política de Colombia y el artículo 37 del Decreto 2591 de 1991, sin que esto signifique pérdida de la facultad investigativa y sancionatoria a la que se refiere lo artículos 76 y 77 de esta Ley.

3. Sin perjuicio de lo mencionado en los numerales anteriores, cuando el tratamiento inadecuado o uso indebido de una determinada base de datos de lugar a un comportamiento delictivo, la autoridad competente será la Fiscalía General de la Nación, quien será la encargada de la persecución penal de dichas conductas.

Artículo 70. Competencia de la Superintendencia Financiera de Colombia como autoridad de control.

Para los casos previstos en el inciso segundo del artículo 17 de la Ley 1266 de 2008 o la que en su momento la adicione, modifique o sustituya, en los que la fuente, usuario y operador de información sea una sociedad vigilada por la Superintendencia Financiera de Colombia, será

dicha entidad quien ejercerá las funciones de vigilancia y control de conformidad con las facultades que le sean propias.

La Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia actuarán de manera autónoma e independiente a efectos de asegurar la protección del derecho fundamental a la protección de los datos personales de los titulares de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países en estas materias.

Artículo 71. Colaboración armónica entre las autoridades de inspección, vigilancia y control. La Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia actuarán bajo el principio de colaboración armónica regulado en el artículo 113 de la Constitución Política de Colombia, en lo que respecta a las facultades a ellas conferidas en materia de protección de datos personales.

Asimismo, colaborarán armónicamente con otras autoridades administrativas o judiciales con facultades de investigación siempre que pueda vislumbrarse una conducta objeto de sanción según su competencia.

Parágrafo. Siempre que la Delegatura para la Protección de Datos determine en sus investigaciones que puede haberse cometido una conducta delictiva, deberá compulsa copias de los resultados a la Fiscalía General de la Nación para que ésta indague. En todo caso, la fiscalía general de la Nación comunicará a la Delegatura los resultados de sus pesquisas con el fin de retroalimentar la investigación iniciada por esta, siempre que no se vea afectada la reserva de la investigación penal.

Artículo 72. Estructura de la Superintendencia de Industria y Comercio como Autoridad Nacional para la Protección de Datos. La estructura de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio se encuentra establecida en el Decreto 4886 de 2011 modificado y adicionado por el Decreto 092 de 2022 o la que en su momento la adicione, modifique o sustituya, a través de la cual se ejercerá la vigilancia y control del cumplimiento de lo establecido en la presente ley.

Artículo 73. Competencia de la Superintendencia de Industria y Comercio como Autoridad Nacional para la Protección de Datos.-La Superintendencia de Industria y Comercio a través de la Delegatura para la Protección de Datos Personales tendrá las competencias que a ella han sido designadas por el Decreto 4886 de 2011 modificado y adicionado por el Decreto 092 de 2022 o la que en su momento la adicione, modifique o sustituya, además de las asignadas por la presente ley.

Artículo 74. Poderes de la Autoridad Nacional de Protección de Datos Personales. La Superintendencia de Industria y Comercio a través de la Delegatura para la Protección de Datos Personales tendrá a su cargo los poderes consultivos, investigativos, correctivos y

sancionatorios, los cuales se desarrollarán en cumplimiento de las funciones otorgadas en la presente ley.

Para el uso de los poderes conferidos, deberán tenerse en cuenta las garantías constitucionales y principios generales que regulan el actuar de la Superintendencia de Industria y Comercio, garantizando en todo momento el derecho al debido proceso y demás garantías procesales.

Artículo 75. Poderes consultivos. La Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales dispondrá de los poderes consultivos indicados a continuación:

a) Asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 52;

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 58 numeral 5;

d) Acreditar los organismos de certificación con arreglo al artículo 61;

e) Expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 60 numeral 5;

f) Adoptar las cláusulas tipo de protección de datos contempladas en el artículo 41 numeral 8 y el artículo 64 numeral 2, literal c);

g) Autorizar las cláusulas contractuales indicadas en el artículo 64 numeral 3, literal a);

h) Autorizar los acuerdos administrativos contemplados en el artículo 64 numeral 3, literal b);

i) Aprobar normas corporativas vinculantes de conformidad con lo dispuesto artículo 65.

Artículo 76. Poderes Investigativos. La Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales dispondrá de los poderes de investigación indicados a continuación:

a) Ordenar a los responsables y encargados del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) Llevar a cabo visitas de inspección, de oficio o a solicitud de parte;

c) Llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 60 numeral 7;

d) Notificar a los responsables y encargados del tratamiento las presuntas infracciones de la presente ley;

e) 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 a la normativa vigente.

Artículo 77. Poderes correctivos y sancionatorios. La Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales dispondrá de los poderes correctivos indicados a continuación:

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

b) Imponer multas de carácter personal o institucional a los responsables y encargados del tratamiento, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido lo establecido en el Título VII y la presente ley.

c) Imponer sanciones operativas y medidas correctivas a los responsables y encargados del tratamiento, además o en lugar de las mencionadas en el presente artículo, cuando las operaciones de tratamiento hayan infringido lo establecido en el Título VII y la presente ley.

d) Ordenar a los responsables y encargados del tratamiento que atiendan las solicitudes de ejercicio de los derechos de los titulares en virtud de la presente ley;

e) Ordenar a los responsables y encargados del tratamiento que se ajusten a las disposiciones de la presente ley, cuando proceda, de una determinada manera y dentro de un plazo específico;

f) Ordenar al responsable del tratamiento que comunique a los titulares los incidentes de seguridad de los datos personales;

g) Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

h) Ordenar los derechos establecidos en los artículos 25, 26, 27, 28, 29 y 30 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo al artículo 27 numeral 2 y el artículo 31 de la presente ley;

i) Retirar u ordenar al organismo de certificación que retire o que no emita una certificación con arreglo a los artículos 60 y 61 si no se cumplen o dejan de cumplirse los requisitos para ello;

j) Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

TITULO VI

DISPOSICIONES RELATIVAS A SITUACIONES ESPECÍFICAS DE TRATAMIENTO

CAPÍTULO I
TRATAMIENTOS EN EL EJERCICIO DE LA LIBERTAD DE EXPRESIÓN Y DE INFORMACIÓN

Artículo 78. Garantías para el tratamiento y libertad de expresión y de información.

1. Los tratamientos realizados bajo el amparo de los derechos de libertad de expresión y de información no deben vulnerar los derechos de protección de datos personales de los titulares.

2. La difusión de información con fines periodísticos que incluyan datos de carácter personal debe tener en cuenta:

a) La veracidad de la información está mediada por un límite de razonabilidad.
b) La minimización de los datos relevantes para la difusión de la información.
c) Hacer referencia a datos personales sobre hechos pasados de la vida del titular, cuando éstos tengan incidencia sobre la situación actual que se pretende informar.

3. Las víctimas o sobrevivientes de violencias basadas en género, acoso sexual, actos de discriminación por cualquier razón y otras formas de abuso, o sus representantes, tendrán derecho a denunciar por cualquier medio de difusión dichos actos. Las denuncias públicas de estos actos constituyen un ejercicio legítimo de la libertad de expresión que goza de protección constitucional reforzada, siempre y cuando, informen y sensibilicen a la sociedad sobre problemáticas de interés público y permitan crear redes de solidaridad entre las víctimas para la protección de sus derechos fundamentales.

