Análisis cuantitativo y cualitativo de las Resoluciones de la Superintendencia de Industria y Comercio en las que sanciona a los Responsables y/o Encargados por indebido tratamiento de datos personales desde el 01 de enero de 2022 al 31 de diciembre de 2022".

Estudiantes:

MARÍA CAMILA MURILLO MUÑOZ

JUAN JOSÉ RIASCOS SARRIA

PROYECTO DE GRADO

PONTIFICIA UNIVERSIDAD JAVERIANA – CALI

FACULTAD DE HUMANIDADES Y CIENCIAS SOCIALES

SANTIAGO DE CALI, 2024

Análisis cuantitativo y cualitativo de las Resoluciones de la Superintendencia de Industria y Comercio en las que sanciona a los Responsables y/o Encargados por indebido tratamiento de datos personales desde el 01 de enero de 2022 al 31 de diciembre de 2022".

Estudiantes:

MARÍA CAMILA MURILLO MUÑOZ.

JUAN JOSÉ RIASCOS SARRIA.

PROYECTO DE GRADO

Director:

LUIS FÉLIX BARRIGA PALOMINO.

PONTIFICIA UNIVERSIDAD JAVERIANA – CALI

FACULTAD DE HUMANIDADES Y CIENCIAS SOCIALES

SANTIAGO DE CALI, 2024

TABLA DE CONTENIDO

Pág.
Introducción 1
Planteamiento del problema. 4
Justificación del planteamiento del problema. 6
Estado del arte. 7
Marco de referencia 8
- Marco Teórico: 9
  - ¿Quién es la fuente de información? 9
  - ¿Qué se entiende por vínculo de cualquier otra índole? 9
  - ¿Quién es el operador de la información? 9
  - ¿Quién es el usuario de la información? 10
  - ¿Qué es el principio de finalidad? 10
  - ¿En qué consiste la circulación restringida? 10
  - ¿Qué es la temporalidad de la información? 10
  - ¿Qué es el principio de interpretación integral de derechos constitucionales? 10
  - ¿En qué consiste el principio de seguridad? 10
- Marco Legal: 11
  - Constitución Política de Colombia: 11
  - Ley 1266 de 2008: 11
  - Sentencia C-1011 de 2008: 11
  - Resolución 8862 de 2010: 11
  - Sentencia C-748 de 2011: 12
  - Ley Estatutaria 1581 de 2012: 12
  - Decreto 1377 de 2013: 12
  - Decreto 886 de 2014: 13
  - Decreto 1074 de 2015: 13

Objetivos 14
- Objetivo general 14
- Objetivos específicos 14

Metodología 15
Hipótesis 20

Pregunta de investigación:..... 20
Conclusiones esperadas..... 20
Limitaciones a la investigación. 20
En cuanto a la facultad sancionatoria de la Superintendencia de Industria y Comercio frente al Indebido Manejo de Datos Personales. 21
En cuanto al procedimiento que adelanta la Superintendencia de Industria y Comercio frente al Indebido Manejo de Datos Personales. 24
En cuanto al desarrollo conceptual de los tópicos relacionados con el Régimen de Protección de Datos Personales y la Protección de Datos Personales. 28
Acerca de las nuevas tecnologías de la información y la comunicación para la obtención de datos personales. 28
Acerca del Régimen de Protección de Datos Personales..... 29
Acerca del Tratamiento de Datos Personales. 30
Acerca de la Protección de Datos Personales. 31
Acerca de las etapas del Ciclo de Vida del Dato Personal..... 31
Recolección de Datos Personales: 32
Circulación de Datos Personales: 33
Disposición Final de Datos Personales: 33
Acerca de la transmisión y la transferencia de los datos personales sujetos al Tratamiento. 34
Acerca de la definición de datos personales. 35
Acerca de la definición de Dato Público. 37
Acerca de la definición de Dato Semiprivado. 37
Acerca de la definición de Dato Privado. 37
Acerca de la definición de Dato Sensible. 38
Acerca de los sujetos obligados en virtud del Régimen de Protección de Datos Personales. 38
Acerca de la definición del titular de la información. 39
Acerca de la autorización del titular de la información para el Tratamiento de Datos Personales. 39
Acerca de la definición de Encargado del Tratamiento de Datos Personales. 40
Acerca de la definición de Responsable del Tratamiento de Datos Personales. 41
Acerca de la vulneración a los mandatos dictados por los regímenes de protección de datos..... 41

Acerca de los niveles adecuados de protección para los Datos Personales sujetos al Tratamiento. 42
Acerca del contrato de Protección de Datos Personales. 43
En cuanto al Fundamento Normativo de las Resoluciones Sanción emitidas por la Superintendencia de Industria y Comercio para el año 2022 por Indebido Manejo de Datos Personales. 43
Acerca del Derecho Fundamental de Hábeas Data. 44
Acerca del Derecho de Acceso a la Información. 45
Acerca del Derecho a la Intimidad. 46
Acerca del Derecho a la privacidad. 49
Acerca del Derecho a la Autodeterminación Informativa. 50
Acerca del Derecho de Rectificación. 51
Acerca del Derecho de Cancelación u Olvido. 52
Acerca del Derecho a la Portabilidad de Datos. 54
Acerca del Derecho de oposición. 55
Acerca del ámbito de aplicación de fundamento normativo. 56
Ley Estatutaria 1266 de 2008: 56
Ley Estatutaria 1581 de 2012: 56
Decreto Único Reglamentario 1074 de 2015: 57
En cuanto a la especificidad de los sujetos investigados respecto del domicilio de la sociedad, compañía o persona natural. 57
Acerca de la sensibilidad de los datos personales objeto del Tratamiento. 58
Acerca de la cantidad y tipo de datos procesados. 58
Acerca de la cultura del cumplimiento normativo. 58
Acerca del historial de incidentes. 59
En cuanto a los derechos de los titulares de la información. 60
En cuanto a la especificidad de los sujetos investigados respecto de la actividad empresarial que ejecuta en el territorio colombiano. 68
En cuanto a los principios del Régimen de Protección de Datos Personales que están comprometidos en la vulneración. 69
Acerca del Principio de legalidad en materia de Tratamiento de datos. 69
Acerca del Principio de finalidad. 70
Acerca del Principio de libertad. 70
Acerca del Principio de veracidad o calidad. 71

Acerca del Principio de transparencia. 72
Acerca del Principio de acceso y circulación restringida. 72
Acerca del Principio de seguridad. 73
Acerca del principio de confidencialidad. 74
En cuanto al total del número de Resoluciones Sanción emitidas por la Superintendencia de Industria y Comercio para el año 2022. 77
En cuanto a la formulación de cargos para las Personas Jurídicas y Personas Naturales investigadas por Indebido Manejo de Datos Personales. 78
En cuanto a la calidad del sujeto investigado por la Superintendencia de Industria y Comercio por Indebido Manejo de Datos Personales. 80
En cuanto a los deberes que le corresponden a los Responsables Del Tratamiento de Datos Personales y/o Encargados Del Tratamiento. 86
Acerca del cumplimiento normativo de los Deberes del Responsable y/o Encargado del Tratamiento de Datos Personales consagrados en la Ley 1581 de 2012. 86
Acerca del tipo de infracción o violación cometida por parte del Responsable y/o Encargado del Tratamiento. 98
En cuanto a la especificidad de los sujetos investigados respecto a la responsabilidad frente al proceso administrativo. 101
Acerca de allanarse o aceptar los cargos formulados. 101
Acerca de no aceptar los cargos formulados. 102
Acerca de guardar silencio ante los cargos formulados. 102
En cuanto a las medidas sancionatorias que adopta la Superintendencia de Industria y Comercio para las conductas vulneratorias por Indebido Manejo de Datos Personales. ... 104
En cuanto a la existencia de requerimiento previo por parte de la Superintendencia de Industria y Comercio a los investigados. 110
En cuanto a la cuantía de las Resoluciones. 112
En cuanto a los parámetros para establecer la cuantía. 114
Acerca de la adecuación típica al caso en concreto. 114
Acerca del cálculo para establecer el valor de la sanción. 115
Acerca del principio de proporcionalidad durante el proceso administrativo sancionatorio. 116
Acerca de la dosificación de la sanción. 117
Acerca de los criterios para graduar las sanciones. 118
Conclusión 122
Bibliografía 126

INDICE DE TABLAS

Pág.

Tabla No. 1 Para el Domicilio del Sujeto Investigado. 59
Tabla No. 2 Para el Inicio de la Investigación. 66
Tabla No. 3 Para los Principios comprometidos en el indebido manejo de datos personales. 75
Tabla No. 4 Para el Estado de las Resoluciones Sanción. 78
Tabla No. 5 Para el Número de cargos de las Resoluciones Sanción. 78
Tabla No. 6 Para la Calidad del Sujeto Investigado de las Resoluciones Sanción. 81
Tabla No. 7 Para la calidad del Sujeto Investigado de las Resoluciones Sanción. 85
Tabla No. 8 Para los Deberes del Responsable del Tratamiento de Datos Personales. 94
Tabla No. 9 Para la Responsabilidad del Sujeto Investigado. 103
Tabla No. 10 Para la medida adoptada por la Superintendencia de Industria y Comercio a los sujetos investigados. 108
Tabla No. 11 para la existencia de requerimiento previos a los sujetos investigados por parte de la Superintendencia de Industria y Comercio. 111
Tabla No. 12 para la cuantía de las Resoluciones. 113
Tabla No. 13 Para los criterios para la graduación de las sanciones. 120

INDICE DE GRÁFICOS

Pág.

Gráfico No. 1 Para el Domicilio del Sujeto Investigado..... 60

Gráfico No. 2 Para el Inicio de la Investigación..... 67

Gráfica No. 3 Para los Principios comprometidos en el indebido manejo de datos personales. 76

Gráfico No. 4 Para el Número de Cargos de la Resoluciones Sanción. 79

Gráfico No. 5 Para la Calidad del Sujeto Investigado de las Resoluciones Sanción..... 81

Gráfico No. 6 Para la calidad del Sujeto Investigado de las Resoluciones Sanción. 86

Gráfico No. 7 Para los Deberes del Responsable del Tratamiento de Datos Personales. 95

Gráfico No. 8 Para los Deberes del Responsable del Tratamiento de Datos Personales. 97

Gráfico No. 9 Para la Responsabilidad del Sujeto Investigado..... 103

Gráfico No. 10 Para la medida adoptada por la Superintendencia de Industria y Comercio a los sujetos investigados. 109

Gráfica No. 11 para la existencia de requerimiento previos a los sujetos investigados por parte de la Superintendencia de Industria y Comercio. 112

Gráfica No. 12 para la cuantía de las Resoluciones.....114

Gráfico No. 13 Para los criterios para la graduación de las sanciones. 121

Glosario y Palabras Claves.

Autorización: Es el consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales. (Ley estatutaria 1581, 2012, Literal A, Artículo 4).

Autoridad Responsable de la Protección de Datos: Se refiere a las autoridades supervisoras establecidas en los Estados Miembros, que tienen la facultad de redactar e implementar las leyes, reglamentos y requisitos relacionados con la protección de Datos Personales, sea a nivel nacional, regional o municipal y de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado. (Principios actualizados sobre la privacidad y la protección de datos personales, Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos).

Para el caso en particular, la autoridad competente es la Superintendencia de Industria y Comercio.

Base de datos: Es el conjunto organizado de datos personales que sea objeto de Tratamiento. (Ley estatutaria 1581, 2012, Literal B, Artículo 4).

Consulta: Se refiere a la solicitud o petición del Titular del Dato o las personas autorizadas por éste o por la ley, para conocer la información que se tiene sobre él en Bases de Datos o archivos de información (Gobernación del Valle del Cauca, s. f.).

Confidencialidad: Se refiere al principio rector respecto al cual, 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. (Principios actualizados sobre la privacidad y la protección de datos personales, Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos).

Dato personal: Se refiere a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley estatutaria 1581, 2012, Literal C, Artículo 4).

Datos personales sensibles: Se refiere a una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal. En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o

arbitraria. (Principios actualizados sobre la privacidad y la protección de datos personales, Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos).

Derecho a la intimidad: Es el derecho fundamental que permite a las personas manejar su propia existencia como a bien lo tengan con el mínimo de injerencias exteriores. (Corte Constitucional, sentencia C-640/10, 2010).

Encargado del tratamiento: Hace referencia a la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley estatutaria 1581, 2012, Literal D, Artículo 4).

Habeas Data: 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. (Corte Constitucional, Sentencia SU-139, 2021).

Objetividad: La objetividad es el modo característico de la interpretación y aplicación de la Ley por parte de la Administración, que opera imponiendo al funcionario el deber de realizar dicha labor hermenéutica y aplicativa adecuándose a la voluntad normativa y prescindiendo de cualquier tipo de fin o interés subjetivo (García, 2011).

Parámetro: Dato o factor que se toma como necesario para analizar o valorar una situación (Real Academia Española, 2023).

Protección: La protección de la privacidad implica también permitir que las personas controlen su experiencia "en línea". Además de tomar medidas de seguridad eficaces. (Principios actualizados sobre la privacidad y la protección de datos personales, Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos).

Principio de imparcialidad: El principio de imparcialidad, como parte del debido proceso disciplinario, debe ser entendido como la garantía con la cual se asegura que el funcionario que adelante la investigación, o que conozca de los recursos interpuestos contra las actuaciones adelantadas, obre efectivamente como tercero neutral, tanto ante el sujeto disciplinado como ante la causa misma y el objeto o situación fáctica que se analiza. Un tercero que además deba desarrollar sus competencias, sin prejuicios ni posturas previas que afecten su ánimo y la sana crítica para actuar y en su momento decidir. (Corte Constitucional, Sentencia C -029/09, 2009).

Principio de Privacidad: Es el ámbito personalísimo de cada individuo o familia, es decir, a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídas a la injerencia o al conocimiento de extraños. (Corte Constitucional, Sentencia C-094, 2020)

El concepto de privacidad o de lo privado corresponde a los asuntos que en principio tocan exclusivamente con los intereses propios y específicos de la persona humana, sin que afecten o se refieran a los demás miembros de la colectividad. (Corte Constitucional, Sentencia T-784, 2004 y Sentencia C-602,2016).

Responsable del tratamiento: Hace referencia a la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley estatutaria 1581, 2012, Literal E, Artículo 4).

Sanción: Pena que una ley o un reglamento establece para sus infractores (Real Academia Española, 2023).

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento. (Ley estatutaria 1581, 2012, Literal G, Artículo 4).

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley estatutaria 1581, 2012, Literal G, Artículo 4).

Transferencia: 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 (Gobernación del Valle del Cauca, s. f.).

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 (Gobernación del Valle del Cauca, s. f.).

Resumen

El presente proyecto de investigación se fundamenta a través del análisis investigativo que pretende elaborar un informe detallado sobre las Resoluciones expedidas por la Superintendencia de Industria y Comercio, en materia de Ley de Protección de Datos Personales o Habeas Data consagrada en la Ley 1581 de 2012 para Colombia en el periodo de tiempo comprendido entre el 01 de enero de 2022 al 31 de diciembre de 2022. La perspectiva adoptada en la investigación es enriquecida por la reflexión del autor Rafael Velásquez Bautista, quien afirma que *"En una sociedad moderna, la protección de datos no se debe plantear en contra de nadie, sino más bien es una garantía más para que todos podamos ejercer nuestros derechos y libertades, cumplamos los deberes y nos traten como ciudadanos, nunca reducidos a la condición de súbditos."*

El enfoque de investigación especialmente se centra frente a los criterios y parámetros sancionatorios. Para esto, se estudian los elementos conceptuales en torno a los titulares del derecho, agentes de protección, tratamiento de datos, así como los tipos de datos protegidos. En este mismo sentido, se analizará la regulación atinente en nuestro sistema. Este enfoque conceptual orientará nuestra investigación hacia la comprensión integral de los principios y fundamentos que respaldan el Tratamiento adecuado de Datos Personales en el ámbito del ordenamiento jurídico colombiano. Para esto, se estudian los aspectos relevantes que compone la parte esencial del Régimen de Protección de Datos Personales, como la identificación de los titulares del derecho, los agentes encargados de la protección de datos, los criterios y parámetros sancionatorios empleados y la regulación de datos personales protegidos por la legislación colombiana. Asimismo, se llevará a cabo un análisis detallado de las disposiciones normativas relevantes en nuestro sistema legal.

Al incorporar esta metodología de investigación buscamos no solo entender el marco legal colombiano frente al Tratamiento de Datos Personales, sino también reconocer la Protección de Datos como una garantía esencial para el ejercicio pleno de los derechos y libertades individuales, fomentando así buenas prácticas en la regulación y ejercicio.