CAPÍTULO II

TRATAMIENTOS DE DOCUMENTOS PÚBLICOS

Artículo 79. Tratamiento y acceso a documentos públicos.

1. Los datos personales de documentos públicos en posesión de algún ente de naturaleza pública o un particular que se encuentre en ejercicio de una misión para el interés público, podrán ser comunicados por ésta, de conformidad con la legislación nacional, a fin de conciliar el derecho

de las personas a acceder a documentos públicos y el derecho a la protección de los datos personales en virtud de la presente ley.

2. Se limita el derecho de acceso a los documentos públicos que cuenten con reserva legal y los demás mencionados en el artículo 24 de la Ley 1437 de 2011 o demás normas que la modifiquen, complementen o sustituyan.

3. En virtud del principio de transparencia, las decisiones que rechacen el acceso de los titulares a información pública deberán hacerse en los términos descritos en el Título III de la Ley 1712 de 2014 o demás normas que la modifiquen, complementen o sustituyan.

Artículo 80. Tratamiento de la Cédula de Ciudadanía.

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 de acuerdo con el artículo 15 numeral 2, 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 bases de datos 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 del artículo 47 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 autorizada.

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 los artículos 24 al 34, 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.

CAPÍTULO III

VIDEOVIGILANCIA

Artículo 81. Tratamientos con fines de videovigilancia.

1. Las personas naturales o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de videovigilancia con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior. No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de 30 días desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 45 de esta ley, salvo en el caso que las imágenes deban o hayan sido puestas a disposición judicial.

4. El deber de información previsto en el artículo 19 de la presente ley se entenderá cumplido mediante la colocación de un medio informativo en lugar suficientemente visible identificando los establecido en el artículo 22 y la forma de acceder a la política de tratamiento de la información completa. También podrá incluirse en el medio informativo un código de conexión o dirección de internet a esta información. En todo caso, el responsable del tratamiento deberá mantener a disposición de los titulares la información a la que se refiere el artículo 19 de la presente ley.

5. Los sistemas de videovigilancia instalados por una persona natural que solamente captan imágenes en el interior de su propio domicilio se consideran excluidos del ámbito de aplicación de la presente ley de conformidad con del artículo 2 numeral, 2 literal b). Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de sistemas de videovigilancia por la Fuerza Pública, o por el INPEC y órganos competentes para la vigilancia y control en los centros penitenciarios, o para el control, regulación, vigilancia y disciplina del tránsito, se regirá por las normas especiales que les sea de aplicación.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en el Decreto 356 de 1994, el Estatuto de Vigilancia y Seguridad Privada.

8. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares en los que exista una expectativa razonable de privacidad o destinados al descanso o esparcimiento de los titulares, tales como vestuarios, aseos y análogos. La utilización de sistemas similares a los referidos para la grabación de sonidos debe estar autorizado por la ley o por una autoridad competente.

CAPÍTULO IV

TRATAMIENTOS DE PUBLICIDAD Y LÍNEA ÉTICA

Artículo 82. Sistemas de exclusión publicitaria.

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

2. Podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los titulares. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los titulares limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas.

3. Cuando un titular manifieste a un responsable su deseo de que sus datos no sean tratados para el envío de comunicaciones comerciales, este deberá darle trámite al ejercicio de derechos e informarle de la existencia del Registro de Número Excluidos administrado por la Comisión de Regulación de Comunicaciones.

4. Quienes pretendan realizar comunicaciones de marketing y publicidad, sin haber obtenido el consentimiento del titular de conformidad al artículo 8 de esta ley, deberán previamente consultar el sistema de exclusión publicitaria.

5. El Registro de Números Excluidos continuará vigente y se regirá de conformidad con lo que establezcan las leyes y las disposiciones aplicables a este.

Artículo 83. Línea Ética

1. Será lícita la creación y mantenimiento de líneas éticas a través de los cuales pueda ponerse en conocimiento de la entidad pública y/o privada, incluso anónimamente, la comisión en el interior de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa vigente general o específica que le fuera aplicable. Los trabajadores y terceros deberán ser informados acerca de la existencia de las líneas éticas.

2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incorporados o no al interior de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan. Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativos, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

4. Los datos de quien formule la comunicación y de los trabajadores y terceros deberán conservarse en las líneas éticas únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión de la línea Ética, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del Programa de Ética Empresarial. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 45 de esta ley.

Transcurrido el término mencionado en el inciso anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme al numeral 2 de este artículo, la investigación de los hechos denunciados, no conservándose en la propia línea ética.

Paragráfo Primero: Los numerales segundo y tercero del presente artículo también serán de aplicación al procedimiento interno creado para prevenir, corregir y sancionar el Acoso Laboral.

Parágrafo Segundo: Lo enunciado en el presente artículo será de aplicación a las líneas éticas que pudieran crearse en las Administraciones Públicas.

CAPÍTULO V

TRATAMIENTOS EN ÁMBITO LABORAL

Artículo 84 Tratamiento en ámbito laboral

En el ámbito de las relaciones laborales, el empleador debe cumplir además de las obligaciones contenidas en esta ley, las siguientes:

1. Cuando la base jurídica que justifique el tratamiento de los datos del empleado sea el consentimiento, además de cumplir con las condiciones contempladas en el artículo 8 debe:
    a. Ser recogido separadamente del contrato de trabajo y de otros documentos necesarios para la ejecución de la relación laboral.
    b. Debe ser individual, no admitiéndose consentimientos plurales mediante la negociación colectiva.
2. El empleador debe incluir en el reglamento interno de trabajo las obligaciones y prohibiciones en relación con el tratamiento de los datos de carácter personal que tenga que realizar el trabajador.
3. El empleador brindará formación en materia de protección de datos a sus trabajadores.
4. El empleador podrá adoptar las prescripciones de orden y seguridad que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta los trabajadores en situación de discapacidad física, psíquica o mental.

PARÁGRAFO*:* El consentimiento del titular en las etapas previas, durante o posterior a la relación laboral, no será válido cuando se proporciona en un contexto de desequilibro claro entre el titular y el responsable del tratamiento, los titulares podrán negarse a otorgarlo sin consecuencias adversas.

CAPÍTULO VI

TRATAMIENTOS CON FINES DE ARCHIVO EN INTERÉS PÚBLICO, INVESTIGACIÓN CIENTÍFICA, HISTÓRICA O ESTADÍSTICA

Artículo 85. Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística.

1. El tratamiento con fines de archivo en interés público, investigación científica, histórica o estadística estará sujeto a las garantías adecuadas, con arreglo a la presente Ley. Dichas garantías harán que se disponga de medidas técnicas y organizativas, que garantice el respeto del principio de minimización de los datos personales y la seudonimización de estos. La seudonimización, podrá realizarse siempre que de esa forma puedan alcanzarse los fines, o

cuando esos fines pueden alcanzarse mediante un tratamiento ulterior que aplique técnicas de anonimización.