Abstract

The present research project is based on investigative analysis aimed at preparing a detailed report on the Resolutions issued by the Superintendence of Industry and Commerce regarding the Law on the Protection of Personal Data or Habeas Data established in Law 1581 of 2012 for Colombia in the period from January 01, 2022, to December 31, 2022. The research perspective is enriched by the reflections of the author Rafael Velásquez Bautista, who asserts that *"In a modern society, data protection should not be posed against anyone but rather is an additional guarantee for all of us to exercise our rights and freedoms, fulfill our duties, and be treated as citizens, never reduced to the status of subjects."*

The research focus specifically centers on sanctioning criteria and parameters. To achieve this, conceptual elements related to the rights holders, protection agents, data processing, as well as types of protected data are studied. In the same vein, the relevant regulation in our system will be analyzed. This conceptual approach will guide our research towards a comprehensive understanding of the principles and foundations that support the proper Treatment of Personal Data within the framework of Colombian legal regulations. To achieve this, the relevant aspects that make up the essential part of the Personal Data Protection Regime are studied, such as the identification of rights holders, data protection agents, criteria and sanctioning parameters used, and the regulation of personal data protected by Colombian legislation. Likewise, a detailed analysis of the relevant normative provisions in our legal system will be carried out.

By incorporating this research methodology, we aim not only to understand the Colombian legal framework regarding the Treatment of Personal Data but also to recognize Data Protection as an essential guarantee for the full exercise of individual rights and freedoms, thereby promoting good practices in regulation and implementation.

Introducción

Actualmente nos encontramos en una sociedad que demanda grandes avances en diferentes áreas de la dinamización del mercado, entre ellas se destaca el sector de las tecnologías de la información y la comunicación, por esta razón, cada nación está haciendo exorbitantes e imperiosos esfuerzos para competir con otros Estados y regular el tema en su ordenamiento jurídico. Ser parte de la corriente de la globalización genera la creación de mercados estratégicos que antes no existían, por tanto, los avances tecnológicos e informáticos están relacionados intrínsecamente con la Protección de Datos Personales en el sentido de que el uso masivo de tecnologías de la información y la comunicación ha generado una mayor recopilación, almacenamiento procesamiento y transmisión de datos personales de los usuarios alrededor del mundo. La legislación en torno a la protección de datos personales, para el caso del ordenamiento jurídico Colombiano, específicamente, la Ley Estatutaria 1581 de 2012, se vuelve esencial para garantizar que estos avances tecnológicos no comprometan la privacidad y seguridad de la información personal de los individuos.

Los agentes del mercado, incluyendo a los consumidores y las empresas, como motor económico que impulsa la economía del país, están llamados a implementar en la cotidianidad del día a día, tecnologías informáticas en cuanto el crecimiento de la sociedad lo amerita, lo cual, se genera gran flujo de datos que contienen información personal y en ocasiones, sensible y semiprivada para los titulares. En este punto crucial, la protección de datos se convierte en una preocupación clave para asegurar que estos se manejen de manera ética, segura y respetando los derechos de privacidad de cada uno de los individuos.

La Ley 1581 de 2012 regula sobre el tema y estipula lo relacionado al manejo del tratamiento de los datos personales que deben tener las empresas de carácter privado y público, respecto a los datos que son obtenidos de los clientes o terceras partes, con los que se realiza cualquier tipo de actividad o transacción que requiera el manejo de este tipo de información. En este orden de ideas, tanto las normas de carácter nacional como internacional, deben estar en constante proceso de evolución, adecuándose a las condiciones cambiantes del mercado, debido al entorno tecnológico en el que nos encontramos, por ello es realmente importante la comprensión y aplicación de conceptos como autorización, base de datos, encargado del tratamiento, responsabilidad, entre otros, son fundamentales para garantizar la integridad y la privacidad de los datos personales en la era de la revolución tecnológica, pues de esto depende que se realice un adecuado manejo de la información de cada individuo, lo cual es una premisa aplicable en nuestros días, que se explica basándose en un estudio de la Facultad de Derecho de la Universidad de los Andes en la cual Nelson Remolina Angarita explica, *"Cada vez más, las decisiones sociales, políticas o económicas giran en torno a la información. Por eso, si la información sobre una persona está desactualizada para adquirir un crédito, será considerada deudora morosa y no le van a prestar el dinero que necesita. Si una historia clínica no está al día, se podrían tomar decisiones equivocadas que afectarían la salud o la vida del paciente. Así que la responsabilidad es muy grande"* (s.f.).

Siendo consecuente con lo anterior, ante la inminente presencia de las tecnologías, se consagra, el Derecho de Hábeas Data, que funge como un aspecto crucial en la Protección de

Datos Personales en Colombia, puesto que, a lo largo del tiempo, ha habido una creciente preocupación por garantizar que las empresas de carácter público y privado cumplan con las disposiciones normativas consagradas en la Ley 1581 de 2012 relacionadas con este derechos y sus conexos, en cuanto, el objetivo de este nuevo mecanismo de protección de derechos fundamentales es salvaguardar a los ciudadanos de extralimitaciones, excesos o errores que se puedan cometer en el almacenamiento y procesamiento de información, sin importar que se hagan mediante medios automatizados o manuales, toda vez que es preciso entender que los límites que tienen las empresas y entidades sobre los datos, recae sobre el titular, quien debe dar su autorización expresa para su recolección y tendrán que contar con un consentimiento para hacer uso la información personal de un ciudadano. Esto implica que la empresa debe manifestar de manera clara para qué se van a utilizar esos datos, cuál es la finalidad, cómo los van a usar, quienes los utilizarán y cuáles serán los medios de tratamiento (Argote, 2021).

Una vez resaltada la importancia del derecho fundamental "Hábeas Data", la Superintendencia de Industria y Comercio desempeña un papel crucial como autoridad competente en la función de control y supervisión. Su responsabilidad principal radica en garantizar que, en el ámbito de la recolección, uso, circulación y tratamiento de datos personales, se respeten los principios, derechos, garantías y procedimientos establecidos tanto en la Constitución como en la Ley. Esto se refiere especialmente a los derechos y principios que rigen el adecuado tratamiento de los datos personales de los titulares de la información. La Superintendencia de Industria y Comercio tiene la función de exigir la salvaguarda del derecho fundamental "´´Hábeas Data", tal como se consagra en el Artículo 15 de la Constitución Política de Colombia. Este artículo confiere a las personas el derecho fundamental de *"Conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas*". En este sentido, la Superintendencia juega un papel crucial al velar por el cumplimiento de este derecho, asegurando que las entidades respeten la integridad y la privacidad de los datos personales, y facilitando el ejercicio pleno de los derechos de los titulares sobre la información que les concierne, teniendo en cuenta las disposiciones de la Superintendencia de Industria y Comercio en donde se expresa que el titular de la información es cualquier persona natural o jurídica que tiene sus datos en una base ya sea de carácter público o privado. La fuente de la información es el vínculo que une al ciudadano con los datos personales que hay en las bases y que serán manejados con la autorización expresa del titular. El ciudadano tendrá el derecho de consultar la información, actualizarla si existe algún error y solicitar su eliminación de la base de datos si su tenencia no está sustentada en una base legal (2021).

En virtud de todo lo anterior, se pretende con el presente documento, realizar un análisis exhaustivo y detallado que tiene por objetivo identificar los criterios y parámetros específicos empleados por la Superintendencia de Industria y Comercio para aplicar sanciones a aquellos responsables que han incurrido en un manejo inadecuado de la Protección de Datos Personales. Esta investigación de proyecto de grado, se llevará a cabo mediante el análisis cuantitativo de las Resoluciones emitidas por la entidad en el período comprendido entre el 1 de enero y el 31 de diciembre de 2022, donde se busca examinar de manera detallada las decisiones tomadas por la entidad durante el mencionado período. De igual forma, este análisis no solo se centrará en la cantidad de sanciones impuestas, sino que también se adentrará en una evaluación cualitativa de las Resoluciones, que pretende comprender la

naturaleza de las infracciones, los factores que contribuyen a la imposición de sanciones y cualquier patrón recurrente que pueda surgir en el tratamiento indebido de datos personales. En última instancia, se procura contribuir al entendimiento de los mecanismos y criterios que la Superintendencia de Industria y Comercio emplea para preservar la integridad de los datos personales y fomentar prácticas adecuadas en su manejo, brindando así una perspectiva completa y detallada sobre la aplicación de sanciones en el ámbito del tratamiento de datos personales durante el período especificado.

Planteamiento del problema.

Colombia es un Estado Social de Derecho y debe garantizar a sus ciudadanos la protección de los derechos fundamentales, consagrados en la Constitución Política de Colombia de 1991, por esta razón, es responsabilidad del Estado propender por la salvaguarda del derecho a la intimidad de las personas y respetarla, pues de allí surge el Derecho de Hábeas Data, el cual tiene toda persona para conocer, actualizar y rectificar la información de carácter personal y confidencial que se haya recopilado respecto de ella en Bancos de Datos y archivos documentales de entidades de naturaleza pública o privada según la Ley 1581 de 2012. Este derecho ha sido definido a instancias de la Corte Constitucional en Sentencia C-748 de 2011, como *"El derecho que le otorga al titular de la información personal de exigir y ordenar a las entidades que administran los datos personales, prerrogativas como el acceso, inclusión, exclusión, corrección, modificación, aclaración de los datos personales, o peticiones como limitar su divulgación, publicación o cesión de esta, según los parámetros de confidencialidad."*. Sin embargo, a pesar de los múltiples esfuerzos que se realizan por parte de la autoridad de control y vigilancia, las sanciones por violaciones a la privacidad a menudo resultan ser insuficientes para reducir el indebido manejo de la Protección a los Datos Personales de los titulares, pues la falta de aplicación efectiva permite que muchas entidades públicas y privadas continúen recopilando, almacenando, compartiendo y exponiendo datos personales de manera irresponsable.

La falta de claridad en los límites del Tratamiento de Datos Personales y el uso de datos personales de manera indiscriminada también hacen parte del problema. Muchas entidades públicas y privadas en Colombia recopilan información sin el consentimiento previo, expreso e informado de los individuos. La ausencia de una cultura sólida de privacidad y educación ciudadana sobre la importancia de proteger los datos personales permite que estas prácticas persistan.

Si bien el Estado Colombiano a través de la Superintendencia de Industria y Comercio impone sanciones al respecto; la falta de protocolos adecuados y medidas de seguridad aumentan el mal uso de datos personales. La recopilación masiva de la información sin la aplicación de los mecanismos adecuados pone en peligro la privacidad de los ciudadanos y produce desconfianza a los mismos.

Algunas entidades a menudo recopilan datos personales de clientes sin el debido consentimiento para posteriormente vender esta información a terceros, por esta razón la falta de transparencia sobre cómo se utilizan y comparten estos datos ocasiona una situación de explotación y abuso en contra de los titulares de la información.

La falta de conciencia ciudadana sobre la importancia de la protección de datos personales agrava la situación. Muchas personas en Colombia desconocen sus derechos en cuanto al hábeas data y no comprenden completamente las implicaciones de la recopilación y el mal manejo de sus datos personales. La educación pública sobre privacidad y seguridad cibernética es esencial para empoderar a los ciudadanos y fomentar una cultura de responsabilidad y respeto por la privacidad.

La transparencia y la rendición de cuentas deben convertirse en pilares fundamentales tanto en el sector público como en el privado. Las empresas deben ser más claras sobre cómo recopilan, almacenan y utilizan los datos personales, y los ciudadanos deben tener el derecho de acceder y controlar la información que se recopila sobre ellos. La implementación de tecnologías de seguridad avanzadas y promoción de buenas prácticas de seguridad son esenciales para proteger los datos contra amenazas internas y externas.

Teniendo en cuenta el objeto de protección de este bien jurídico, es importante analizar cómo resuelve el ordenamiento jurídico colombiano, a través del órgano de control y vigilancia, la tensión y preocupación existente entre el derecho a la autodeterminación de la información y el acceso y el manejo de ésta por administradores de bases de datos, portales de Internet y/o motores de búsqueda.

Justificación del planteamiento del problema.

Este estudio tiene gran importancia en la actualidad, pues desde hace varios años se está observando que gracias a la globalización se abre paso la apertura a los mercados y a las nuevas formas de comunicación, generando así un gran desarrollo tecnológico, por esta razón, el manejo adecuado del Derecho Fundamental de Hábeas Data es un aspecto crucial. En el contexto colombiano, se puede afirmar que estamos frente a una serie de desafíos significativos que afectan la privacidad de los ciudadanos y ponen en riesgo la seguridad de la información.

La protección de datos personales es un derecho fundamental que debe ser salvaguardado para preservar la dignidad y autonomía de los individuos. Colombia, al igual que muchos otros países, ha adoptado medidas legislativas como la Ley Estatutaria 1581 de 2012 para regular la Protección de Datos Personales. Sin embargo, la implementación efectiva de la normativa y su supervisión son críticas para garantizar que se respeten y protejan los derechos de privacidad, confidencialidad e intimidad de los ciudadanos. Resolver el manejo de Hábeas Data implica fortalecer los mecanismos de aplicación y sanción para aquellos que violan estas normativas.

La confianza en las instituciones gubernamentales y en las empresas es esencial para que una sociedad funcione adecuadamente, por el contrario, un manejo descuidado de habeas data expone a los ciudadanos a riesgos innecesarios. Si las personas sienten que sus datos no están siendo manejados debidamente, la confianza en las instituciones desaparece, lo que puede generar consecuencias negativas a la hora de adoptar servicios digitales. Resolver este problema es crucial para preservar y fortalecer la confianza de cada uno de los titulares de la información. La seguridad de los datos es esencial para proteger tanto la privacidad de los individuos como la estabilidad de las instituciones.

De allí la conveniencia de conocer por medio del análisis mixto de las Resoluciones de la Superintendencia de Industria y Comercio en las que sanciona a los responsables por indebido tratamiento de datos personales desde el 01 de enero de 2022 al 31 de diciembre de 2022, los parámetros usados frecuentemente para determinar la imparcialidad u objetividad de la valoración sancionatoria, y la forma en cómo sanciona la entidad y evidenciar cómo funciona el tratamiento de datos personales en el territorio Colombiano.

Estado del arte.

En la actual era digital, la recopilación y manejo de datos personales han adquirido un papel fundamental en diversos aspectos de la sociedad. El crecimiento vertiginoso de la tecnología de la información y la comunicación ha desencadenado una expansión masiva en la cantidad de información personal que se genera, comparte y procesa en todo el mundo. En este contexto, la privacidad y la protección de datos personales se han convertido en preocupaciones centrales, exigiendo una regulación precisa para salvaguardar los derechos fundamentales de los individuos.

En el marco colombiano, la Ley Estatutaria 1581 de 2012 establece las bases legales para garantizar un tratamiento adecuado de los datos personales, asegurando que este avance tecnológico no comprometa la privacidad y seguridad de la información personal de los ciudadanos. En este contexto normativo, la Superintendencia de Industria y Comercio emerge como la autoridad competente encargada de supervisar y sancionar el indebido tratamiento de datos personales, desempeñando un papel crucial en la preservación de los derechos fundamentales.

Esta investigación se propone realizar un análisis detallado y exhaustivo a través de medios cuantitativos y cualitativos de las Resoluciones emitidas por la Superintendencia de Industria y Comercio durante el periodo comprendido entre el 1 de enero y el 31 de diciembre de 2022. El objetivo principal es identificar los criterios y parámetros específicos utilizados por esta entidad para imponer sanciones a los responsables por el indebido tratamiento de datos personales.

En este contexto, el Estado del Arte se erige como un componente esencial de esta investigación, proporcionando un marco teórico y conceptual que contextualiza la relevancia y la necesidad de la presente indagación. A través de la revisión de antecedentes, normativas legales, jurisprudencia y conceptos clave, se pretende sentar las bases para comprender a fondo la protección de datos personales en el contexto colombiano y la labor de la Superintendencia de Industria y Comercio como garante de estos derechos.

El Estado del Arte abordará temas fundamentales como la evolución de la legislación colombiana en materia de protección de datos, la definición y alcance del derecho de Hábeas Data, la actuación de la Superintendencia de Industria y Comercio, así como los conceptos teóricos esenciales que enmarcan esta investigación. Este análisis proporcionará una comprensión profunda de los fundamentos teóricos y prácticos necesarios para abordar la pregunta central de este estudio: ¿Cuáles son los parámetros usados por la Superintendencia de Industria y Comercio para imponer sanciones por el indebido tratamiento de datos personales?