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos podrá establecer excepciones a los derechos contemplados en los artículos 24, 25, 30 y 33, sujetas a las condiciones y garantías indicadas en el numeral 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

3. Cuando se traten datos personales con fines de archivo en interés público, se podrá prever excepciones a los derechos contemplados en los artículos 24, 25, 30, 31, 32 y 33 sujetas a las condiciones y garantías citadas en el numeral 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

4. En caso de que el tratamiento a que hacen referencia los numerales 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos numerales.

CAPÍTULO VII

TRATAMIENTOS RELACIONADOS CON LA ACTIVIDAD COMERCIAL Y PROFESIONAL

Artículo 86. Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 7 numeral 1, literal f) de la presente ley, el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas naturales que presten servicios para una persona jurídica siempre que se cumplan los siguientes requisitos:

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el titular preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales, contratistas y/o los profesionales independientes, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas naturales.

3. Los responsables o encargados del tratamiento a los que se refiere los artículos 39 y 40 de la Ley 489 de 1998, Rama judicial, Rama legislativa, Órganos de Control, Organización electoral, Fundaciones de iniciativa pública, y los particulares que cumplen funciones públicas o administrativas, podrán también tratar los datos mencionados en los dos numerales anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

4. Cuando los datos personales se obtengan directamente del titular o de la persona jurídica en la que éste preste sus servicios, el responsable del tratamiento no estará obligado a cumplir con el deber establecido en el artículo 20 de la presente ley, siempre y cuando se cumpla con los numerales 1 y 2 del presente artículo y se garantice el ejercicio de derechos de los artículos 24 a 34 de la presente ley.

Artículo 87. Tratamientos relacionados con la realización de determinadas operaciones mercantiles.

1. Salvo prueba en contrario, se presumirán lícitos el acceso a los datos por parte de un tercero con carácter previo al desarrollo de cualquier operación mercantil, siempre que los tratamientos fueran necesarios para el buen fin de la operación.

El acceso se realizará mediante la firma de un contrato que contenga como mínimo las siguientes garantías:

a) Identificación de los datos a los que accederá el tercero;
b) Asegurar que tratará los datos personales únicamente para analizar o realizar la operación mercantil;
c) 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 con el tercero;
d) Tomar todas las medidas necesarias de conformidad con el artículo 47;
e) Pedir autorización al responsable del tratamiento en caso de recurrir el tercero a un encargado del tratamiento, quien debe comprometerse a cumplir lo estipulado en los numerales anteriores.

2. En el caso de que la operación no llegara a concluirse, el tercero y su encargado deberán proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 45 de la presente ley.

3. En el caso que se concluya la operación mercantil se producirá una modificación del responsable del tratamiento como consecuencia de la fusión, escisión, adquisición de acciones o cualquier otra forma de operación mercantil, o cualquier operación de reestructuración

societaria de análoga naturaleza, contemplada por la normativa mercantil o societaria, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 19 de la presente ley.

Artículo 88. Tratamiento de datos en el ámbito de la función estadística pública.

1. El tratamiento de datos personales llevado a cabo por las entidades que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica y en la presente ley.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 7 numeral 1, literal e) de la presente ley, en los casos en que la estadística para la que se requiera la información venga incluida en los instrumentos de programación estadística previstos en la ley.

De conformidad con lo dispuesto en la ley serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los titulares, los datos a los que se refieren los artículos 15, 16 y 17 de la presente ley, salvo que los mismos se recolecten mediante técnicas especiales que garanticen la imposibilidad de asociar o identificar al titular de los datos.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los titulares de los derechos establecidos en los artículos 24 a 34 de la presente ley cuando los datos se encuentren amparados por reserva legal.

CAPÍTULO VIII

TRATAMIENTO REALIZADO POR TECNOLOGÍAS DE APRENDIZAJE, RASTREO Y NEUROTECNOLOGÍAS

Artículo 89. Inteligencia artificial. Las empresas y organizaciones que utilicen Inteligencias Artificiales u otras tecnologías y/o sistemas informáticos con capacidad de aprendizaje, autonomía y toma de decisiones, y gran capacidad de procesamiento y análisis avanzados para el tratamiento de datos personales deben cumplir con los principios y disposiciones establecidos en la presente ley, y en particular:

1. El procesamiento de datos personales debe priorizar la aplicación de mecanismos de anonimización o disociación.
2. En caso de que sea necesario identificar al titular de los datos para el entrenamiento de la tecnología se debe observar la protección de datos desde el diseño y por defecto.
3. Se deberá realizar evaluaciones de impacto para identificar y mitigar los riesgos asociados al uso de estas tecnologías en el procesamiento de datos personales.

La Superintendencia de Industria y Comercio será responsable de mantener una lista actualizada de las Inteligencias Artificiales o tecnologías similares prohibidas. Las empresas y organizaciones que no cumplan con estas disposiciones estarán sujetas a las sanciones establecidas en la presente ley.

Artículo 90. Neuroderechos. Quienes desarrollen o hagan uso de la neurotecnologia deberán garantizar la protección de los derechos fundamentales a la intimidad de las personas, por lo que se establecen las siguientes obligaciones:

1. Se prohíbe cualquier forma de manipulación o coerción que comprometa la integridad cerebral o afecte negativamente la salud mental. La aplicación de la neurotecnología respetará la dignidad y la integridad física y psíquica de las personas.
2. Los neurodatos se considerarán como datos personales sensibles y se debe implantar las medidas de seguridad en atención al riesgo de conformidad al artículo 47.
3. Se deberá realizar evaluaciones de impacto para identificar y mitigar los riesgos asociados al uso de las neurotecnologías en el procesamiento de datos personales.
4. Para cualquier intervención o recopilación de datos relacionados con la actividad cerebral la base jurídica que legitima el tratamiento será el consentimiento y/o el interés vital. En ningún caso la aplicación de las anteriores bases jurídicas puede considerarse consentimiento informado y para ello debe consultarse la normativa que regula la relación médico-paciente.
5. El deber de información además de cumplir los requisitos de la presente ley debe contener los objetivos, riesgos y beneficios de la obtención de los datos.
6. El uso de tecnologías que afecten la actividad cerebral estará sujeto a requisitos y restricciones proporcionales, con el propósito de evitar la discriminación, estigmatización o manipulación indebida.
7. Los datos obtenidos mediante neurotecnología no pueden ser utilizados para la explotación económica.
8. Queda prohibido cualquier neurotecnología que pueda ocasionar la pérdida de identidad personal a través de la conexión a redes digitales externas.

La Superintendencia de Industria y Comercio promoverá la concientización y educación sobre el uso responsable de las neurotecnologías, con el fin de fomentar la comprensión de los riesgos potenciales y salvaguardar la Identidad personal, Libre albedrío, Privacidad mental, Acceso equitativo, Protección contra los sesgos. También, la Superintendencia de Industria y Comercio establecerá los mecanismos de supervisión y control para garantizar el cumplimiento de las obligaciones en materia de neuroderechos, incluyendo la revisión de los procedimientos de consentimiento y el monitoreo de la recopilación y uso de datos cerebrales, con sanciones por incumplimiento.

Artículo 91. Tecnologías de rastreo.

1. Es necesario obtener el consentimiento del usuario para utilizar las tecnologías de rastreo. Las acciones de aceptar o rechazar tienen que presentarse en un lugar y formato destacados, y ambas acciones deben estar al mismo nivel, sin que sea más complicado rechazarlas que aceptarlas. No se considerará acción afirmativa utilizar los servicios sin manifestar la aceptación o 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 usuario, están exentas del requisito de obtener el consentimiento del usuario.

Las tecnologías consideradas técnicamente necesarias cumplen con los siguientes criterios:

a) Son temporales y se eliminan al cerrar el navegador. Se utilizan para mantener la sesión del usuario, establecer parámetros libremente elegidos por el usuario 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 iniciada y autenticar al usuario como registrado mientras navega por el sitio web.

d) Se utilizan para garantizar la seguridad de las interacciones en el sitio web, detectando actividades potencialmente maliciosas o no autorizadas.

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

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

TITULO VII

INDEMNIZACIÓN Y RÉGIMEN SANCIONATORIO

CAPÍTULO I

DISPOSICIONES GENERALES Y GRADUACIÓN DE LAS SANCIONES

Artículo 92. 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 legales 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 Superintendencia de Industria y Comercio 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 93. 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. Los representantes de los responsables o encargados de los tratamientos, no establecidos en el territorio nacional.

4. Las entidades de certificación.

5. 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 94. Condiciones generales para la imposición de sanciones.

1. La Superintendencia de Industria y Comercio garantizará que la imposición de las sanciones con arreglo al presente Título por las infracciones a la presente ley y aquellas indicadas en los artículos 96, 97 y 98 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 77. 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) Cualquier medida tomada por el responsable o encargado del tratamiento para contener y mitigar los daños y perjuicios sufridos por los titulares;
f) El grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 38 y 47;
g) La reincidencia en la comisión de la infracción por el responsable o el encargado del tratamiento;
h) El grado de cooperación con la autoridad de control con el fin de contener y mitigar los posibles efectos adversos de la infracción;
i) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Autoridad de Control;

j) Las categorías de los datos de carácter personal afectados por la infracción;
k) La afectación a los derechos de los menores de edad;
l) La posibilidad de que la conducta del titular hubiera podido inducir a la comisión de la infracción;
m) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente;
n) La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
o) El incumplimiento de las medidas indicadas en el artículo 77 cuando hayan sido ordenadas previamente contra el responsable o el encargado en relación con el mismo asunto;
p) La renuencia o desacato a cumplir las órdenes impartidas por la Autoridad de Control;
q) La adhesión a códigos de conducta en virtud del artículo 58 o a mecanismos de certificación aprobados con arreglo al artículo 60;
r) Disponer, cuando no fuere obligatorio, de un Oficial de protección de datos;
s) El reconocimiento o aceptación expresos que haga el responsable o encargado del tratamiento sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar;
t) El sometimiento por parte del responsable o encargado, 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) Si las infracciones fueron realizadas con el propósito de cometer alguna de las conductas tipificadas por la Ley 1273 de 2009 o cualquiera que la adicione, modifique o sustituya;
v) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso.

3. Si un responsable o un encargado del tratamiento incumpliera de forma dolosa o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, cualquiera de las obligaciones contenidas en la presente ley, la cuantía total de la sanción no será superior a la cuantía prevista para las infracciones consideradas muy graves.

4. En el evento en el cual la Autoridad de Control advierta un presunto incumplimiento de una entidad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva a la procuraduría delegada competente para ello.

5. El ejercicio por la Superintendencia de Industria y Comercio de sus poderes en virtud del presente artículo estará sujeto a las garantías del debido proceso.

Parágrafo: En virtud del principio *non bis in idem*, en caso de existir un pronunciamiento previo y de fondo en relación con el mismo sujeto obligado, idénticos hechos e idéntico bien jurídico, la Superintendencia de Industria y Comercio se abstendrá de emitir una nueva decisión.

CAPÍTULO II

DE LAS INFRACCIONES EN MATERIA DE PROTECCIÓN DE DATOS

Artículo 95. Infracciones. Constituyen infracciones los actos y conductas que resulten contrarios a la aplicación de los principios y obligaciones de la presente ley, en especial, aquellas contempladas en los artículos 96, 97 y 98.

Artículo 96. Infracciones consideradas muy graves.

Se consideran muy graves las infracciones que supongan una vulneración sustancial de los artículos de la presente ley y, en particular, las siguientes:

1. El tratamiento de datos personales vulnerando los principios básicos para el tratamiento, bases de legitimación, condiciones para el consentimiento o el tratamiento de datos sensibles en virtud de los artículos 6, 7, 8, 15 y 90;
2. El tratamiento de datos personales de un menor de edad sin recabar su consentimiento o el de sus representantes legales en las condiciones aplicables establecidas en el artículo 9 de la presente ley;
3. El tratamiento de datos personales relativos a delitos y condenas penales o medidas de aseguramiento conexas fuera de los supuestos permitidos por el artículo 16 de la presente ley;
4. El tratamiento de datos personales relacionados con multas e infracciones fuera de los supuestos permitidos por el artículo 17 de la presente ley;
5. La omisión del deber de informar al titular acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 20 y 21 de la presente Ley;
6. La vulneración de los derechos de los titulares en virtud de los artículos 24 a 34;
7. El impedimento, obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 24 a 34 de la presente ley;
8. La vulneración del principio de confidencialidad establecido en el artículo 6 de esta ley;
9. Las transferencias de datos personales a un destinatario en un tercer país o una organización internacional cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 63 a 67;
10. Toda obligación en virtud del Título VI;
11. El incumplimiento de una orden dictada por la Superintendencia de Industria y Comercio de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de esta con arreglo o el no facilitar acceso en incumplimiento del artículo 77;
12. El incumplimiento de las resoluciones de la autoridad de control en virtud del artículo 75;
13. El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 45 de esta ley cuando la misma sea exigible;

14. No facilitar el acceso de los funcionarios de la Superintendencia de Industria y Comercio a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la misma para el ejercicio de sus poderes de investigación en virtud del artículo 76;
15. La resistencia u obstrucción del ejercicio de la función inspectora por la Superintendencia de Industria y Comercio;
16. La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

Artículo 97. Infracciones consideradas graves.