Marco de referencia

- **Marco Contextual:**

El avance tecnológico y la creciente digitalización de la sociedad han generado un aumento significativo en la recopilación y manejo de datos personales. En este contexto, la protección de la privacidad y la seguridad de la información se han convertido en preocupaciones fundamentales. Por esta razón, encontramos noticias como: **"Cada día en Colombia se presentan cerca de 79 casos de violaciones de protección de datos personales"**, pues actualmente se ha vuelto normal "recibir llamadas telefónicas de empresas o entidades con las cuales no se tiene vínculo, percatarse de reportes erróneos de obligaciones que no están en mora, o atender llamadas con objetivo de estafa, son algunas de las principales denuncias presentadas por los ciudadanos ante las autoridades y que hacen parte de la lista de casos en donde se atenta contra la protección de datos personales." (Universidad de los andes, s.f.)

De igual manera, Ana Brian Nougreres relatoría de la Organización de Naciones Unidas (ONU) afirma que: "se necesita educación -en todos los niveles de enseñanza, formal e informal- y concientización en todos los lugares, explicándoles a las personas de qué manera pueden utilizar sus datos y cómo pueden verse discriminadas como consecuencia de una mala utilización de esos datos". (Universidad de los andes, s.f.)

Es importante que además de conocer los derechos frente a la protección de datos, las personas como recomendación de seguridad lean y revisen los términos de tratamiento de datos, también es recomendable que no se realice registro de datos personales en sitios no seguros o desconocidos. En este punto entonces se debe destacar la responsabilidad de las empresas que captan la información, para garantizar que se cumpla la ley sobre tratamiento de datos personales, sobre todo si se tienen en cuenta las consecuencias de un uso inadecuado de la información para las personas. (Universidad de los andes, s.f.)

Se dice que: "Cada vez más, las decisiones sociales, políticas o económicas giran en torno a la información". Por ello, es importante que se realice un manejo adecuado sobre los datos personales de cada una de las personas pues esto puede generar consecuencias realmente negativas cuando se trata de datos personales sensibles que no pueden ser divulgados.

Colombia tiene un gran reto, el cual es fortalecer la protección de los datos de los ciudadanos, para que "los responsables o encargados del tratamiento de datos personales en el país, sean entidades públicas o privadas, hagan bien su tarea, sean diligentes, sean profesionales e implementen mecanismos idóneos, no solo porque la ley se los exige, sino porque eso genera confianza. Las entidades y organismos gubernamentales deben entender que la efectividad de un derecho en la práctica no depende de su mera regulación, sino de que los responsables y encargados cumplan sus deberes legales. Se debe pasar de una protección formal, a una protección real y efectiva que es lo que demandan o solicitan los ciudadanos", destacó Remolina. (Universidad de los andes, s.f.)

- **Marco Teórico:**

La privacidad y la protección de datos personales son elementos cruciales en la era digital. La Ley Estatutaria 1581 de 2012 establece los fundamentos legales para garantizar el respeto de estos derechos en Colombia. Conceptos clave, como autorización, base de datos, tratamiento, entre otros, son definidos en la normativa para establecer un marco claro y preciso.

El derecho de Hábeas Data, reconocido en la Constitución y desarrollado por la Corte Constitucional, otorga a los individuos el control sobre su información personal. La Superintendencia de Industria y Comercio, como autoridad competente, desempeña un papel crucial en la aplicación y supervisión de estas normativas.

Por ello la Superintendencia de Industria y Comercio (SIC), como encargada de velar por el debido tratamiento de datos personales, establece las siguientes definiciones:

¿Quién es la fuente de información?

La fuente de información es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Ejemplo: El proveedor de servicios de comunicaciones (Superintendencia de Industria y Comercio, 2021).

Si la fuente entrega la información directamente a los usuarios, y no a través de un operador, tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos (Superintendencia de Industria y Comercio, 2021).

¿Qué se entiende por vínculo de cualquier otra índole?

El vínculo de cualquier otra índole debe entenderse como aquel que genere una o más obligaciones entre la fuente y el titular que legitime al primero a reportar información tanto negativa como positiva del último por lo que es claro que, el contar solamente con la autorización de reporte no genera obligación alguna entre la supuesta fuente y el reclamante; será requisito indispensable la existencia de una obligación entre estos para que sea posible realizar un reporte (Superintendencia de Industria y Comercio, 2021).

¿Quién es el operador de la información?

Se denomina operador de información a la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la ley. Ejemplo: Central de Información Financiera CIFIN y Data crédito (Superintendencia de Industria y Comercio, 2021).

¿Quién es el usuario de la información?

El usuario es la persona natural o jurídica que puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. Ejemplo: Las entidades bancarias que solicitan la información con el fin de analizar el riesgo crediticio, o los proveedores de servicios de comunicaciones quienes pueden actuar como fuente de información, y asimismo como usuarios de la misma (Superintendencia de Industria y Comercio, 2021).

¿Qué es el principio de finalidad?

El principio de finalidad obliga a que las actividades de recolección de datos personales obedezcan a una finalidad legítima de acuerdo con la Constitución y la ley. Con fundamento en este principio la finalidad debe ser comunicada al titular de la información previa o concomitante con el otorgamiento del titular de la autorización, cuando ella sea necesaria o, en general, siempre que el titular solicite información al respecto (Superintendencia de Industria y Comercio, 2021).

¿En qué consiste la circulación restringida?

El principio de circulación restringida consiste en que a menos que la información sea pública, los datos personales no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que dicho acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o a los usuarios autorizados para ello (Superintendencia de Industria y Comercio, 2021).

¿Qué es la temporalidad de la información?

El principio de temporalidad de la información se refiere a la necesidad de que el dato del titular no podrá ser suministrado a los usuarios cuando deje de servir para la finalidad del banco de datos (Superintendencia de Industria y Comercio, 2021).

¿Qué es el principio de interpretación integral de derechos constitucionales?

La interpretación integral de derechos constitucionales consiste en que la normas que rigen los datos personales se interpretarán en el sentido que se amparen otros derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Asimismo, se refiere a que los derechos de los titulares se interpretarán en armonía con el derecho a la información y demás derechos constitucionales aplicables (Superintendencia de Industria y Comercio, 2021).

¿En qué consiste el principio de seguridad?

El principio de seguridad impone que en la información contenida en los bancos de datos, así como aquella que resulte de las consultas que realicen los usuarios, se incorporen las medidas

técnicas necesarias para garantizar la seguridad de los registros, con el fin de evitar su adulteración, pérdida, consulta o uso no autorizado (Superintendencia de Industria y Comercio, 2021).

- **Marco Legal:**

El Habeas Data surge a partir de la Constitución Política de 1991, pues aquí se marca una transición de un régimen autoritario a uno democrático con enfoque hacia los derechos fundamentales. Esta constitución inició principios rectores que sentaron las bases de protección de la privacidad y los datos personales.

- **Constitución Política de Colombia:**

El Artículo 15 de la Constitución Política de 1991 consagra el derecho a la intimidad como un derecho fundamental e inalienable. Este artículo establece que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el estado debe respetarlos y hacerlos respetar". Es esta disposición la que sienta las bases para el desarrollo posterior del hábeas data en el país. Aunque la Constitución Política de 1991 sentó las bases, fue necesario un marco normativo más específico para abordar cuestiones relacionadas con la protección de datos personales y es allí cuando aparece la Ley 1266 de 2008.

- **Ley 1266 de 2008:**

En este contexto, la Ley 1266 de 2008 se erige como un hito clave. Esta ley, conocida como la Ley de Habeas Data, desarrolló el régimen de protección integral de datos personales y reguló aspectos fundamentales relacionados con su recolección, almacenamiento, circulación y tratamiento. Esta otorga a los ciudadanos el derecho de conocer, actualizar y rectificar la información que se haya recogido sobre ellos en bases de datos, así como el derecho a solicitar pruebas de la autorización otorgada para su recolección. Además, introdujo mecanismos para la consulta de información crediticia y establecieron la obligación de obtener el consentimiento previo del titular de los datos para su tratamiento.

- **Sentencia C-1011 de 2008:**

Esta sentencia es de gran importancia porque resalta ciertos principios de administración de datos personales que fueron identificados gracias a la jurisprudencia en materia constitucional, los cuales son todos aquellos sujetos que se encuentran involucrados en los procesos de tratamiento, recolección y circulación de datos, independientemente de la posición que ocupen en el tratamiento de datos personales.

- **Resolución 8862 de 2010:**

Esta resolución expedida por la SIC, inició las pautas para el registro de las bases de datos ante esta entidad. Este registro se convirtió en un requisito esencial para las empresas que

manejan información personal, asegurando así la transparencia y el cumplimiento de las normativas relacionadas con la protección de datos.

El papel de la Superintendencia de Industria y Comercio ha sido fundamental en la implementación y supervisión del habeas data en Colombia. La SIC, como entidad encargada de velar por la protección de la competencia y los derechos del consumidor, asumió un rol protagónico en la regulación y control de la gestión de datos personales.

- **Sentencia C-748 de 2011:**

Este fallo es realmente importante en el contexto colombiano, dado que para proteger el derecho fundamental de Habeas data la corte se pronunció sobre los deberes de los responsables y de los encargados del tratamiento, deberes que, en términos generales, buscan garantizar el pleno ejercicio del derecho al habeas data por parte de los titulares, así como los principios de la administración de datos personales. Estos deberes en cabeza del responsable y del encargado del tratamiento, permiten garantizar, prima facie, el ámbito de protección del derecho de hábeas data.

- **Ley Estatutaria 1581 de 2012:**

En un esfuerzo por fortalecer la protección de datos personales, Colombia promulgó la esta ley, que rige el manejo de la información personal, estableciendo principios fundamentales para el tratamiento de datos como el principio de finalidad, necesidad y consentimiento.

Uno de los aspectos más relevantes de la Ley 1581 de 2012 es la creación del Registro Nacional de Bases de Datos (RNBD), administrado por la SIC. Este registro centraliza la información sobre las bases de datos existentes en el país y facilita la supervisión y control por parte de las autoridades. Además, la ley establece las obligaciones de los responsables y encargados del tratamiento de datos, así como los derechos de los titulares, consolidando un marco legal integral en materia de hábeas data.

- **Decreto 1377 de 2013:**

Este decreto resalta de la protección de datos personales los derechos de los ciudadanos y establece unos lineamientos para el tratamiento de datos, los deberes de los responsables y encargados de los datos personales esta norma busca estar conforme los lineamientos internacionales, por esta razón, tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización de los titulares de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros.

- **Decreto 886 de 2014:**

Este decreto reglamentó la Ley 1266 de 2008 y desarrolló las normas para el manejo de bases de datos en el país. Este decreto detalla aspectos técnicos y procesales, brindando a las entidades responsables de la gestión de datos las pautas para garantizar la seguridad y privacidad de la información personal.

- **Decreto 1074 de 2015:**

En el Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, Industria y Turismo, en su capítulo 25, mediante el cual se reglamenta la Ley 1581 de 2012, establece los objetivos, aspectos relacionados con la autorización del titular de la información, definiciones, recolección de los datos personales, autorización para el tratamiento de datos sensibles, avisos de privacidad, medidas de seguridad, políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, las transferencias de datos personales y la responsabilidad frente al tratamiento de datos personales.

Objetivos

Objetivo general

Analizar de manera cuantitativa y cualitativa las Resoluciones de la Superintendencia de Industria y Comercio en las que sanciona a los responsables por indebido Tratamiento de Datos Personales desde el 01 de enero de 2022 al 31 de diciembre de 2022 para determinar los parámetros en la forma en cómo sanciona la entidad encargada del control y vigilancia de los Responsables y Encargados del Tratamiento.

Objetivos específicos

1. Presentar al lector un análisis detallado de los aspectos fundamentales del Régimen de Protección de Datos Personales de conformidad con el contenido teórico de la Ley 1581 de 2012 y de la información contenida en las Resoluciones emitidas por la Superintendencia de Industria y Comercio relacionadas con sanciones por el indebido tratamiento de datos personales en el período de tiempo del 01 de enero de 2022 al 31 de diciembre de 2022, que a su vez, son las directrices que delimitan la gestión adecuada de datos personales en Colombia.

2. Presentar al lector un análisis estructurado de las Resoluciones por indebido tratamiento de datos personales en el período de tiempo del 01 de enero de 2022 al 31 de diciembre de 2022, para evidenciar los parámetros que utiliza la Superintendencia de Industria y Comercio para establecer la cuantía de las sanciones, a través de criterios relevantes como la gravedad de la infracción, el incumplimiento normativo a los deberes contenidos en el Régimen de Protección de Datos Personales, el impacto en los datos personales de los afectados, la adecuación típica y la proporcionalidad, entre otros, por medio de gráficos estadísticos que permitan la comparación entre la teoría y los hallazgos de investigación.
3. Elaborar conclusiones a partir del análisis de investigación, fundamentadas en los resultados obtenidos mediante el análisis cuantitativo y teórico, con el propósito de identificar aspectos cruciales en el procedimiento de imposición de sanciones a los Responsables y/o Encargados por el tratamiento inadecuado de datos personales, llevado a cabo por la Superintendencia de Industria y Comercio.

Metodología

Para el diseño de estudio de la presente investigación, la teoría del Derecho Fundamental de *"Hábeas Data"* será el marco conceptual que guiará tanto el enfoque cuantitativo como cualitativo de la investigación. Este marco teórico permitirá evaluar de manera integral el Régimen de Protección de Datos Personales desde una perspectiva jurídica, considerando tanto la normativa legal como la jurisprudencia relacionada. Por otro lado, la comprensión profunda del Indebido Manejo de Datos Personales y del Régimen de Protección de Datos Personales en el contexto colombiano será esencial para interpretar y contextualizar las Resoluciones analizadas. Se examinarán los principios legales, los deberes y derechos de las partes involucradas, así como cualquier evolución normativa que haya impactado en la toma de decisiones de la Superintendencia de Industria y Comercio. Con esta metodología, se busca ofrecer una visión completa y detallada de las sanciones impuestas por la Superintendencia de Industria y Comercio en el ámbito del tratamiento indebido de datos personales, contribuyendo así al entendimiento de los mecanismos y criterios aplicados en la protección de la privacidad y derechos fundamentales en el entorno de Protección de Datos Personales en Colombia.

En concordancia, para el Enfoque Cuantitativo respecto al Análisis Estadístico de Resoluciones y para el Enfoque Cualitativo en cuanto al Análisis Detallado de Resoluciones Seleccionadas, se especifica que la primera fase de la investigación consistirá en una revisión exhaustiva de todas las Resoluciones emitidas por la Superintendencia de Industria y Comercio en el periodo comprendido entre el 1 de enero y el 31 de diciembre de 2022. Por tanto, se recopila información, que será objeto de un estudio de datos cuantitativos relevantes que permita obtener hallazgos respecto a cualquier patrón temporal identificable. Este enfoque permitirá una visión panorámica de las acciones disciplinarias tomadas por la entidad. Bajo la misma línea, en una segunda fase, se llevará a cabo un análisis cualitativo detallado de un subconjunto representativo de Resoluciones seleccionadas. Esta elección se realizará con base en la relevancia de los casos, la naturaleza de las infracciones y cualquier patrón emergente identificado en la fase cuantitativa. El análisis cualitativo se centrará en la identificación de factores específicos que contribuyan al comprender la naturaleza del indebido manejo de datos personales, las características comunes de las infracciones, y la aplicación de los principios del Régimen de Protección de Datos Personales y el Derecho Fundamental de *"Hábeas Data"* en cada caso.

Con la finalidad de responder a los objetivos planteados, tanto el objetivo general como los objetivos específicos del presente trabajo, realizaremos un análisis documental de las resoluciones de la Superintendencia de Industria y Comercio respecto a las sanciones por infracciones de protección de datos personales, empleando así una estrategia cuantitativa y cualitativa desde la teoría del Derecho Fundamental de *"Hábeas Data"*, el Indebido Manejo de Datos Personales y el Régimen de Protección de Datos Personales, que nos permita analizar la tendencia de las Resoluciones expedidas por la misma, en razón a que, por la naturaleza de los datos, se requiere de una investigación cuantitativa con base a la investigación directa de campo y de observación, siendo las Resoluciones de estudio las siguientes:

1. Resolución 88011 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Charry Trading S.A.S.

2. Resolución 86797 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Master Travel Sale S.A.S Sigla Master Sale 38.

3. Resolución 85183 de 2022 por medio de la cual se impone una sanción administrativa a la compañía CareStream Health Colombia LTDA En liquidación.

4. Resolución 83133 de 2022 por medio de la cual se impone una sanción administrativa al Club Residencial VIZTA Propiedad Horizontal.

5. Resolución 81963 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Simba Software S.A.S.

6. Resolución 79999 de 2022 por medio de la cual se impone una sanción administrativa a la compañía J.M.G Consultores S.A.S.

7. Resolución 79324 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Servicios Especializados FCB S.A.S.

8. Resolución 78501 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Salud Actual IPS LTDA.

9. Resolución 77654 de 2022 por medio de la cual se impone una sanción administrativa a la Compañía Integral de Servicios Técnicos en Limpieza CISTEL LTDA.

10. Resolución 77643 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Seguridad El Progreso LTDA.

11. Resolución 77643 de 2022 por medio de la cual se impone una sanción administrativa al Conjunto Residencial Los Arrayanes de Sauzalito P.H.

12. Resolución 77556 de 2022 por medio de la cual se impone una sanción administrativa al Instituto De Neurorehabilitación y Psiquiatría de Colombia S.A.S.

13. Resolución 75666 de 2022 por medio de la cual se impone una sanción administrativa a la compañía COLENER S.A.S.

14. Resolución 74662 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Fitness People-Centro Médico Deportivo S.A.S

15. Resolución 73813 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Hotel Termales del Otoño S.C.A.

16. Resolución 73807 de 2022 por medio de la cual se impone una sanción administrativa al Sindicato de Trabajadores del Hospital San Juan De Dios.

17. Resolución 72784 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Dicomercial De Inversiones y CIA S.C.A.

18. Resolución 69533 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Surti-Global Distribuciones y Representaciones S.A.S

19. Resolución 69177 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Be On Travel S.A.S.

20. Resolución 68923 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Asesorías MontePrieto Limitada.

21. Resolución 64958 de 2022 por medio de la cual se impone una sanción administrativa a la compañía MERVICOL S.A.S.

22. Resolución 60419 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Integral Business Center S.A.S.

23. Resolución 86800 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Carbones Quintana Alvarado S.A.S.

24. Resolución 86027 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Asociación para el Desarrollo Integral de la Comunidad ADICO Alma de Mujer.

25. Resolución 85259 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Gourmet & Vacation People S.A.S.

26. Resolución 85241 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Colombia Móvil S.A E.S.P.

27. Resolución 77559 de 2022 por medio de la cual se impone una sanción administrativa a la compañía DLM Alianza Inmobiliaria LTDA.

28. Resolución 72798 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Comunicación Celular S.A COMCEL S.A

29. Resolución 65630 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Ingeniería de Colombia INCO S.A.S.

30. Resolución 64633 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Blue Suppliers S.A.S.

31. Resolución 63771 de 2022 por medio de la cual se impone una sanción administrativa a la compañía DataSet Tecnologies S.A.S.

32. Resolución 58601 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Grupo Empresarial Dinámica S.A.S.

33. Resolución 55739 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Caja Colombiana de Subsidio Familiar Colsubsidio.

34. Resolución 54056 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Colombia Telecomunicaciones S.A E.S.P BIC.

35. Resolución 53733 de 2022 por medio de la cual se impone una sanción administrativa a la compañía CRC Outsourcing S.A.S.

36. Resolución 51177 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Clínica de la Visión del Valle S.A.S.

37. Resolución 50206 de 2022 por medio de la cual se impone una sanción administrativa a la compañía TSQ S.A.S.

38. Resolución 44870 de 2022 por medio de la cual se impone una sanción administrativa a la compañía NETGOSIT S.A.S.

39. Resolución 42758 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Argeco S.A.S En Reorganización.

40. Resolución 41824 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Liceo Cristiano Vida Nueva EU.

41. Resolución 37431 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Colombia Móvil S.A E.S.P.

42. Resolución 33153 de 2022 por medio de la cual se impone una sanción administrativa a la persona natural Diego Fernando Pino Paredes.

43. Resolución 8028 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Infraestructura Nacional LTDA.

44. Resolución 37200 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Banco Pichincha S.A.

45. Resolución 28367 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Conjunto Residencial Mirador de Takay Propiedad Horizontal.

46. Resolución 13114 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Distribuidora de Pinturas y Acabados 1A Limitada.

47. Resolución 54923 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Clínica Vascular Navarra S.A.

48. Resolución 51683 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Conjunto Residencial Parques de Primavera I Etapas I y II Propiedad Horizontal.

49. Resolución 51179 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Etapa International S.A.S.

50. Resolución 50048 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Centro de Idiomas Universal Learning Academics S.A.S.

51. Resolución 49983 de 2022 por medio de la cual se impone una sanción administrativa a la compañía ZION Group S.A.S.

52. Resolución 47032 de 2022 por medio de la cual se impone una sanción administrativa a la compañía MercadoLibre Colombia LTDA.

53. Resolución 42771 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Torres Aqua P.H.

54. Resolución 40839 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Universidad Católica de Colombia.

55. Resolución 28552 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Grupo Reddial S.A.S.

56. Resolución 26106 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Candamil & Toro Abogados Asociados S.A.S En Liquidación.

57. Resolución 25867 de 2022 por medio de la cual se impone una sanción administrativa a la compañía RAPPI S.A.S.

58. Resolución 25067 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Instituto Triángulo S.A.

59. Resolución 17360 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Grupo Sergem De Colombia A & I S.A.S.

60. Resolución 15909 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Tecnik Limitada.

61. Resolución 15043 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Estructuración y Desarrollo de Proyectos Inmobiliarios S.A.S.

62. Resolución 13593 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Ingeniería y Proyectos de Construcción S.A.S Sigla INPRODCO S.A.S.

63. Resolución 9212 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Proteka S.A.S.

64. Resolución 9128 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Plantar de Colombia Limitada.

65. Resolución 32236 de 2022 por medio de la cual se impone una sanción administrativa a la compañía Academía de Pilotos De Aviación S.A.

Hipótesis

Se hipotetiza que, mediante el análisis cuantitativo y cualitativo de las Resoluciones de la Superintendencia de Industria y Comercio que sancionan a los responsables por indebido tratamiento de datos personales en el periodo de enero a diciembre de 2022, se identificarán patrones y criterios específicos utilizados por la entidad encargada en la imposición de sanciones. Se espera demostrar que la Superintendencia de Industria y Comercio se basa en factores objetivos como la gravedad de la infracción, el impacto en los datos personales de los afectados, la dimensión del daño o peligro a los intereses jurídicos tutelados, el fundamento normativo, y otros criterios relevantes, para aplicar medidas disciplinarias de manera coherente y proporcional a la conducta. La hipótesis se fundamenta en la premisa de que la Superintendencia de Industria y Comercio busca salvaguardar la protección del Derecho Fundamental de Hábeas Data y la privacidad de los Datos Personales con la imperiosa necesidad de imponer sanciones efectivas para garantizar el cumplimiento de las normativas del Régimen de Protección de Datos Personales en Colombia.

Pregunta de investigación:

¿Cuáles son los parámetros específicos que la Superintendencia de Industria y Comercio utiliza para imponer sanciones a los responsables por el indebido tratamiento de datos personales, conforme al análisis de las Resoluciones emitidas por la entidad durante el período de tiempo comprendido entre el 01 de enero de 2022 y el 31 de diciembre de 2022?

Conclusiones esperadas.

Se espera que la investigación proporcione una visión detallada de los criterios y parámetros utilizados por la Superintendencia de Industria y Comercio en la imposición de sanciones por el indebido tratamiento de datos personales. Esto permitirá entender mejor el enfoque de la entidad para preservar la privacidad y proteger los derechos fundamentales en la era digital.

Limitaciones a la investigación.

La investigación se limitará al análisis de las Resoluciones de la Superintendencia de Industria y Comercio emitidas en el año 2022. Además, la disponibilidad y accesibilidad de la información podrían influir en la exhaustividad del análisis.

A continuación, se presenta el Capítulo Número Uno (1) de la Tesis de Grado respecto al Indebido Manejo de Datos Personales con un enfoque en el contenido teórico de los tópicos que componen el Régimen de Protección de Datos Personales en la Ley 1581 de 2012 y los aspectos contenidos en las Resoluciones emitidas por la Superintendencia de Industria y Comercio en el año 2022 para el tema en particular.

En cuanto a la facultad sancionatoria de la Superintendencia de Industria y Comercio frente al Indebido Manejo de Datos Personales.

Para comenzar, es menester mencionar que, en algunos temas en específico de la sociedad, se establecen en la organización territorial autoridades de inspección, control, vigilancia y supervisión, que tienen básicamente por función, analizar si se cumplió o no con la ley e imponer las sanciones en los eventos donde se han infringido los preceptos legales que tienen la capacidad de afectar los derechos de los consumidores, particularmente para este caso en concreto, los derechos de los titulares de la información personal. En Colombia, esta facultad recae en la Superintendencia de Industria y Comercio en el ejercicio de sus facultades jurisdiccionales.

Al igual que, el régimen de la libre competencia, la protección del consumidor, la metrología legal y los reglamentos técnicos, la protección de datos personales, la propiedad industrial y los asuntos jurisdiccionales, son los pilares sobre los cuales la economía de mercado encuentra un equilibrio entre los derechos de carácter económico y social, y las garantías constitucionales de los ciudadanos y consumidores, por ello, la ineludible necesidad de que exista una autoridad competente para dar trámite a las conductas vulneratorias de los derechos inherentes al individuo y el progreso como sociedad.

En consideración al organigrama de la Superintendencia de Industria y Comercio, los encargados de manejar lo relacionado en materia de manejo de Datos Personales, son la Delegatura de Protección de Datos Personales, que cuenta con dos direcciones, a saber, la dirección de Hábeas Data y la dirección de Investigaciones de Protección de Datos Personales. De conformidad con lo establecido en los Artículos 19 y 21 de la Ley 1581 de 2012, la Dirección de Investigación de Protección de Datos Personales, es competente para investigar e imponer las sanciones pertinentes a los Responsables y Encargados del Tratamiento de datos una vez verifique el incumplimiento de las disposiciones en materia de protección de datos.

Por lo que se refiere a la función de inspección, control, supervisión y vigilancia, los siguientes artículos facultan dicha función para la autor, en cuanto a que,

El Artículo 19 de la Ley 1581 de 2012, establece de manera literal que, la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley. Por otro lado, la vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma, como lo es, precisamente el manejo de la

información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, y de servicios.

El Artículo 21 de la Ley 1581 de 2012, establece de manera literal que, con respecto a las funciones que le conciernen, dispone lo siguiente,

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos

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

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

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

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

g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;

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

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

k) Las demás que le sean asignadas por ley.

Para el caso en concreto, y de conformidad con la información recaudada en la investigación de las Resoluciones emitidas por la Superintendencia de Industria y Comercio en el año 2022, específicamente en materia de Indebido Manejo de Datos Personales, se puede evidenciar, que con relación a las funciones en cabeza de la autoridad competente, aquellas que son comúnmente más observadas en el desarrollo de los procedimientos de investigación a los

Responsables o Encargados del Tratamiento son los siguientes literales contenidos en el Artículo 21 de la Ley 1581 de 2012,

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;

Esta disposición hace referencia a que la Superintendencia de Industria y Comercio tiene la responsabilidad de garantizar que las empresas, compañías, sociedades, y demás agentes del mercado sujetos a su supervisión cumplan en su totalidad con las disposiciones legales relacionadas con el Régimen de Protección de Datos Personales. Esto implica asegurarse a través de procesos de inspección, control, supervisión y vigilancia de que las organizaciones limiten su actuar de conformidad con las normativas establecidas en la legislación vigente.

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;

Esta disposición hace referencia a que la Superintendencia de Industria y Comercio tiene la facultad dispositiva de iniciar investigaciones de oficio o en respuesta a una petición interpuesta por un ciudadano. Como resultado de las pertinentes investigaciones, la autoridad está facultada para emitir órdenes con el objetivo de garantizar el ejercicio efectivo del Derecho Fundamental de Hábeas Data, incluyendo la rectificación, actualización o supresión de datos personales del titular cuando se evidencie que es necesario.

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

Esta disposición hace referencia a que la Superintendencia de Industria y Comercio dentro de sus facultades puede proporcionar instrucciones y directrices de orientación y establecer pautas para que los Responsables y Encargados del Tratamiento ajusten sus operaciones de acuerdo con las disposiciones legales en materia de Protección de Datos Personales, para que no se presenten conductas vulneratorias en donde los sujetos Encargados y Responsables del Tratamiento de Datos extralimitan sus operaciones.

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

Esta disposición hace referencia a que la Superintendencia de Industria y Comercio dentro de sus funciones tiene la facultad de solicitar por medio de requerimientos la información necesaria a los sujetos Encargados y Responsables del Tratamiento de Datos para llevar a cabo sus funciones de supervisión y regulación, para verificar que aquellos sujetos están cumpliendo con las disposiciones normativas aplicables.

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;

Esta disposición hace referencia a que la Superintendencia de Industria y Comercio es la autoridad responsable de administrar el Registro Nacional Público de Bases de Datos, que es es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos; además tiene la potestad enmarcada dentro de sus funciones para emitir órdenes y actos necesarios para garantizar su correcto funcionamiento.

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

Esta disposición hace referencia a que la Superintendencia de Industria y Comercio puede a través de oficios a los sujetos Encargados y Responsables del Tratamiento de Datos, proponer ajustes, correcciones o adaptaciones a la normativa vigente, de acuerdo con los avances y cambios en tecnología, informática o comunicación, con el objetivo de mantener actualizadas las regulaciones en materia de Protección de Datos Personales.

En cuanto al procedimiento que adelanta la Superintendencia de Industria y Comercio frente al Indebido Manejo de Datos Personales.

Acerca del procedimiento que adelanta la Superintendencia de Industria y Comercio frente a la existencia de una conducta que vulnere el Régimen de Protección de Datos Personales, la Superintendencia de Industria y Comercio, la Ley 1581 de 2012, en el Artículo 22 y en el Artículo 23 estipula los procedimientos, trámites y sanciones.

El Artículo 22 de la Ley 1581 de 2012, establece lo relacionado al trámite, por tanto, le corresponde a Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes.

El Artículo 23 de la Ley 1581 de 2012, establece literalmente las sanciones a que haya lugar, por ello, La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

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

c) Cierre 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;

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

Se hace la aclaración que las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Para el caso en concreto, y de conformidad con la información recaudada en la investigación de las Resoluciones emitidas por la Superintendencia de Industria y Comercio en el año 2022, específicamente en materia de Indebido Manejo de Datos Personales, se puede evidenciar, que con relación a la función en cabeza de la autoridad competente, en cuanto, podrá impartir las medidas o imponer las sanciones correspondientes bajo el supuesto que se evidencia una conducta vulneratoria al Régimen de Protección de Datos Personales, las sanciones generalmente más usadas por la Superintendencia de Industria y Comercio, son todas aquellas consagradas en el Artículo 23 de la Ley 1581 de 2012, y detalladamente se especifica que,

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

Esta sanción implica la imposición de multas económicas tanto a nivel personal como institucional. La cuantía de estas multas pueden alcanzar hasta el equivalente de dos mil salarios mínimos mensuales legales vigentes al momento de la imposición. Es importante destacar que las multas pueden ser aplicadas de manera sucesiva mientras persista el incumplimiento que generó la sanción, lo que implica que se busca incentivar la corrección de las prácticas indebidas.

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

Esta disposición hace referencia a que la Superintendencia de Industria y Comercio dentro de sus facultades puede ordenar la suspensión de las actividades empresariales relacionadas con el Tratamiento de Datos por un período máximo de hasta seis meses. Durante el acto de

suspensión, se especificarán los correctivos que deben ser implementados para levantar la suspensión temporal. Esta medida está encaminada a detener temporalmente las operaciones que incumplen con las disposiciones normativas de Protección de Datos, por tanto, la entidad sancionada debe abstenerse de llevar a cabo cualquier operación relacionada con el tratamiento de datos personales, dando la oportunidad de corregir sus prácticas, y garantizar que se tomen las acciones correctivas necesarias para levantar la suspensión.

c) 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;

Esta disposición hace referencia a que, si, después del período de suspensión, la entidad no adopta los correctivos ordenados por la Superintendencia de Industria y Comercio, la autoridad competente dentro de sus facultades puede ordenar el cierre temporal de las operaciones relacionadas con el tratamiento de datos personales. Esta medida en comparación con el literal anterior es una restricción más severa que la suspensión de carácter temporal, ya que implica una paralización adicional de las actividades después de que se haya dado la oportunidad de corregir las prácticas vulneratorias. En consecuencia, el cierre temporal se aplica como consecuencia de la falta de corrección de las prácticas después de la suspensión, por ello, busca presionar a la entidad para que tome las medidas necesarias y evite la continuidad de operaciones que violen las disposiciones normativas de protección de datos personales.