Se consideran graves las infracciones que supongan una vulneración sustancial de los artículos de la presente ley y, en particular, las siguientes:

1. El impedimento, la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del titular, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación;
2. La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, en los términos exigidos por el artículo 38 de la presente ley;
3. La falta de adopción de aquellas medidas técnicas y organizativas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, en los términos exigidos por el artículo 38 de la presente ley;
4. La falta de adopción o falta de debida diligencia en la aplicación de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 47 de la presente ley;
5. El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio nacional, conforme a lo previsto en el artículo 40 de la presente ley;
6. La falta de atención por el representante del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de control o por los titulares;
7. La contratación por el responsable del tratamiento de un encargado que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Título III de la presente ley;
8. Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 41 numeral 3 de la presente ley;

9. La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles;
10. La infracción por un encargado del tratamiento al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 41 numeral 10 de la presente ley;
11. No disponer del registro de actividades de tratamiento o incumplir cualquiera de las obligaciones derivadas del registro de actividades como lo establece en el artículo 43 de la presente ley;
12. El incumplimiento por parte del responsable o encargado del tratamiento del deber de notificar un incidente de seguridad en los términos del artículo 49 de la presente ley;
13. El incumplimiento del deber de comunicación al titular de un incidente de seguridad de los datos de conformidad con lo previsto en el artículo 50 de la presente ley. Así como la renuencia del responsable del tratamiento que hubiera sido requerido por la autoridad control para llevar a cabo dicha comunicación;
14. El tratamiento de datos personales sin haber llevado a cabo la evaluación de impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible;
15. El tratamiento de datos personales sin haber recibido de la Superintendencia de Industria y Comercio la consulta previa en los casos en que la misma resulte preceptiva conforme al artículo 52 de la presente ley o cuando la ley establezca la obligación de consultar;
16. El incumplimiento de la obligación de designar un Oficial de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 53 de esta ley. Así como, no posibilitar la efectiva participación del mismo en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones;
17. La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado;
18. Obtener la acreditación como organismo de certificación presentando información inexacta y fraudulenta sobre el cumplimiento de los requisitos exigidos por el artículo 61 de la presente ley;
19. El desempeño de funciones que la presente ley reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 61;
20. El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 60 y 61 de la presente ley;
21. El desempeño de funciones que el artículo 59 de la presente ley reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de control;

22. La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso de que se hubiera producido una infracción del código, conforme exige el artículo 59 numeral 4 de la presente ley;

Artículo 98. Infracciones consideradas leves.

Se consideran leves las infracciones de carácter meramente formal de los principios y obligaciones contenidos en la presente ley y, en particular, las siguientes:

1. El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 20 y 21 de la presente ley;
2. La exigencia del pago de una tarifa para facilitar al titular la información exigida por los artículos 20 y 21 o por atender las solicitudes de ejercicio de derechos de los titulares previstos en los artículos 24 a 34 de la presente ley, cuando así lo permita el artículo 19 numeral 5, si la tarifa excediese los gastos administrativos afrontados para facilitar la información o realizar la actuación solicitada;
3. El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 31 de la presente ley;
4. El incumplimiento de la obligación de informar al titular, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento;
5. El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 4 de esta ley;
6. La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los titulares al que se refiere el artículo 39 de la presente ley o la inexactitud en la determinación de las mismas;
7. No poner a disposición de los titulares los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 39 numeral 2 de la presente ley;
8. La falta del cumplimiento de la obligación del encargado de informar al responsable acerca de la posible infracción por una instrucción recibida de este de las disposiciones de la presente ley, o conforme a lo exigido por el artículo 41 numeral 4;
9. Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 43 de la presente ley;
10. La notificación incompleta, tardía o ineficaz a la autoridad de control de la información relacionada con un incidente de seguridad de los datos personales de conformidad con lo previsto en el artículo 49 de la presente ley;

11. El incumplimiento de la obligación de documentar cualquier incidente de seguridad, exigido por el artículo 49 numeral 5 de la presente ley;
12. La redacción de una comunicación al titular de un incidente de la seguridad de los datos que entrañe un alto riesgo para los derechos y garantías fundamentales en un lenguaje complejo y abstracto, contrariando lo exigido por el artículo 50 numeral 2 de la presente ley;
13. Facilitar información inexacta a la Superintendencia de Industria y Comercio, en los supuestos en los que el responsable del tratamiento deba solicitar una consulta previa, conforme al artículo 52 de la presente ley;
14. No publicar los datos de contacto del Oficial de protección de datos, o no comunicarlos a la Superintendencia de Industria y Comercio, cuando su nombramiento sea exigible de acuerdo con el artículo 54 de esta ley;
15. El incumplimiento por los organismos de certificación de la obligación de informar a la Superintendencia de Industria y Comercio de la expedición, renovación o revocatoria de una certificación, conforme a lo exigido por los numerales 1 y 4 del artículo 61 de la presente ley;
16. El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a la Superintendencia de Industria y Comercio acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 59 numeral 4 de la presente ley.

CAPÍTULO III

DE LA IMPOSICIÓN DE SANCIONES

Artículo 99. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los responsables y encargados del Tratamiento las siguientes sanciones:

1. Multas de carácter personal o institucional:

a) Las infracciones consideradas leves descritas en el artículo 98 se sancionarán con multas de 1.000 salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción como máximo o, tratándose de sujetos obligados al Registro de Bases de Datos, de una cuantía equivalente al 1 % como máximo de las utilidades que genere el año fiscal anterior, optando por la de mayor cuantía.
b) Las infracciones consideradas graves descritas en el artículo 97 se sancionarán con multas de 1.500 salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción como máximo o, tratándose de sujetos obligados al Registro de Bases de Datos, de una cuantía equivalente al 2 % como máximo de las utilidades que genere el año fiscal anterior, optando por la de mayor cuantía.
c) Las infracciones consideradas muy graves descritas en el artículo 96 se sancionarán con multas de 2.000 salarios mínimos mensuales legales vigentes al momento de la imposición

de la sanción como máximo o, tratándose de sujetos obligados al Registro de Bases de Datos, de una cuantía equivalente al 4 % como máximo de las utilidades que genere el año fiscal anterior, optando por la de mayor cuantía.

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 Superintendencia de Industria y Comercio;
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 control de acuerdo a las facultades otorgadas por el artículo 77 literal c), dependiendo de cada caso individual y serán independientes de la imposición de multas.

Artículo 100. Prescripción de la Sanción.

1. La Sanciones impuestas por la Superintendencia de Industria y Comercio prescribirán en los siguientes términos:

a) Dos años para las infracciones leves;
b) Tres años para las infracciones graves;
c) Cinco años para las infracciones muy graves.

2. El término de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que la resolución por la que se impone la sanción haya quedado en firme o haya transcurrido el término para recurrirla.

3. La prescripción se interrumpirá por la iniciación del procedimiento de cobro coactivo, volviéndose a reanudar el término si transcurridos seis meses no se hubiere realizado el acto necesario para continuar el trámite, por causa no imputable al infractor.

Artículo 101. Caducidad de la facultad sancionatoria de la Autoridad de Control.

1. La facultad que tiene la Superintendencia de Industria y Comercio para imponer las sanciones a las que se refiere el artículo 99 caducan en el término de tres años.

2. El término para caducidad se contará desde el momento de ocurrido el hecho, la conducta u omisión que pudiere ocasionarlas, término dentro del cual el acto administrativo que impone la sanción debe haber sido expedido y notificado.

3. Cuando se trate de un hecho o conducta continuada, este término se contará desde el día siguiente a aquel en que cesó la infracción y/o la ejecución.

TITULO VIII

RÉGIMEN DE TRANSICIÓN

Artículo 102. **Condiciones del consentimiento.** El consentimiento de los titulares recabados con anterioridad a la expedición de esta ley será válido durante un año posterior a la entrada en vigencia, plazo en el cual el responsable del tratamiento deberá obtenerlos en las condiciones previstas en la presente ley o legitimar el tratamiento en otra base jurídica de conformidad con el artículo 7.