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

Esta disposición establece la sanción más drástica que la Superintendencia de Industria y Comercio en Colombia puede imponer a los Encargados y Responsables del Tratamiento de Datos, la cual es el cierre inmediato y definitivo de la operación que involucra el tratamiento de datos sensibles. Los datos sensibles son aquellos que, por su naturaleza, pueden afectar la intimidad del titular, como información médica, orientación sexual, creencias religiosas, entre otros; y el cierre definitivo se aplica como medida extrema en casos graves de incumplimiento que involucren este tipo de información. Esta medida busca proteger de manera efectiva la privacidad y los derechos de los individuos cuyos datos sensibles están siendo tratados de manera inapropiada a las disposiciones normativas, por ello, la gravedad de esta sanción refleja la importancia de resguardar la información más delicada y personal de los titulares.

Concretamente, la diferencia entre suspensión de las actividades relacionadas con el Tratamiento de Datos, el cierre temporal de las operaciones que involucre el Tratamiento de Datos y el cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles consiste en que,

La suspensión o el cese de operaciones que involucre el Tratamiento de Datos es una medida temporal que detiene las operaciones por un período de tiempo en específico, durante el cual se espera que la entidad adopte los correctivos indicados. Sumado a, el cierre temporal, en cambio, ocurre después de que se presenta la suspensión de las operaciones y sólo si los correctivos no se han implementado de manera correcta, lo cual implica una detención adicional de las operaciones hasta que se cumplan las correcciones ordenadas. En otro orden de ideas, el cierre inmediato y definitivo, representa la medida más extrema y radical entre las tres. Se implementa cuando la gravedad del incumplimiento es tan significativa que la entidad no puede o no está dispuesta a corregir las deficiencias identificadas, este nivel de cierre implica la interrupción total y permanente de la operación que involucra el Tratamiento de Datos Sensibles.

De esta manera, la suspensión brinda una oportunidad para corregir las prácticas vulneratorias, mientras que el cierre temporal se aplica en caso de que no se hayan adoptado los correctivos después de la suspensión, lo que refleja una mayor gravedad en el incumplimiento por parte del Encargado o Responsable del Tratamiento de Datos. Sin embargo, ambas medidas impartidas por la Superintendencia de Industria y Comercio en Colombia buscan asegurar el cumplimiento de las normativas de Protección de Datos Personales y proteger los derechos de los titulares de la información. En resumen, la suspensión, el cierre temporal y el cierre inmediato y definitivo son herramientas escalonadas diseñadas para abordar infracciones a la seguridad y protección de datos de manera proporcional a la gravedad de la situación. Cada una de estas medidas busca garantizar el cumplimiento de las regulaciones de privacidad y la salvaguardia de los derechos de los titulares de la información.

Es importante destacar que estas acciones impartidas por la Superintendencia de Industria y Comercio no solo tienen el propósito de imponer sanciones vistas como castigos a la entidad Responsable o Encargada del Tratamiento de Datos Personales, sino que también buscan fomentar una cultura de cumplimiento y responsabilidad en el manejo de datos personales, especialmente de aquellos datos personales que son considerados como sensibles por contener información confidencial, semiprivada o privada. Al proporcionar oportunidades para corregir deficiencias a través de la suspensión y el cierre temporal, se brinda a las empresas o compañías la posibilidad de rectificar sus prácticas y cumplir con las normativas establecidas. En última instancia, el uso de estas medidas debe de considerarse cuidadosamente, evaluando la proporcionalidad y la necesidad de cada una de ellas en función de la gravedad de la violación o vulneración y la disposición de la entidad para abordar y corregir las deficiencias identificadas en el Tratamiento de Datos Personales.

En cuanto al desarrollo conceptual de los tópicos relacionados con el Régimen de Protección de Datos Personales y la Protección de Datos Personales.

Acerca de las nuevas tecnologías de la información y la comunicación para la obtención de datos personales.

En la era digital, las Nuevas Tecnologías de la Información y la Comunicación (TIC) han revolucionado la forma en que interactuamos con el mundo. Sin embargo, este avance tecnológico no está exento de controversias, especialmente cuando se trata de la obtención de datos personales. Colombia, como muchos otros países, se encuentra en un punto crítico donde la necesidad de balancear la adquisición de información de manera ética y legal choca con prácticas cuestionables que podrían violar la privacidad de los individuos, puesto que, en la actualidad, una gran cantidad de datos sobre las personas alrededor del mundo se almacenan en bases de datos en la web de dominio público o privado. La obtención de estos datos, en muchas ocasiones, el titular de la información los ha facilitado por intermedio de su consentimiento y autorización previa, o el polo opuesto, sin su consentimiento, aún cuando es obligatorio obtener la autorización expresa del titular.

El problema fundamentalmente radica en el entorno dinámico de las Nuevas Tecnologías de la Información y la Comunicación (TIC) dentro del ordenamiento jurídico colombiano, donde la obtención de datos personales se convierte en una batalla de confrontación entre la legalidad de las disposiciones normativas y por otro lado, las prácticas que vulnera la privacidad, la intimidad, y la autodeterminación informativa de los titulares de la información, lo que genera debates sobre los derechos fundamentales y la protección de datos.

Por un lado, la obtención legal de datos personales de los titulares mediante las Tecnologías de la Información y la Comunicación, han facilitado la recopilación y gestión eficiente de información para mejorar diversos aspectos de la sociedad. Empresas y organizaciones gubernamentales utilizan estas tecnologías para ofrecer servicios personalizados, mejorar la toma de decisiones y optimizar procesos. En Colombia, la implementación de sistemas tecnológicos en áreas como la salud, la educación y la administración pública ha permitido avanzar hacia una sociedad más conectada y eficiente, por ejemplo, la implementación de sistemas de información ha mejorado la gestión de registros médicos, agilizando el acceso a la atención médica y facilitando la toma de decisiones clínicas. Además, en el ámbito educativo, las plataformas tecnológicas han posibilitado el acceso a la educación a distancia, democratizando el conocimiento y brindando oportunidades a regiones remotas. Sin embargo, este progreso coexiste con una preocupante realidad: La obtención ilegal de datos personales a través de prácticas vulneratorias al Régimen de Protección de Datos Personales.

No obstante, el lado oscuro de estas tecnologías emerge cuando se trata de la obtención ilegal de datos personales. La falta de regulación efectiva y la vulnerabilidad de los sistemas de seguridad pueden verse como la puerta de entrada a prácticas invasivas que comprometen la privacidad de los ciudadanos colombianos. En ocasiones, entidades malintencionadas pueden

acceder a información sensible sin el consentimiento de los individuos, lo que lleva a riesgos como el robo de identidad, el robo de información confidencial, la manipulación de datos personales y la exposición no autorizada de información personal, amenazando la privacidad de los ciudadanos colombianos, debilitando la confianza en la era digital.

En este contexto, el Derecho fundamental a la intimidad con otros aquellos derechos conexos, como el Derecho a la Privacidad y primordialmente el Derecho Fundamental del Hábeas Data, consagrados en la Constitución Política de Colombia de 1991, se erigen como un pilar fundamental, porque los ciudadanos tienen el derecho inalienable de controlar la información que se recopila, almacena y utiliza sobre ellos, es decir, el derecho a controlar su información personal y a decidir cómo y cuándo se comparte. Es por ello que, las operaciones que se enmarcan dentro de las nuevas tecnologías para acceder a la información, como herramientas poderosas, deben operar dentro de límites éticos y legales que respeten estos derechos y libertades individuales.

De lo antes planteado, en el contexto colombiano, la creciente preocupación por la privacidad ha llevado a un debate sobre la necesidad de fortalecer la legislación y la regulación en torno a la protección de datos personales, que se erige como una pieza clave en este rompecabezas. Por ello, el Estado Colombiano, a través de la autoridad competente, la Superintendencia de Industria y Comercio, busca fortalecer su marco legal para salvaguardar la privacidad de sus ciudadanos, alineándose con estándares internacionales de protección, la constante vigilancia, supervisión y control han sido pasos cruciales hacia una mayor seguridad en el manejo de la información personal, sin comprometer o poner en riesgo la seguridad y la privacidad de los ciudadanos. La implementación de medidas como leyes de protección de datos más estrictas, auditorías de seguridad cibernética y la concientización a los Encargados y Responsables del Tratamiento de Datos Personales sobre los riesgos asociados puede contribuir a mitigar los peligros de la obtención ilegal de datos. De ahí que, la importancia de la investigación del presente trabajo de grado, se base en determinar los parámetros en la forma en cómo sanciona la entidad encargada del control y vigilancia de los Responsables y Encargados del Tratamiento a través del análisis a detalle de las Resoluciones Sanciones que emite la Superintendencia de Industria y Comercio por Indebido Manejo de Datos Personales, conforme a los parámetros de investigación.

Acerca del Régimen de Protección de Datos Personales.

En el marco del ordenamiento jurídico colombiano, la regulación de la protección de datos personales encuentra su fundamento principalmente en la segunda parte del Inciso Primero y en el Inciso Segundo del Artículo 15 de la Constitución Política de Colombia. El propósito fundamental de este régimen está orientado a determinar la manera en la que se va a posibilitar el conocimiento, actualización y rectificación de la información que se haya recogido sobre las personas en las bases de datos o archivos, y la protección de las demás potestades, facultades y garantías que emanan de la constitución con relación al tema.

La jurisprudencia derivada del Artículo 15 de la Constitución Política de Colombia ha proporcionado orientación sobre los derechos y obligaciones resultantes de este mandato. Sin embargo, no fue hasta el año 2008 que se promulgó una ley específica que estableciera un marco claro para la protección de datos personales. En ese año, entró en vigor la Ley 1266 de 2008, que delimita el ámbito de protección de la información en bancos de datos de índole financiera. Esta ley principalmente define los derechos de los titulares de la información y las responsabilidades de las entidades que manejan datos personales relacionados con información financiera, crediticia y comercial. No obstante, la Sentencia C-1011 de 2008 evaluó el marco de protección establecido por dicha ley y concluyó que la protección se limitaba claramente a un tipo específico de datos. Como resultado, se consideró necesario establecer un ámbito de protección más amplio que cubriera todos los tipos de datos procesados por cualquier entidad, ya sean pertenecientes a una persona natural o jurídica. Por ello, surge la Ley 1581 de 2012, que establece disposiciones generales sobre la protección de datos, exige el cumplimiento de los principios que la ley describe para todo tipo de datos y diferencia claramente la regulación de la Ley 1266.

El Régimen General de Protección de Datos Personales, en la Ley de Protección de Datos Personales reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

Acerca del Tratamiento de Datos Personales.

Según la ley 1581 del año 2012, debe entenderse por tratamiento, "*Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"*.

Esta definición abarca una amplia gama de acciones que pueden llevarse a cabo con la información personal de los titulares, resaltando la necesidad de comprender las distintas fases que abarca el manejo conforme al Tratamiento de Datos Personales y regular todo el ciclo de vida del dato. Respecto a las operaciones que se pueden desarrollar con los datos personales; la recolección engloba la obtención inicial de datos personales, ya sea de manera directa o indirecta por parte del Encargado o Responsable del Tratamiento a través de bases de datos. El almacenamiento de los datos personales se refiere a la retención y conservación de dicha información en sistemas o archivos generalmente por medio de las Tecnologías de la Información y la Comunicación. El uso de los datos personales de los titulares implica la utilización de los datos para los fines previamente establecidos y autorizados a los Encargado o Responsable del Tratamiento en el desarrollo de sus actividades empresariales. La circulación comprende la transferencia, difusión o comunicación de los datos a terceros, ya sea dentro del país o hacia el exterior. La supresión, por su parte, se refiere a la eliminación o destrucción de los datos una vez que ya no son necesarios para los propósitos para los cuales fueron recolectados.

La definición de lo que debe entenderse por Tratamiento busca garantizar que todas las etapas del proceso de tratamiento de datos personales de los titulares de la información estén sujetas

a regulaciones específicas y que se protejan los derechos de los titulares de la información en cada una de estas instancias. En este contexto, la Ley 1581 de 2012 establece los lineamientos claros para asegurar que el tratamiento de datos personales se realice de manera transparente, segura y respetando la privacidad y autonomía de las personas involucradas.

Acerca de la Protección de Datos Personales.

La protección de datos personales es un concepto circunscrito al marco del derecho informático; se trata fundamentalmente del derecho de cualquier persona de ejercer control y autoridad sobre la información respecto de la cual le asiste una titularidad, y ello se hace en la medida en que sobre ella se está realizando un tratamiento de datos en el ejercicio de las funciones de manejo y/o administración, por parte de una entidad pública o privada y en esa medida se debe proveer un sistema o régimen legal que determine cómo debe realizarse el mismo.

En este contexto, la protección de datos personales se erige como un mecanismo fundamental para salvaguardar la privacidad, la autonomía y los derechos de las personas en relación con la información que les concierne. Este derecho implica que las entidades encargadas de recopilar, almacenar, utilizar o compartir datos personales deben hacerlo de manera ética, transparente y conforme a las disposiciones legales establecidas.

La implementación efectiva de un régimen de protección de datos implica la definición de normativas claras que regulen el tratamiento de la información personal, establezcan los derechos de los titulares de datos y delineen las responsabilidades de las entidades que manejan dicha información. Este enfoque legal busca equilibrar la necesidad de utilizar la información para diversas finalidades legítimas con la protección de la privacidad y los derechos individuales. En última instancia, la protección de datos personales contribuye a preservar la confianza en los procesos de manejo de información y promover un entorno en el que las personas puedan ejercer un control adecuado sobre sus datos personales.

El sistema legal colombiano busca, por tanto, equilibrar la necesidad de las entidades de realizar tratamientos de datos para sus funciones legítimas con la protección de los derechos fundamentales de los individuos. En este sentido, se destaca la importancia de obtener el consentimiento informado de los titulares de los datos antes de su tratamiento, así como la obligación de garantizar la seguridad de la información y respetar los derechos de acceso, rectificación, actualización y supresión de los datos por parte de los titulares.

En resumen, la protección de datos personales en Colombia no solo se concibe como una obligación legal, sino como un medio para promover la confianza y el respeto hacia la privacidad de los ciudadanos, contribuyendo así al desarrollo de un entorno digital seguro y ético.

Acerca de las etapas del Ciclo de Vida del Dato Personal.

En el contexto de la gestión de datos personales en Colombia, las etapas del ciclo de vida de la información son cruciales para garantizar el cumplimiento de la legislación de protección

de datos y respetar los derechos fundamentales de los individuos. A continuación, se abordan las etapas de recolección, circulación y disposición final de los datos personales:

Recolección de Datos Personales:

Dentro del ciclo de vida de los datos, la etapa de recolección de datos personales desempeña un papel crucial. En esta fase inicial, las organizaciones deben llevar a cabo procesos meticulosos para garantizar la gestión ética y legal de la información personal de los individuos.

Primero, se destaca la importancia de establecer claramente el propósito para el cual se recopilan los datos. Esto implica definir con precisión los objetivos específicos que justifican la recolección, asegurándose de que esté alineada con las metas de la organización y que cumpla con los requisitos legales y éticos. Además, los datos recogidos deben ser pertinentes y necesarios para cumplir de manera efectiva con ese propósito específico, evitando la obtención de información innecesaria o excesiva.

Así mismo, el Responsable y/o Encargado del Tratamiento de Datos Personales, en la etapa de recolección de información del titular, dentro del desarrollo de sus deberes tiene la obligación de indicar la siguiente información de manera expresa, clara y detallada, así las cosas,

a) El tratamiento al cual serán sometidos y la finalidad con la que es recaudado el dato personal.

b) Los derechos que le asisten como Titular de la información.

c) La información y los canales de comunicación a través de los cuales los Titulares pueden ejercer sus derechos ante el Responsable y/o Encargado del Tratamiento.

d) El carácter facultativo que tiene el Titular de dar o no respuesta a preguntas que versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

Un aspecto esencial de esta fase es obtener el consentimiento informado de los titulares de los datos. Este proceso debe ser claro, transparente y comprensible para los individuos, permitiéndoles tomar decisiones informadas sobre el uso de sus datos personales. El respeto por la privacidad y la autonomía del individuo se refleja en la necesidad de obtener el consentimiento de manera voluntaria y libre de coerción. Asimismo, se destaca la premisa de recolectar la cantidad mínima de datos requerida para cumplir con el propósito establecido. Este enfoque busca evitar la recopilación excesiva de información, promoviendo la limitación en el procesamiento de datos para salvaguardar la privacidad de los individuos.

De ahí las cosas que, la etapa de recolección de datos personales en el ciclo de vida de la información es esencial para el buen manejo de la privacidad y el cumplimiento normativo. Al establecer propósitos claros, obtener consentimiento informado y limitar la recopilación a datos relevantes, las organizaciones contribuyen a construir un entorno de tratamiento de datos ético y responsable.

Circulación de Datos Personales:

En el contexto del ciclo de vida de los datos, la etapa de circulación de datos personales representa una fase crucial que requiere una cuidadosa consideración. Durante esta etapa, la información recolectada se traslada o circula, ya sea dentro de la misma organización o hacia terceros, y es fundamental garantizar que este proceso se realice de manera segura y conforme a las normativas de protección de datos.

En primer lugar, se destaca la importancia de evaluar y gestionar la transferencia internacional de datos. Si la circulación implica la transferencia de información a otro país, se deben tomar medidas para asegurar que dicho país ofrezca un nivel adecuado de protección de datos. En caso contrario, es esencial establecer salvaguardias apropiadas que protejan la privacidad de los individuos de acuerdo con las leyes y regulaciones colombianas.

Cuando terceros están involucrados en la circulación de datos, se subraya la necesidad de establecer contratos y acuerdos sólidos que regulen la relación entre las partes. Estos documentos deben garantizar que los terceros cumplan con los estándares de protección de datos exigidos por la legislación colombiana, asegurando así la integridad y seguridad de la información personal circulante. La transparencia en el proceso de circulación también juega un papel crucial. Los titulares de datos deben ser informados de cualquier transferencia de sus datos a terceros y deben tener la posibilidad de otorgar su consentimiento para dicha circulación, cuando sea requerido por la normativa de protección de datos.

En definitiva, la etapa de circulación de datos personales en el ciclo de vida de la información demanda un enfoque diligente y ético. Al gestionar la transferencia internacional, establecer contratos sólidos y garantizar la transparencia, las organizaciones contribuyen a construir un entorno de circulación de datos que respete la privacidad y cumpla con las normativas vigentes en Colombia y más allá.

Disposición Final de Datos Personales:

Dentro del ciclo de vida de los datos, la etapa de disposición final de datos personales marca el cierre y la conclusión del tratamiento de la información. Es una fase crítica que requiere atención para garantizar que la privacidad de los individuos se preserve incluso después de que los datos hayan cumplido su propósito inicial.

En primer lugar, es esencial implementar una política de retención limitada. Los datos personales deben conservarse únicamente durante el tiempo necesario para cumplir con el propósito para el cual fueron recopilados. Esta práctica contribuye a evitar riesgos de privacidad asociados con la retención innecesaria de información y garantiza que la organización cumpla con las disposiciones legales y normativas aplicables.

La fase de purgado o eliminación de datos se vuelve crucial en esta etapa. Se deben establecer procedimientos claros y efectivos para la eliminación de datos, asegurándose de que esta acción se lleve a cabo de manera oportuna y en cumplimiento con los plazos establecidos por la normativa. La ausencia de procesos adecuados podría resultar en la retención prolongada de datos más allá de lo necesario, exponiendo a la organización a posibles sanciones y riesgos

reputacionales. Durante la disposición final, ya sea mediante la destrucción de documentos físicos o la eliminación de datos digitales, se deben implementar medidas de seguridad. Esto garantiza la confidencialidad de la información y previene accesos no autorizados, asegurando que los datos no sean comprometidos durante el proceso de eliminación.

Así pues, la etapa de disposición final de datos personales en el ciclo de vida de la información requiere una gestión cuidadosa y responsable. La aplicación de políticas de retención limitada, procedimientos efectivos de purgado y medidas de seguridad sólidas contribuyen a salvaguardar la privacidad de los individuos y a cumplir con las obligaciones legales en materia de protección de datos en el contexto colombiano y más allá.

Por último, en cada una de las etapas del ciclo de vida del Dato, las entidades públicas o privadas encargadas o responsables del Tratamiento de Datos Personales Colombianas deben actuar de conformidad con los preceptos normativos contenidos en la Ley Estatutaria 1581 de 2012 y sus decretos reglamentarios, así como con los principios fundamentales de protección de datos, en cuanto, la comprensión y la debida diligencia en cada una de las etapas contribuyen a fortalecer la seguridad y privacidad de los datos personales, salvaguardando los derechos y libertades de los individuos en un entorno digital que está en constante evolución.

Acerca de la transmisión y la transferencia de los datos personales sujetos al Tratamiento.

De conformidad con la Superintendencia de Industria y Comercio, la operación respecto a 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.

Es decir, en este contexto, la transferencia de datos implica el movimiento de información más allá de las fronteras nacionales, ya sea hacia organizaciones afiliadas o terceros en el extranjero. Este proceso está sujeto a las regulaciones y disposiciones establecidas por las autoridades competentes para garantizar la protección adecuada de los datos personales durante su transmisión y tratamiento en el destino final. En efecto, es fundamental que tanto el Responsable como el Encargado del Tratamiento adopten medidas y salvaguardas adecuadas para asegurar que la transferencia de datos cumpla con los principios y normativas de privacidad aplicables, tanto a nivel nacional como internacional. Estas medidas pueden incluir la firma de acuerdos de transferencia de datos, la verificación de estándares de seguridad en el país receptor y la obtención de autorizaciones correspondientes, según sea necesario.

Por otro lado, la operación acerca de la transmisión de datos personales por su parte implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia y tiene por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable.

Es decir, en este contexto, la transmisión de datos se produce cuando el Responsable del Tratamiento confía al Encargado la tarea específica de llevar a cabo ciertas operaciones o

procesos relacionados con la información personal. Esta comunicación puede implicar la transferencia de datos a terceros, ya sea dentro del país o en el extranjero, siempre que sea necesario para el cumplimiento de las finalidades establecidas en el tratamiento de datos.

En cuanto, la posibilidad de transferir Datos Personales a terceros países, de conformidad con la Ley 1581 de 2012, prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Sin embargo, esta prohibición no regirá cuando se trate de las siguientes condiciones a saber,

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

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

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

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

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

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

Es menester mencionar que, es esencial que esta transmisión de datos se realice en estricto cumplimiento de las normativas y principios legales aplicables a la protección de datos personales. Tanto el Responsable como el Encargado del Tratamiento deben garantizar que se tomen las medidas necesarias para preservar la confidencialidad, integridad y disponibilidad de la información durante todo el proceso de transmisión y tratamiento. Por otro lado, dentro del desarrollo de estas operaciones se suelen requerir la formalización de acuerdos contractuales entre el Responsable y el Encargado, estableciendo claramente las responsabilidades, obligaciones y medidas de seguridad a ser implementadas para salvaguardar los datos personales involucrados en la transmisión.

Acerca de la definición de datos personales.

En términos generales, la Superintendencia de Industria y Comercio, ha definido los Datos Personales, como, toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.

Los datos personales son un pilar fundamental para que una persona pueda interactuar con otros individuos, empresas o entidades, permitiendo su plena individualización en la

sociedad. Esta información es la base para la generación de flujos de datos que contribuyen al crecimiento económico y al mejoramiento de bienes y servicios. Por ejemplo, al solicitar un crédito, se deben proporcionar datos personales en formularios, o al realizar una compra, la factura puede requerir información como el número de documento de identidad, correo electrónico, dirección y teléfono de contacto. El intercambio de datos personales juega un papel esencial en las transacciones cotidianas, facilitando la comunicación y la prestación de servicios. Sin embargo, es crucial manejar esta información de manera responsable, respetando la privacidad y cumpliendo con las regulaciones para garantizar la confidencialidad y seguridad de los datos de cada individuo.

La Ley 1581 de 2012 hace énfasis en que, los principios y disposiciones normativas de la legislación en materia de Protección de Datos Personales se extenderán a la información personal inscrita en cualquier banco de datos que pueda ser objeto de procesamiento dentro del territorio colombiano, ya sea por entidades de naturaleza pública o privada. Asimismo, esta aplicación será válida cuando el Responsable del Tratamiento o Encargado del Tratamiento, que no esté establecido en el territorio nacional, esté sujeto a las leyes colombianas debido a disposiciones de normativas y acuerdos internacionales.

En este orden de ideas, también se especifica, a qué tipo de datos no se aplican las disposiciones normativas consagradas en la Ley 1581 de 2012, por tanto, no están sujetos a dicho régimen los siguientes,

a) Los datos personales contenidos en bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. No obstante, cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al titular y solicitar su autorización. En este caso, los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.

b) Los datos personales contenidos en bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.

c) Los datos personales contenidos en bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.

d) Los datos personales contenidos en bases de datos y archivos de información periodística y otros contenidos editoriales.

e) Los datos personales contenidos en bases de datos y archivos regulados por la Ley 1266 de 2008.

f) Los datos personales contenidos en bases de datos y archivos regulados por la Ley 79 de 1993.

En la misma línea acerca de las disposiciones normativas acerca del Tratamiento de Datos Personales, se especifica lo relacionado con la información personal de menores de edad, que cuenta con una protección especial, prohibiendo el tratamiento de los datos personales en

cabeza de menores de edad, a menos que se refiera a datos de carácter público según lo dispuesto en el Artículo 7° de la Ley 1581 de 2012. En casos en los que dicho tratamiento cumpla con los siguientes criterios y requisitos:

a) Debe estar en concordancia y respetar el interés superior de los niños, niñas y adolescentes.

b) Se debe garantizar el respeto de sus derechos fundamentales.

Como consecuencia de los criterios mencionados anteriormente, una vez cumplidos los requisitos anteriores, la autorización deberá ser otorgada por el representante legal del menor, previo al ejercicio por parte del menor de su derecho a ser escuchado. La opinión del menor será evaluada considerando su madurez, autonomía y capacidad para comprender el asunto. Cualquier responsable o encargado involucrado en el tratamiento de los datos personales de menores deberá asegurar el uso adecuado de los mismos, aplicando los principios y obligaciones establecidos en la Ley 1581 de 2012 y su decreto reglamentario.

Ahora bien, las disposiciones sobre protección de datos, establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación, y se encuentran clasificadas de la siguiente manera; Dato Público, Dato Semiprivado, Dato Privado y Dato Sensible, las cuales serán detalladas a continuación.

Acerca de la definición de Dato Público.

Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados. Es decir, dentro de esta acepción se encuentra la información que no es considerada como privada y está disponible para el público en general. Estos datos pueden ser consultados y utilizados sin restricciones, ya que su divulgación no afecta la privacidad de la persona. Ejemplos incluyen información en registros públicos, datos en directorios telefónicos y datos publicados oficialmente por entidades gubernamentales.

Acerca de la definición de Dato Semiprivado.

Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas. Es decir, dentro de esta definición se encuentra la información que no es de naturaleza íntima, pero cuyo acceso y uso están restringidos a un grupo específico de personas o entidades. Requiere autorización del titular para su tratamiento. Ejemplos pueden ser datos laborales o académicos que, aunque no son íntimos, no están destinados al conocimiento público general.

Acerca de la definición de Dato Privado.

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información. Es decir, dentro de esta acepción se encuentra la información de carácter sensible que afecta la intimidad del titular. Su tratamiento y divulgación están sujetos a la autorización expresa del titular. Ejemplos incluyen datos biométricos, historias clínicas,

orientación sexual, creencias religiosas, entre otros, que están reservados a la esfera privada de la persona.

Acerca de la definición de Dato Sensible.

Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación. Es decir, dentro de esta definición se encuentra la categoría especial de datos personales que pueden revelar aspectos íntimos o particulares del titular. El tratamiento de estos datos requiere un nivel más alto de protección y generalmente está sujeto a restricciones más estrictas. Incluye información sobre la salud, origen étnico, opiniones políticas, afiliación sindical, entre otros aspectos sensibles de la vida de una persona.

En términos generales, la Ley 1581 de 2012 prohíbe el Tratamiento de Datos Sensibles, salvo en las siguientes condiciones:

a) Cuando el Titular haya otorgado su autorización explícita para dicho tratamiento, a menos que la ley no exija específicamente dicha autorización.

b) En caso de que el tratamiento sea necesario para preservar el interés vital del Titular y este se encuentre incapacitado física o legalmente. En tales circunstancias, se requiere la autorización de los representantes legales.

c) Cuando el tratamiento se realice dentro de las actividades legítimas de una fundación, Organización No Gubernamental (ONG), asociación u otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre y cuando se refiera exclusivamente a sus miembros o a personas que mantengan contactos regulares en función de sus objetivos. En estos casos, los datos no podrán ser proporcionados a terceros sin la autorización expresa del Titular.

d) Si el tratamiento está relacionado con datos necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e) Cuando el tratamiento tenga una finalidad histórica, estadística o científica, siempre y cuando se tomen medidas adecuadas para garantizar la supresión de la identidad de los titulares de la información.

Acerca de los sujetos obligados en virtud del Régimen de Protección de Datos Personales.

La Ley 1266 de 2008 introduce dos conceptos fundamentales, a saber, la fuente de la información, que es la persona encargada de recibir datos del titular en el contexto de relaciones comerciales u otros servicios, y el operador de la información, quien administra y divulga dicha información a los usuarios. Este último es aquel que tiene acceso directo a estos datos y, por ende, está sujeto a las responsabilidades establecidas por la ley.

Por otro lado, la Ley 1581 de 2012 aborda dos factores clave en el tratamiento de datos. En primer lugar, se menciona al Encargado del Tratamiento de Datos, ya sea una persona natural

o jurídica, responsable de llevar a cabo el tratamiento conforme a las indicaciones del responsable. En segundo lugar, se hace referencia al Responsable del Tratamiento de Datos, que es la persona encargada de decidir cómo se realiza el tratamiento de las bases de datos. En este contexto, ambas leyes establecen un marco legal que regula las responsabilidades y roles de quienes manejan y gestionan información personal.

Acerca de la definición del titular de la información.

En lo que respecta a la definición del titular de la información, tanto el marco legal establecido por la Ley 1266 de 2008 como el de la Ley 1581 de 2012 abordan este concepto. En este análisis, se considera titular de la información a toda persona, ya sea natural o jurídica, que está siendo objeto de manipulación en relación con sus datos almacenados en una base o banco de datos.

No obstante, existen diferencias fundamentales entre ambos sistemas de protección de datos. Mientras que el régimen establecido por la Ley 1266 del año 2008 protege datos de personas tanto naturales como jurídicas, la Ley 1581 del año 2012 se enfoca exclusivamente en la protección de datos de personas naturales. Además, cabe destacar que, a diferencia de la ley promulgada en 2008, la ley de 2012 abarca un marco general de protección en lugar de limitarse únicamente a la información financiera. Estas distinciones delinean claramente las áreas de cobertura y los enfoques específicos de cada uno de estos regímenes de protección de datos personales.

Acerca de la autorización del titular de la información para el Tratamiento de Datos Personales.

La autorización del titular de la información se refiere al consentimiento previo, expreso e informado otorgado por el Titular para llevar a cabo el Tratamiento de sus Datos Personales.

Este consentimiento debe obtenerse utilizando cualquier medio que pueda ser consultado posteriormente dado las circunstancias en que sea necesario y se requiera. El Responsable del tratamiento está obligado a implementar procedimientos que le permitan solicitar la autorización del Titular, como máximo en el momento de la recolección de sus datos. Además, debe informar al Titular sobre los datos personales que se recolectarán y todas las finalidades específicas del tratamiento para las cuales se solicita el consentimiento.

La autorización del titular de la información se considera válida y legal cuando se expresa por escrito, de forma oral a través de medios electrónicos, de manera física y presencial o mediante conductas inequívocas del Titular que permitan concluir razonablemente que ha otorgado su consentimiento. No será necesaria la autorización en ciertos casos, como cuando se trata de información solicitada por una entidad pública o administrativa en ejercicio de sus funciones legales, datos de naturaleza pública, situaciones de urgencia médica o sanitaria, tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos, o datos relacionados con el Registro Civil de las personas.

En casos de tratamiento de datos sensibles, no se puede condicionar ninguna actividad que implique la recolección de datos personales y el suministro de información al hecho de que el Titular proporcione datos sensibles. Sin embargo, si el tratamiento es posible según lo establecido en la Ley 1581 de 2012, se deben cumplir las obligaciones siguientes:

a) Informar al Titular que no está obligado a autorizar el tratamiento de datos sensibles.

b) Informar de manera explícita y previa, además de cumplir con los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos serán tratados como sensibles, la finalidad del tratamiento y obtener su consentimiento expreso.

Sintetizando, la autorización en el tratamiento de datos personales representa un aspecto fundamental para garantizar el respeto a la privacidad y autonomía del Titular. La obligación del Responsable del tratamiento de informar de manera clara y detallada sobre los datos a recolectar y las finalidades específicas del tratamiento, así como la posibilidad de obtener el consentimiento de manera expresa, contribuye a establecer una relación transparente y ética en el manejo de la información personal.