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 103. 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 las bases de datos que existieran al momento de la entrada en vigencia de la presente ley se llevara 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 bases de datos automatizadas.

b) Respecto de las bases de datos no automatizadas que existieran al momento de la entrada en vigencia de la presente ley, en el plazo máximo de un año.

2. Las bases de datos, 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 Superintendencia de Industria y Comercio el responsable de Tratamiento deberá demostrar que está llevando a cabo la implementación de las medidas de seguridad en las bases de datos existentes en el momento de la entrada en vigencia de la presente ley.

Artículo 104. 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 105. Contratos de encargados del tratamiento. Los contratos de encargado del tratamiento suscritos con anterioridad a esta ley serán válidos hasta dieciocho meses después de su entrada en vigencia.
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 41 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 41.

Artículo 106. Transferencias Internacionales. Las declaraciones de conformidad a terceros países realizadas por la Superintendencia de Industria y Comercio tendrán una validez de hasta 2 años contados a partir de la entrada en vigencia de la presente ley.

Artículo 107. 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 Superintendencia de Industria y Comercio 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 108. Vigencia y Derogatorias.

La presente ley entra en vigencia desde su promulgación y será de aplicación obligatoria seis meses 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.

Atentamente,

MARÍA FERNANDA CARRASCAL ROJAS Representante a la Cámara por Bogotá	**DUVALIER SÁNCHEZ ARANGO** Representante a la Cámara por Valle del Cauca - Alianza Verde
HÉCTOR DAVID CHAPARRO Representante a la Cámara por Boyacá Partido Liberal Colombiano	**JUAN CAMILO LONDOÑO BARRERA** Representante a la Cámara por Antioquia Partido Alianza Verde

Norman David Bañol Álvarez Representante a la Cámara Circunscripción especial indígena MAIS	**LEIDER ALEXANDRA VÁSQUEZ OCHOA** Representante a la Cámara por Cundinamarca PACTO HISTÓRICO
DAVID ALEJANDRO TORO RAMÍREZ Representante a la Cámara por Antioquia Pacto Histórico	**AGMETH JOSÉ ESCAF TIJERINO** Representante a la Cámara por el departamento del Atlántico Pacto Histórico
GERMÁN GÓMEZ Representante a la Cámara Partido Comunes	**ALEJANDRO GARCÍA RÍOS** Representante a la Cámara Risaralda Partido Alianza Verde

JUAN CARLOS WILLS OSPINA Representante a la Cámara por Bogotá	**ANDRÉS DAVID CALLE AGUAS** Representante a la Cámara por Córdoba Partido Liberal Colombiano

PROYECTO DE LEY NÚMERO _____ DEL 2023
"Por la cual se dictan disposiciones para el Régimen General de Protección de Datos Personales"

EXPOSICIÓN DE MOTIVOS

La presente exposición de motivos está compuesta por nueve (9) 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. 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 normatividad 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.

Según la Superintendencia Financiera de Colombia, en un periodo de alrededor 10 años (enero de 2013 a junio de 2023), se presentaron un total de 468.795 quejas relacionadas con habeas data, las cuales fueron presentadas ante: las entidades vigiladas, la Superintendencia Financiera de Colombia - SFC, el Defensor del Consumidor Financiero y otras autoridades que dieron traslado de estas a la Superintendencia, el total de quejas se detalla a continuación:

Tabla 1. Total inconformidades 2013 - 2023 (I semestre)

Instancia	# Quejas	Porcentaje
Entidades Vigiladas	366.772	78,2%
Superintendencia Financiera de Colombia	58.302	12,4%
Defensor del Consumidor Financiero	42.214	9,0%
Otra (remisión por competencia)	1.507	0,3%
TOTAL	**468.795**	**100,0%**

Fuente: Superintendencia Financiera de Colombia mediante derecho de petición

En el presente año, se han recibido un total de 15.190 quejas relacionadas con habeas data, de las cuales el 60,1% fueron presentadas ante las Entidades Vigiladas, 23,4% ante la SFC, 12,6% ante el Defensor del Consumidor Financiero y 3,9% a otras entidades.

En relación con lo anterior, la SFC identificó los macromotivos por los cuales los consumidores financieros presentaron las 15.190 quejas relacionadas con habeas data

conforme a la clasificación que asignan las Entidades Vigiladas en lo corrido del año 2023. A continuación, se detallan los 3 de ellos:

1. En primer lugar, se identificaron 12.827 quejas relacionadas con el reporte injustificado a centrales de riesgo, lo que representa un 84,4% del total.
2. En segundo lugar, se identificaron 2.055 quejas relacionadas con el no levantamiento de reporte negativo a centrales de riesgo, lo que representa un 13,53% del total.
3. Finalmente, se identificaron 308 quejas relacionadas con problemas relacionados con centrales de riesgo y/o tratamiento de datos personales, lo que representa un 2,03% del total.

Como parte de las funciones de la SFC como órgano de control, a la fecha, ha emitido órdenes administrativas a dos establecimientos bancarios, una fiduciaria y una corredora de seguros, por la vulneración al principio de temporalidad del tratamiento de datos personales establecido en el literal d) del artículo 4 de la Ley 1266 del 2008.

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)

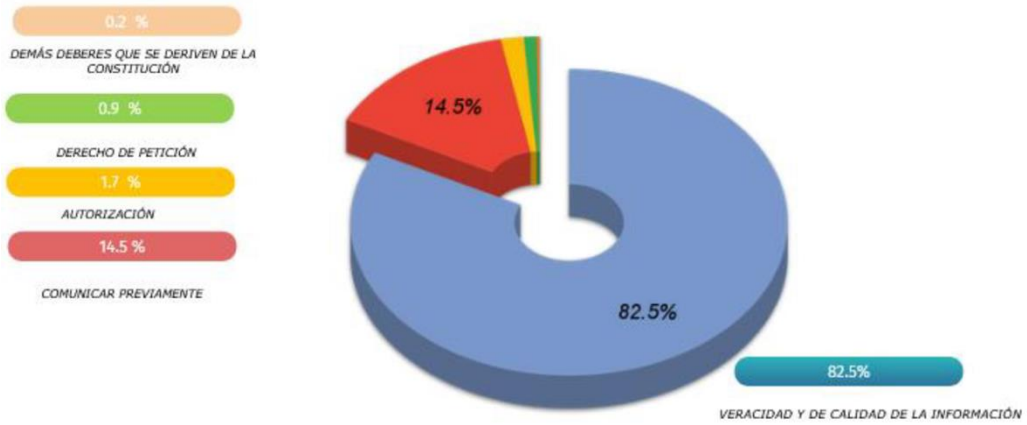
Año	Número de quejas
2013	3.954
2014	5.634
2015	6.134
2016	6.875
2017	7.317
2018	10.057

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:

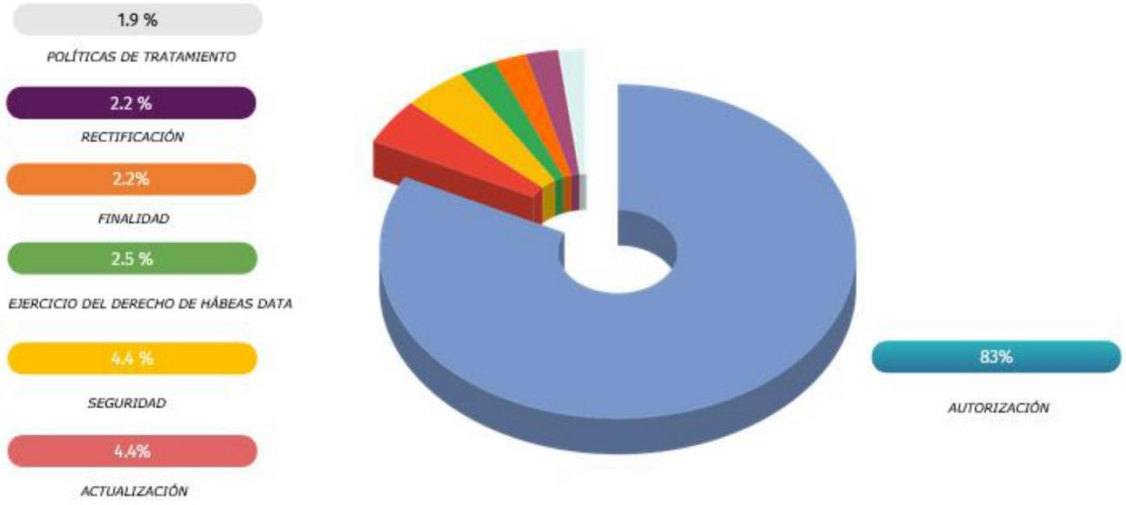
Imagen 1. Número de quejas



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

Los artículos 15 y 20 de la Constitución Política de Colombia introdujeron en la carta de derechos fundamentales a la intimidad personal y familiar, y buen nombre, además de la Libertad de Expresión e Información. Posteriormente, a nivel jurisprudencial, se reconoció en el *Habeas Data* una acción ciudadana que permitía 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 (T-729, 2002). Ya en 1995, la Corte Constitucional reconoce una nueva línea interpretativa de la cual se desprende que el Hábeas Data es un derecho autónomo cuyo núcleo principal es la Autodeterminación Informática (SU-082, 1995)[1]. Esta última, tal y como se señala en la Sentencia SU 139 de 2021, garantiza a los ciudadanos *el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*. Asimismo, el artículo 15 de la Constitución Política

[1] (Sentencia T-729 de 2022): Sobre el derecho innominado a "conocer, actualizar y rectificar las informaciones recogidas en archivos y bancos de datos" de que trata el artículo 15 de la Constitución, y que ha sido asociado al concepto de *habeas data*, la Corte en la sentencia T-414 de 1992 lo definió como derecho a la "libertad informática". Así mismo, en la sentencia SU-082 de 1995, lo definió como derecho a la "autodeterminación informática", y en la sentencia T-552 de 1997 como "autodeterminación informativa".

establece que *en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*.

Por ello, resulta pertinente hablar del derecho fundamental a la protección de datos, que salvaguarda la autodeterminación informática al proveer de acciones a los titulares de los datos para que tenga control sobre la información que circula sobre ellos; así como una estructura institucional representada en una autoridad de control autónoma que asegura la observancia efectiva de la normativa en materia de protección de datos; acciones de compensación al titular en caso de que el tratamiento de sus datos en infracción de la normativa les cause daños y perjuicios; e impone una serie de obligaciones que rigen la circulación de los datos para la consolidación de acuerdos comerciales, que puedan implicar flujo transfronterizo de los mismos.

En el año 2012, se promulgó la Ley 1581 de protección de datos, que respondía a los desafíos tecnológicos de esa época y se alineaba con las exigencias internacionales, tomando en cuenta las garantías establecidas por el Comité de Derechos Humanos en su Observación General 16 sobre el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. Esta ley fue un hito importante en el campo de la protección de datos, ya que abordaba las necesidades y preocupaciones del momento.

La ley 1581 de 2012 en Colombia ha seguido el modelo europeo considerando especialmente las pautas dadas por la Directiva 95/46/CE de la Unión Europea, que dio lugar a múltiples normas nacionales en Europa, entre ellas, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007 que desarrolla dicha ley. Estas normativas españolas han sido fundamentales para la configuración de la normativa colombiana en el ámbito de protección de datos, lo cual demuestra la preocupación del legislador colombiano por adoptar estándares internacionales y fortalecer la protección de datos en el país, buscando que Colombia sea reconocida por su compromiso en este aspecto.

El desafío al que nos enfrentamos en la actualidad es que la tecnología avanza más rápido que la legislación, lo que ha dejado rezagada nuestra normativa frente a los nuevos tiempos. Todas las referencias internacionales que adoptamos en el 2012 y que fueron consideradas en su momento han sido derogadas, como por ejemplo la Directiva 96/45/CE fue reemplazada por el actual Reglamento General de Protección de Datos en 2016, que obligó a España a derogar la ley 15 de 1999 en el año 2018 y promulgar en

su reemplazo la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El Reglamento General de Protección de Datos ha tenido un impacto trascendental a nivel internacional al establecer estándares y requisitos para la protección de datos que deben ser cumplidos por organizaciones de todo el mundo que manejen datos de ciudadanos de la Unión Europea. Este reglamento ha provocado un cambio significativo en el ámbito global de protección de datos, impulsando la adopción de marcos normativos sólidos en muchos países y elevando los estándares de privacidad y seguridad en el procesamiento de datos personales a nivel mundial. Desafortunadamente, Colombia se encuentra en una etapa anterior y es necesario tomar medidas para actualizar y fortalecer nuestra normativa de protección de datos, a fin de cumplir con los estándares internacionales y salvaguardar adecuadamente la privacidad de los ciudadanos.

En suma, la actual normativa de protección de datos perdió su capacidad de abordar de manera adecuada los riesgos que suponen el uso de nuevas tecnologías a la privacidad de los individuos. Por tanto, es necesario llevar a cabo una actualización normativa que se base en las nuevas directrices internacionales en materia de protección de datos, en línea con la Revolución Industrial 4.0.

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.
- Neuroderechos.
- 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. Inteligencia artificial

Hace ya algunos años, Colombia viene tratando de no quedarse atrás. Es por eso que el Departamento Nacional de Planeación, el Ministerio de Tecnologías de la Información y las Tecnologías, y el Departamento Administrativo de la Presidencia de la República, en el CONPES 3975 del 2019, definen la Inteligencia Artificial como: "un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o seres inteligentes. Se entienden como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos". (CONPES 3975. 2019. Página 20).

El Gobierno de Colombia con apoyo del Banco de Desarrollo de América Latina CAF y el Banco Interamericano de Desarrollo BID ha expedido un Marco Ético en octubre de 2021 para la Inteligencia Artificial en Colombia donde realizan una serie de recomendaciones, allí encontramos algunas en seguridad como: «Los sistemas de inteligencia artificial no deben generar afectaciones a la integridad y salud física y mental de los seres humanos con los que interactúan. La seguridad y confidencialidad de los

datos personales y en especial de los datos sensibles son factores fundamentales para evitar afectaciones a la seguridad física y mental de los individuos» (MARCO ETICO PARA LA INTELIGENCIA ARTIFICIAL. 2021. Página 32).