Es imperativo reconocer que, si bien existen excepciones en las cuales la autorización no es necesaria, dichas excepciones deben interpretarse y aplicarse con cautela, asegurando siempre la protección integral de los datos sensibles. La conciencia y el cumplimiento riguroso de estas normativas son esenciales para preservar la confianza del público en el manejo de sus datos personales, así como para respaldar los principios fundamentales de privacidad en el entorno digital y legal.

Acerca de la definición de Encargado del Tratamiento de Datos Personales.

Hace referencia a la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

En relación con la definición de Encargado del Tratamiento, esta hace alusión a la figura de la persona natural o jurídica, ya sea de carácter público o privado, que lleva a cabo el tratamiento de datos personales en nombre y por cuenta del Responsable del Tratamiento. Este rol implica que el Encargado asume la responsabilidad de gestionar los datos conforme a las directrices y especificaciones establecidas por el Responsable.

El Encargado del Tratamiento puede operar de manera independiente o en colaboración con otros actores, desempeñando un papel fundamental en la ejecución de las operaciones relacionadas con el tratamiento de datos personales. Su función abarca desde la recopilación y almacenamiento de la información hasta su procesamiento y eventual disposición final, todo ello bajo la supervisión y autorización del Responsable del Tratamiento.

Esta relación entre el Responsable y el Encargado está fundamentada en la confianza y la necesidad de asegurar que el tratamiento de datos se lleve a cabo de manera ética y conforme a las normativas de protección de datos vigentes. La colaboración efectiva entre estas dos

partes contribuye a garantizar la integridad y la seguridad de la información personal, así como el cumplimiento de las obligaciones legales y normativas aplicables en materia de protección de datos.

Acerca de la definición de Responsable del Tratamiento de Datos Personales.

Hace referencia a la Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

La figura del Responsable del Tratamiento es esencial en el marco de la protección de datos personales. Este término hace referencia a la persona natural o jurídica, ya sea de carácter público o privado, que, de manera independiente o en colaboración con otros, tiene la facultad de tomar decisiones fundamentales sobre la base de datos y el tratamiento de los datos personales asociados.

El Responsable del Tratamiento asume una posición central en el proceso de gestión de datos, ya que es quien determina los propósitos y las modalidades del tratamiento. Su responsabilidad se extiende desde la recopilación inicial de la información hasta su eventual disposición final, pasando por todas las fases intermedias del ciclo de vida de los datos.

La toma de decisiones sobre el tratamiento de datos implica considerar aspectos cruciales como la finalidad del tratamiento, la necesidad de recopilación de información específica, los métodos de procesamiento y las medidas de seguridad implementadas. El Responsable del Tratamiento debe actuar de manera diligente y ética, garantizando el cumplimiento de las normativas de protección de datos y respetando los derechos fundamentales de los titulares de la información.

Además, su papel incluye la supervisión y gestión de las relaciones con los Encargados del Tratamiento, si los hubiera, así como la atención a solicitudes de los titulares de datos en el ejercicio de sus derechos. En resumen, la figura del Responsable del Tratamiento representa la piedra angular de la responsabilidad y la transparencia en el manejo de datos personales, contribuyendo al desarrollo de un entorno confiable y seguro para los individuos y las organizaciones involucradas.

Acerca de la vulneración a los mandatos dictados por los regímenes de protección de datos.

La vulneración de las disposiciones normativas establecidas por los regímenes de protección de datos, como los contemplados en la Ley 1266 de 2008 y la Ley 1581 de 2012, implica una seria amenaza para la privacidad y los derechos de los titulares de la información. Ambas leyes establecen mecanismos para la solución de controversias en beneficio de los titulares, siendo la consulta y la reclamación los instrumentos principales.

Estos procedimientos, si bien comparten similitudes esenciales, se aplican de manera específica según la legislación correspondiente. La consulta y la reclamación representan vías para que los titulares de la información ejerzan sus derechos y busquen respuestas o

rectificaciones en caso de posibles vulneraciones. En situaciones donde se sospeche una vulneración de la privacidad o un manejo inadecuado de la información, los titulares tienen el derecho de iniciar procesos de consulta y reclamación. Estos procedimientos se presentan ante las entidades u organizaciones responsables de cumplir con los regímenes de protección de datos, exigiendo respuestas claras y acciones correctivas.

La efectividad de estos mecanismos radica en su capacidad para proporcionar soluciones rápidas y justas en casos de presunta violación de los derechos de los titulares de la información. Estos sistemas no solo fortalecen la protección de la privacidad, sino que también fomentan la rendición de cuentas y la transparencia en el tratamiento de datos personales, contribuyendo así a la confianza en los procesos de gestión de información.

Acerca de los niveles adecuados de protección para los Datos Personales sujetos al Tratamiento.

El término *"nivel adecuado"* en el manejo de datos personales se refiere al grado de protección y seguridad que un país o entidad proporciona a la información personal de los individuos. Este concepto está vinculado a la privacidad y la seguridad de los datos, y generalmente implica que el país o entidad cumple con ciertos estándares y normativas para garantizar la integridad, confidencialidad y disponibilidad de la información personal.

El nivel adecuado de protección de datos puede incluir aspectos como la existencia de leyes y regulaciones sólidas en materia de privacidad, la implementación de medidas de seguridad tecnológicas y organizativas, la supervisión por parte de autoridades competentes, y la existencia de mecanismos efectivos para hacer valer los derechos de los individuos respecto a sus datos personales.

En el contexto de transferencias internacionales de datos, algunos países o regiones pueden considerar que otros países ofrecen un nivel adecuado de protección de datos, lo que facilita la transferencia de información personal entre ellos. En caso contrario, es posible que se requieran medidas adicionales, como cláusulas contractuales, acuerdos específicos o la aprobación de autoridades regulatorias, para garantizar la protección de los datos personales en el país receptor.

Se considera que un país garantiza un nivel adecuado de protección de datos cuando cumple con los estándares establecidos por la Superintendencia de Industria y Comercio en materia de protección de datos. Estos estándares no pueden ser inferiores a los exigidos por la ley nacional a sus destinatarios.

Sin embargo, en situaciones excepcionales, se permite la transferencia internacional de datos a países que no ofrecen niveles adecuados de protección de datos. Esto solo es posible si la Superintendencia de Industria y Comercio emite una Declaración de Conformidad relacionada con la transferencia internacional de datos personales. Para llevar a cabo este proceso, la Superintendencia tiene la facultad de solicitar información y realizar las diligencias necesarias para verificar el cumplimiento de los requisitos que hacen viable la operación.

Acerca del contrato de Protección de Datos Personales.

El contrato suscrito entre el Responsable y los Encargados para el tratamiento de datos personales bajo la jurisdicción y responsabilidad del primero es un documento que establece los parámetros y alcances del tratamiento de datos. En dicho contrato se detallan las actividades específicas que el Encargado llevará a cabo en nombre del Responsable para el manejo de los datos personales, así como las obligaciones que el Encargado asume tanto hacia el Titular como hacia el Responsable.

Este acuerdo contractual compromete al Encargado a aplicar las obligaciones establecidas por el Responsable en su política de tratamiento de la información, y a realizar el tratamiento de datos de acuerdo con la finalidad autorizada por los Titulares y en conformidad con las leyes pertinentes.

Adicionalmente a las obligaciones derivadas de las normativas aplicables, el contrato deberá incluir ciertas obligaciones específicas para el Encargado, entre las cuales se encuentran:

a) Tratar los datos personales conforme a los principios que los protegen.

b) Garantizar la seguridad de las bases de datos que contengan datos personales.

c) Mantener la confidencialidad en relación con el tratamiento de los datos personales.

Asimismo, se establece que las transmisiones internacionales de datos personales entre el Responsable y el Encargado, necesarias para que este último lleve a cabo el tratamiento en representación del Responsable, no requerirán la notificación al Titular ni la obtención de su consentimiento, siempre y cuando exista un contrato que contemple los términos mencionados anteriormente.

En cuanto al Fundamento Normativo de las Resoluciones Sanción emitidas por la Superintendencia de Industria y Comercio para el año 2022 por Indebido Manejo de Datos Personales.

El Régimen de Protección de Datos Personales en el ordenamiento jurídico colombiano está fundamentado en una serie de prerrogativas contenidas en leyes y normativas que buscan salvaguardar y proteger los derechos fundamentales de los titulares de la información personal en relación con el tratamiento de sus datos personales que constituyen la esfera de la información personal, en ocasiones con contenido privado y sensible.

El marco normativo basa su sustento como punto de partida, principalmente en el contenido que se desprende de la Constitución Política de Colombia de 1991, que reconoce un conglomerado de derechos como parte integral de la Protección de los Datos Personales, entre ellos, el principal derrotero en materia de regulación normativa, que es, el Derecho Fundamental de Hábeas Data consagrado en el Artículo 15 de la Carta Política, con otros derechos en conexión con este, como lo son, el Derecho acceso a la Información, el Derecho a la Intimidad, Derecho a la Privacidad, Derecho a la Autodeterminación Informativa,

Derecho de Rectificación, Derecho de Cancelación u Olvido, Derecho a la Portabilidad de Datos y Derecho de Oposición.

A continuación se presenta una explicación detallada de cada uno de los derechos anteriormente mencionados;

Acerca del Derecho Fundamental de Hábeas Data.

El Derecho Fundamental de Hábeas Data en Colombia, consagrado en el Artículo 15 de la Constitución Política de Colombia de 1991, está concebido como el derecho de hábeas data es aquel que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.

La Corte Constitucional lo definió como el derecho que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de su divulgación, publicación o cesión, de conformidad con los principios que regulan el proceso de administración de datos personales. Asimismo, ha señalado que este derecho tiene una naturaleza autónoma que lo diferencia de otras garantías con las que está en permanente relación, como los derechos a la intimidad y a la información.

Este derecho fundamental, que es autónomo que tiene por objeto la protección de datos personales y es diferenciado de otros, como el derecho a la intimidad y a la información, ha sido objeto de análisis jurisprudencial que ha identificado prerrogativas mínimas, tales como el acceso a la información, la inclusión de nuevos datos, la actualización y rectificación de la información, así como la exclusión de datos salvo excepciones. Además, se reconoce su estrecha relación con derechos fundamentales, como la intimidad y el buen nombre. A nivel internacional, diversos instrumentos, como la Carta de los Derechos Fundamentales de la Unión Europea, respaldan la protección de datos personales; dentro del ámbito interno, las Leyes Estatutarias 1266 de 2008 y 1581 de 2012 constituyen la base normativa, siendo la última la ley general que establece principios y límites para el tratamiento de datos personales en Colombia.

Ante la necesidad de llenar el vacío jurídico existente en materia de protección de datos personales en el país, fue promulgada la Ley Estatutaria 1581 de 2012. Esta disposición normativa tiene como finalidad asegurar la protección efectiva de los datos personales, de tal manera que durante todo su tratamiento (recolección, almacenamiento, registro, uso o divulgación) se aseguren altos estándares de calidad en el manejo de la información. Con este propósito, establece una serie de límites para el uso y administración de los datos personales; impone responsabilidades y deberes respecto al tratamiento de los datos, y brinda a sus titulares herramientas para exigir su protección frente a cualquier vulneración.

De esta suerte, la Ley 1581 de 2012 constituye el marco legal general para el tratamiento de los datos personales en nuestro país. Una de las características más importantes de la Ley 1581 de 2012 es la incorporación de una serie de principios que contribuyen en la interpretación de sus disposiciones. Se trata de los principios de legalidad, finalidad, libertad,

veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Este marco legal refleja la evolución y la importancia del derecho de hábeas data para garantizar altos estándares de calidad en el manejo de la información personal en el país.

Acerca del Derecho de Acceso a la Información.

Según la Corte Constitucional de Colombia, en Sentencia T-198 de 2015, el Derecho de Acceso a la Información, debe ser entendido como aquel derecho que,

> *"Implica deberes de conservación documental a cargo de las entidades que custodian y administran la información contenida en archivos y bases de datos, necesaria para acceder al goce efectivo de otros derechos fundamentales. Así, los datos personales, la información laboral, información médica, información financiera y de otra índole contenida en archivos y bases de datos, son la fuente primaria para determinar el acceso o el alcance de ciertos derechos o el cumplimiento de los requisitos para el reconocimiento de derechos y prestaciones sociales."* (Corte Constitucional, Sala Octava de Revisión, T-198,2015).

De aquí que, la Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, respecto a regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, en su Artículo 4 explica a cabalidad el Derecho de Acceso a la Información Pública, estableciendo que, el ejercicio del derecho fundamental de acceso a la información, permite a cualquier persona conocer la existencia y acceder a la información pública que esté en posesión o bajo el control de las entidades obligadas.

El Artículo 4 de la Ley 1712 de 2012, expresa de manera literal que, en ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. De ahí que, el acceso a la información solamente podrá ser restringido bajo condiciones excepcionales. Las excepciones serán limitadas y proporcionales, deberán estar contempladas en la ley o en la Constitución y ser acordes con los principios de una sociedad democrática.

El Derecho de Acceso a la Información genera la obligación correlativa de divulgar proactivamente la información pública y responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes de acceso de los titulares de la información o de terceros interesados, lo que a su vez conlleva la obligación de producir o capturar la información pública. Para cumplir estas disposiciones, los sujetos obligados deberán implementar procedimientos archivísticos que garanticen la disponibilidad en el tiempo de documentos electrónicos auténticos.

Es menester mencionar que el artículo anterior juega un papel realmente importante, en cuanto a que previamente a la expedición de la Ley 1712 de 2014, la Corte Constitucional de

Colombia realizó una revisión de constitucionalidad sobre lo que hasta ese momento era simplemente un proyecto de Ley Estatutaria, con el fin de pronunciarse acerca del Deber de Conservación Documental a cargo de las entidades, afirmando que:

> *El derecho de acceso a documentos públicos impone al menos dos deberes correlativos a todas las autoridades estatales. En primer lugar, para garantizar el ejercicio de este derecho, las autoridades públicas tienen el deber de suministrar a quien lo solicite, información clara, completa, oportuna, cierta y actualizada, sobre su actividad. En segundo lugar, también es necesario que las autoridades públicas conserven y mantengan la información sobre su actividad, ya que, de no hacerlo, se vulnera el derecho de las personas al acceso a la información pública y, en consecuencia, el derecho a que ejerzan un control sobre sus actuaciones.* (Corte Constitucional, Sala Plena, C-274, 2013).

El Derecho de Acceso a Documentos Públicos impone responsabilidades fundamentales a las autoridades encargadas, exigiendo que proporcionen información de manera clara, completa, oportuna, veraz y actualizada a quienes la soliciten, Este compromiso es esencial para asegurar la plena realización de dicho derecho, garantizando así la plena realización de este derecho, siendo de gran relevancia y de interés público que las autoridades conserven y gestionen de manera efectiva la información sobre sus actividades, puesto que, el incumplimiento de esta obligación tendría repercusiones significativas, ya que, la falta de cumplimiento de este deber, afecta el derecho de las personas al acceso a la información pública y, en consecuencia, su capacidad para supervisar las acciones vinculadas al ejercicio de este derecho.

Por último, la relación intrínseca entre el Derecho de Acceso a la Información y la Protección de Datos Personales se establece en un equilibrio delicado entre la transparencia en el manejo de la información contenida en Datos Personales y la salvaguarda de la privacidad individual. El Derecho de Acceso a la Información permite a los ciudadanos solicitar datos en posesión de entidades públicas y privadas, pero esta prerrogativa debe armonizarse con la protección de Datos Personales según la Ley Estatutaria 1581 de 2012. Al ejercer el derecho de acceso, las entidades deben evaluar cuidadosamente la divulgación de información, especialmente de la información considerada como sensible para evitar violar la privacidad de los titulares. Esta interacción entre ambas esferas legales busca conciliar el principio democrático de acceso a la información con la necesidad de resguardar la intimidad, estableciendo límites y condiciones que garanticen una gestión adecuada y ética de los datos personales en el contexto de la administración pública y privada en Colombia.

Acerca del Derecho a la Intimidad.

El Derecho a la intimidad está reconocido como un derecho fundamental protegido por la Constitución Política de Colombia de 1991 en el Artículo 15, que consagra de manera literal que,*"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar".*

La intimidad es un derecho humano fundamental, consagrado en numerosos instrumentos internacionales de derechos humanos. Es esencial para la protección de la dignidad humana y constituye la base de cualquier sociedad democrática. También respalda y refuerza otros derechos, como la libertad de expresión, información y asociación. En consecuencia, las actividades que restringen el derecho a la intimidad, como la vigilancia y la censura, sólo pueden justificarse cuando han sido establecidas por la ley, son necesarias para lograr un objetivo legítimo y son proporcionales al objetivo perseguido.