La Superintendencia de Industria y Comercio también ha puesto en conocimiento las Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial, recogidas por la Red Iberoamericana de Protección de Datos (RIPD) de la cual hace parte Colombia. Sin embargo, es importante destacar que ninguna de estas recomendaciones, ni las mencionadas en el marco ético anteriormente comentado, son suficientes por sí solas para garantizar la seguridad jurídica en la privacidad y protección de los datos de los titulares.

Aunque estas recomendaciones brindan orientación y directrices para el tratamiento de datos en el contexto de la inteligencia artificial, es necesario reconocer que la evolución tecnológica y los desafíos asociados con la privacidad y la protección de datos requieren un enfoque más amplio y sólido. La complejidad de las tecnologías de inteligencia artificial, así como la cantidad y sensibilidad de los datos personales involucrados, demandan regulaciones más exhaustivas y específicas, pero sin afectar el buen uso y aprovechamiento de ellas para desarrollos beneficiosos para el país.

Para garantizar la seguridad jurídica en la privacidad y protección de datos, es necesario contar con marcos normativos robustos que establezcan obligaciones claras para los responsables del tratamiento de datos y brinden derechos sólidos a los titulares de los datos. Estas regulaciones deben abordar aspectos como la recopilación y el consentimiento informado de datos, el almacenamiento seguro, la transferencia de datos, la transparencia en los algoritmos o redes neuronales utilizadas y la rendición de cuentas por parte de las entidades involucradas.

Además, es crucial promover una cultura de responsabilidad y ética en el desarrollo y aplicación de la inteligencia artificial. Esto implica fomentar buenas prácticas de privacidad desde el diseño (*privacy by design*) y garantizar la evaluación y mitigación de posibles riesgos para la privacidad a lo largo de todo el ciclo de vida de los sistemas de inteligencia artificial.

4.2.2. Neuroderechos

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 con los neuroderechos. Pero *¿A qué se le aplica los llamados neuroderechos?* 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". (CALDERON, R.A. 2021). Entonces, esa barrera que se rompió con las nuevas tecnologías para obtener acceso a nuestra actividad cerebral debe ser regulada de manera que se protejan nuestros derechos y libertades**.**

La regulación de la privacidad y protección de datos en el uso de la neurotecnología es importante 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 neurotecnologías, garantizando su identidad personal, libre albedrío, privacidad mental, acceso equitativo y protección contra sesgos. También se promueve la concientización, educación y buenas prácticas en el ámbito de las neurotecnologías para salvaguardar los intereses individuales y el bienestar de la sociedad en general.

4.2.3. 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 garantizarle 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 solo sea utilizada de manera legítima y con su consentimiento. Además, se establecen salvaguardias para proteger los intereses de los titulares y se les brinda información oportuna sobre cualquier cambio en el tratamiento de sus datos. En conjunto, estas disposiciones promoverían la protección de la privacidad y los derechos de los titulares en todos los entornos.

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

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

Por ende, el fortalecimiento de la Seguridad como principio y como deber, implica la adopción de medidas técnicas y organizativas que conjugan la aplicación de la tecnología y buenas prácticas como elementos constitutivos de un sistema de seguridad que

garantice la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

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

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

La Seguridad y Privacidad de la información busca que los sujetos obligados implementen *lineamientos de seguridad y privacidad de la información en todos sus proce-sos, 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 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 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 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"[2] en *strictu sensu*, como se conoce a nivel internacional, y la transmisión[3] 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

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

[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

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 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.»*

Si 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)[4]. 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

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

falencias al momento de comprobar la veracidad de los datos, muchos titulares terminan asumiendo obligaciones que no adquirieron, ocasionando perjuicios económicos y daños a su reputación crediticia.

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

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

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

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

Esto no es más que la materialización del *ius punendi*, que debe regirse por los principios de legalidad, tipicidad, debido proceso, proporcionalidad e independencia de la sanción penal. En esta nueva propuesta legislativa no solo es menester incorporar nuevas infracciones con ocasión de las diferentes figuras jurídicas introducidas, sino que

también, se establece un Régimen Sancionatorio más claro que permite tipificar mejor las infracciones que puedan llegar a ser cometidas por los actores involucrados en el tratamiento de datos personales.

Con respecto al principio de legalidad, corresponderá al legislador definir la licitud del Régimen una vez se discuta el contenido definitivo del proyecto de ley que debe ser sometido a trámite legislativo; con respecto a la tipicidad, presenta este proyecto de ley una descripción específica, precisa y exhaustiva de las acciones y omisiones que se consideran infracciones en materia de protección de datos, incluso modulando las mismas por nivel de gravedad; en cuanto al debido proceso, si bien, este proyecto de ley continúa con que la actuación administrativa que inicie la investigación se circunscriba a lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, establece sujetos responsables, condiciones generales para la imposición de sanciones, distinción entre los tipos de sanciones 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 a 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 que 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 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 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 N.º 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 Nº 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 Nº 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 Nº 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 5 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 5 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.*
>
> *. 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 5 de 1992 modificado por la Ley 2003 de 2019, no exime al Congresista de identificar causales adicionales en las que pueda estar incurso.

Atentamente,

 **MARÍA FERNANDA CARRASCAL ROJAS** Representante a la Cámara por Bogotá	 **DUVALIER SÁNCHEZ ARANGO** Representante a la Cámara por Valle del Cauca Alianza Verde
 **HÉCTOR DAVID CHAPARRO** Representante a la Cámara por Boyacá Partido Liberal Colombiano	 **JUAN CAMILO LONDOÑO BARRERA** Representante a la Cámara por Antioquia Partido Alianza Verde
 **LEIDER ALEXANDRA VÁSQUEZ OCHOA** Representante a la Cámara por Cundinamarca PACTO HISTÓRICO	 **DAVID ALEJANDRO TORO RAMÍREZ** Representante a la Cámara por Antioquia Pacto Histórico

 **AGMETH JOSÉ ESCAF TIJERINO** Representante a la Cámara por el departamento del Atlántico Pacto Histórico	 **MARÍA DEL MAR PIZARRO GARCÍA** Representante a la Cámara - Bogotá Coalición Pacto Histórico
 **GERMÁN GÓMEZ** Representante a la Cámara Partido Comunes	 CARLOS FELIPE QUINTERO OVALLE Representante a la Cámara Departamento del Cesar
 **SANTIAGO OSORIO MARIN** Representante a la Cámara Coalición Alianza Verde - Pacto Histórico	 **ALEJANDRO GARCÍA RÍOS** Representante a la Cámara Risaralda Partido Alianza Verde

JUAN CARLOS WILLS OSPINA Representante a la Cámara por Bogotá	**ANDRÉS DAVID CALLE AGUAS** Representante a la Cámara por Córdoba Partido Liberal Colombiano

9. REFERENCIAS

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

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

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

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

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

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

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

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

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

PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Página 6. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

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