Este derecho garantiza la esfera más íntima y personal de los individuos, resguardándolos contra intromisiones indebidas en su vida privada, divulgación de hechos privados y restricciones no justificadas en su libertad para tomar decisiones en asuntos que solo conciernen a la persona o su familia. Según la Corte Constitucional de Colombia, en Sentencia T-280 de 2022, se ha considerado en reiteradas ocasiones que el Derecho de Intimidad tiene repercusiones en diferentes niveles o contexto, ya sea el ámbito personal, familiar y social, así como se distinguen otros que se han identificado como ámbitos que cuentan con una protección reforzada.

A saber, en el nivel de mayor resguardo se encuentra la esfera más íntima, que abarca pensamientos o sentimientos muy personales que el individuo expresa solo de manera muy confidencial, como en cartas o diarios estrictamente privados. En este ámbito, la garantía de la intimidad es casi absoluta, ya que solo situaciones o intereses excepcionalmente importantes justifican una intromisión; en el segundo nivel se ubica la esfera privada en un sentido más amplio. Esto se refiere a la vida en entornos generalmente considerados como privados, como el hogar o el ámbito familiar. Aquí, también existe una fuerte protección constitucional, aunque con mayores posibilidades de legítima injerencia externa; el tercer nivel corresponde a la esfera social, relacionada con las características de una persona en sus ámbitos laborales o públicos. En este espacio, la protección constitucional de la intimidad se evidencia en menor proporción, aunque no es inexistente.

De igual manera, la misma Corte Constitucional en las sentencias C-602 de 2016, T-574 de 2017 y C-094 de 2020 expone que el Derecho a la Intimidad tiene diferentes posiciones y relaciones entre las que se encuentran las siguientes,

> *Por una parte, ese derecho le confiere a su titular una facultad. Esta le permite oponerse (cuando no existe justificación suficiente) a: la intromisión en la órbita que se ha reservado para sí o su familia y la divulgación de los hechos privados o resistir a las restricciones a su libertad para tomar las decisiones sobre los asuntos que solo le conciernen a la persona.* (Corte Constitucional, Sala Plena, C-602, 2016).
>
> *En segundo lugar, del derecho a la intimidad se deriva una prohibición o un deber de abstención tanto para las autoridades como para los particulares. Unas y otros se deben abstener de ejecutar actos que impliquen: la intromisión injustificada en dicha órbita; la divulgación de los hechos privados o la restricción injustificada de la libertad de elegir sobre asuntos que solo le conciernen a la persona o a su familia. En tercer lugar, el derecho a la intimidad les impone a las autoridades el deber positivo u obligación de adoptar todas las medidas normativas, judiciales y*

administrativas para asegurar el respeto de las diferentes dimensiones del derecho. (Corte Constitucional, Sala Plena, C-602, 2016).

Desde luego, el derecho a la intimidad puede ser objeto de limitaciones si estas se encuentran debidamente justificadas. Cuando exista autorización del titular o una orden proferida por una autoridad competente y en ejercicio de sus funciones, los terceros pueden conocer asuntos que, en principio, estarían comprendidos por su ámbito de protección. En otras palabras, el derecho a la intimidad puede ser: "susceptible de limitación por razones legítimas y debidamente justificadas constitucionalmente". (Corte Constitucional, Sala Tercera de Revisión, T-574,2017).

Finalmente, el derecho a la intimidad está sustentado en cinco principios que aseguran la inmunidad del individuo frente a la injerencia de los demás y que lo conectan con el habeas data. Por una parte, el principio de libertad. Según este, el registro o divulgación de los datos personales de una persona requiere de su consentimiento libre, previo, expreso o tácito o que el ordenamiento jurídico le imponga una obligación de revelar dicha información con el fin de cumplir un objetivo constitucionalmente legítimo. En segundo lugar, el principio de finalidad. Este implica que la recopilación y la divulgación de los datos de una persona atienda a una finalidad constitucionalmente legítima. En tercer lugar, el principio de necesidad. De acuerdo con el cual la información personal que se tenga que divulgar debe tener una relación de conexidad con la finalidad pretendida mediante su revelación. En cuarto lugar, el principio de veracidad. Este exige que los datos personales correspondan a situaciones reales. Por último, el principio de integridad que ordena que la información que se divulga se presente de manera completa. (Corte Constitucional, Sala Plena, C-094, 2020).

De acuerdo con la Jurisprudencia Colombiana, se puede afirmar entonces que, en relación con la Protección de Datos Personales, el Derecho a la Intimidad confiere al titular de este derecho la facultad de oponerse a la intromisión injustificada en su esfera personal, así como a la divulgación de hechos privados, y le permite resistir a restricciones no justificadas en su libertad para tomar decisiones que solo conciernen a él o a su familia. Este derecho impone tanto a las autoridades como a los particulares la obligación de abstenerse de realizar actos que violen la intimidad de una persona. Además, las autoridades tienen el deber positivo de adoptar medidas normativas, judiciales y administrativas para garantizar el respeto de las diferentes dimensiones de este derecho. Sin embargo, este derecho puede ser objeto de limitaciones debidamente justificadas, como la autorización del titular o una orden de una autoridad competente. En este contexto, el derecho a la intimidad se sustenta en principios como el de libertad, finalidad, necesidad, veracidad e integridad, que aseguran la inmunidad del individuo frente a la injerencia de terceros y lo conectan con el principio del habeas data. En síntesis, el Derecho a la Intimidad en Colombia, según la jurisprudencia, implica tanto facultades como obligaciones, respaldadas por principios que buscan salvaguardar la privacidad y la integridad de los datos personales.

El Derecho a la intimidad y la Protección de Datos Personales están intrínsecamente entrelazados, reflejando la importancia de resguardar la esfera íntima de los individuos en la era digital. La Constitución Política de Colombia de 1991 garantiza el Derecho a la intimidad, mientras que el Régimen de Protección de Datos Personales, estipulado en la Ley 1581 de 2012, establece los marcos normativos para un tratamiento adecuado de la información personal de los titulares de la información. Esta interrelación se materializa a través de la exigencia de consentimiento informado para el manejo de datos y la aplicación de principios que respetan la privacidad de los ciudadanos. Así, la regulación colombiana busca armonizar la necesidad de utilizar datos personales con la protección de los derechos fundamentales, creando un equilibrio que salvaguarda la intimidad y la seguridad de la información en un contexto cada vez más digitalizado.

Acerca del Derecho a la privacidad.

Este derecho ha estado experimentando diferentes cambios, por ello ya no se trata solamente de un límite para la no interferencia a la privacidad o en el ámbito de la vida privada del individuo, sino de salvaguardar la intimidad en un contexto de creciente transferencia y transmisión de datos personales en el entorno de las comunicaciones y la tecnología. Por esta razón, la Corte Constitucional en la Sentencia T-784 de 2004, afirma que, el término de privacidad o de lo privado, se refiere a aquellos asuntos que, en principio, están relacionados exclusivamente con los intereses particulares y específicos de una persona, sin tener impacto o referencia a los demás individuos que conforman la sociedad.

De igual manera la Corte Constitucional de Colombia a través Jurisprudencia ha establecido que la garantía del Derecho a la Privacidad depende de:

> *"En gran parte del lugar donde tienen lugar las acciones humanas. Desde esa perspectiva existen "espacios públicos, en los que el interés general prima sobre el particular y por tanto la intimidad se ve ciertamente menguada; espacios privados en los que el carácter personalísimo del entorno hace que la protección de la intimidad presente un estándar ciertamente más estricto; espacios intermedios, como lo son los semi-privados y otros semi-públicos, que integran características tanto públicas como privadas, los primeros, respectivamente, relacionados con escenarios "cerrados en los que un conjunto de personas comparten una actividad y en los que el acceso al público es restringido" y los segundos, con "acceso relativamente abierto en los que diferentes personas se encuentran en determinado momento para realizar cierta actividad puntual dentro de un espacio compartido: un cine, un centro comercial, un estadio". (Corte Constitucional, Sala Segunda de Revisión, T-407,2012).*

De lo anterior se puede inferir que, el Derecho a la Privacidad no es simplemente un límite a la interferencia en la esfera privada de un individuo, sino que se ha convertido en una salvaguarda de la intimidad en un contexto de creciente transferencia y transmisión de datos personales en el ámbito de las comunicaciones y la tecnología.

En condiciones donde se hace imperiosa la necesidad de salvaguardar la intimidad y la privacidad del individuo, se recalca que el término de privacidad se refiere a asuntos vinculados exclusivamente con los intereses particulares de una persona, sin afectar o referirse a los demás individuos de la sociedad. Además, la garantía del Derecho a la Privacidad, según la jurisprudencia, depende en gran medida del lugar donde tienen lugar las acciones humanas, distinguiendo entre espacios públicos, privados e intermedios. Esta última categoría, que incluye espacios semi-privados y semipúblicos, representa situaciones en las que la protección de la intimidad presenta estándares más flexibles, considerando la naturaleza compartida de ciertos entornos con otros individuos. Inclusive, la Ley estatutaria 1581 de 2012 cumple un rol fundamental, dado que esta busca armonizar la recopilación y tratamiento de información con el deber de respetar la privacidad de los individuos. La Superintendencia de Industria y Comercio es la encargada de supervisar y garantizar la privacidad y la protección de datos personales en Colombia, que se erige como un garante esencial para preservar la dignidad y autonomía de los ciudadanos en el contexto digital que se encuentra en constante evolución.

El Derecho a la Privacidad y la Protección de Datos Personales en Colombia están intrínsecamente ligados, siendo ambos aspectos fundamentales para salvaguardar los derechos individuales en un entorno digital y físico cada vez más interconectado. La Constitución Política de Colombia reconoce expresamente el derecho a la intimidad personal y familiar, estableciendo las bases para la protección de datos como una extensión esencial de la privacidad.

La Ley 1581 de 2012, en cuanto a Protección de Datos Personales, constituye un marco normativo que regula el tratamiento de la información personal por parte de entidades públicas y privadas. Esta ley establece principios rectores, como el consentimiento informado, la finalidad del tratamiento, la calidad de la información, y otros, que buscan garantizar un manejo ético y responsable de los datos. La Superintendencia de Industria y Comercio supervisa y controla el cumplimiento de estas normas, asegurando que las entidades públicas y privadas respeten los derechos de los titulares de la información. El consentimiento, como principio fundamental, se erige como un pilar en la relación entre privacidad y protección de datos, exigiendo que el tratamiento de información personal se realice con la aprobación explícita del titular. Asimismo, los derechos de los titulares, como el acceso, rectificación y supresión, brindan a las personas un control activo sobre su información. En conjunto, este entramado legal y regulatorio busca armonizar la necesidad de utilizar datos personales con el respeto a la privacidad, promoviendo una cultura de protección de datos que salvaguarde los derechos fundamentales de los individuos en la era digital.

Acerca del Derecho a la Autodeterminación Informativa.

Este derecho plantea desafíos importantes para la época actual, puesto que, en la era digital se busca equilibrar el acceso a la información para que los derechos de cada uno de los titulares no sean vulnerados, por ello a través de desarrollo doctrinal, se afirma que:

> *"Ya no se trata de un derecho delimitador de un ámbito de no interferencia, sino que por el contrario representa una forma de protección a la intimidad, pues con el procesamiento de los datos personales, el derecho a la intimidad adquiere hoy perfiles nuevos y distintos, dado que la invasión de la vida privada de los ciudadanos por parte de otros agentes sociales, públicos o privados, y la colisión de este derecho con otro igualmente protegible, el derecho a la información, lo sitúa como derecho ejercitable activamente."* (Riande, s.f, p.6)

> *El Derecho a la Autodeterminación Informativa se conceptualiza como un derecho personal que ostenta las siguientes características: Es originario porque nace con el sujeto activo; Es subjetivo privado, al garantizar el goce de las facultades del individuo; Es absoluto, pues es posible oponerse a las demás personas; Es personalísimo, ya que sólo su titular puede ejercitarlo; Es irrenunciable porque no puede desaparecer por la voluntad; Es variable, dado que su contenido obedece a las circunstancias en las cuales se desarrolla; Es imprescriptible, pues el transcurso del tiempo no lo altera; y es interno, por su consistencia particular y de conciencia.* (Riande, s.f, p.6)

El Derecho a la Autodeterminación informativa es fundamental en la protección de la privacidad del individuo, puesto que la existencia de un entorno más digitalizado, nos recuerda la importancia de salvaguardar el ámbito personal frente a las irrupciones no autorizadas en la era de la información.

El Derecho a la Autodeterminación Informativa está relacionado de manera directa con la Protección de Datos Personales en Colombia, especialmente en el contexto actual de la era digital. Este derecho plantea desafíos relevantes al buscar equilibrar el acceso a la información sin vulnerar los derechos de los titulares de datos. En la actualidad, este derecho no se limita a ser una barrera de no interferencia, sino que se ha transformado en una forma de protección de la intimidad. Con el procesamiento de datos personales, el derecho a la intimidad adquiere nuevos perfiles y se convierte en un derecho activamente ejercitable, en medio de la creciente invasión de la vida privada por parte de diversos agentes sociales, ya sean públicos o privados, y la colisión con otros derechos igualmente protegibles, como el derecho a la información. La Autodeterminación Informativa se conceptualiza como un derecho personal con características como su origen con el sujeto activo, su naturaleza subjetiva privada, su carácter absoluto al permitir la oposición a terceros, su condición personalísima, irrenunciable, variable según las circunstancias, imprescriptible en el tiempo y de índole interno por su consistencia particular y de conciencia. Estas características reflejan la importancia de este derecho como un componente esencial en la protección de la privacidad y la gestión ética de los datos personales en el entorno jurídico colombiano.

Acerca del Derecho de Rectificación.

Este derecho se puede observar como un mecanismo de defensa ante posibles perjuicios derivados de datos imprecisos o erróneos, por ello, contribuye a garantizar la calidad y veracidad de la información que se maneja tanto en las entidades públicas como privadas.

Por esta razón es importante el pronunciamiento de la Corte Constitucional frente a este derecho, el cual lo concibe como:

> *El derecho de rectificación es fundamental. El artículo 20 de la Constitución Política prescribe, en su último inciso, que "se garantiza el derecho a la rectificación en condiciones de equidad". Según la Corte, el ejercicio de este derecho "conlleva la obligación de quien haya difundido información inexacta o errónea de corregir la falta con un despliegue equitativo" y "busca reparar tanto el derecho individual transgredido como el derecho colectivo a ser informado de forma veraz e imparcial".* (Corte Constitucional, Sala Quinta de Revisión, T-921,2002) (Corte Constitucional, Sala Tercera de Revisión, T-512,1992).

Este derecho no solo busca reparar el daño individual causado por información incorrecta, sino también salvaguardar el derecho colectivo a recibir información veraz e imparcial. En este punto lo más importante es preservar la integridad y precisión de la información personal para cumplir de la mejor manera con los principios de legalidad, finalidad, veracidad y calidad que rigen el manejo responsable de los datos personales.

El Derecho de Rectificación, conferido a los titulares de la información en Colombia, establece un vínculo fundamental con la Protección de Datos Personales, en concordancia con los principios de veracidad y actualización consagrados en la normativa de privacidad. Este derecho concede a los individuos la facultad de corregir cualquier inexactitud, imprecisión o desactualización en la información personal que reposa en bases de datos y archivos. Al hacerlo, se contribuye directamente a salvaguardar la veracidad de los datos almacenados, un elemento esencial en la protección de datos personales. Este mecanismo no solo faculta a los titulares de la información, otorgándoles un mayor control sobre su propia información, sino que también se alinea con los principios fundamentales de la legislación de Protección de Datos Personales en Colombia, promoviendo prácticas éticas y garantizando el cumplimiento de los derechos fundamentales de los individuos en el contexto de la gestión de sus datos personales. Así, el derecho de rectificación emerge como una herramienta clave para fortalecer la integridad y la veracidad de la información personal, promoviendo una relación equitativa entre los titulares y aquellos responsables de manejar sus datos en el marco de la protección de datos personales en Colombia.

Acerca del Derecho de Cancelación u Olvido.

Este derecho le permite a las personas eliminar sus datos personales cuando estos ya no son necesarios para la finalidad para la cual fueron recopilados, o cuando ya se ha alcanzado el propósito original del tratamiento. Este derecho está consagrado en numerosos instrumentos internacionales, y es aplicado en distintas legislaciones, por ejemplo, en el ordenamiento jurídico Estadounidense, se utiliza la expresión, *"Right to be forgotten"*, es decir, el derecho a que se olviden de uno, por otro lado, en el ordenamiento jurídico francés, se recurre a la expresión, *"Droit à I'oubli numérique"*, es decir, el derecho al olvido numérico o digital. Por ello, se entiende por este derecho como, la facultad que tienen los individuos para

solicitar la eliminación de su información personal almacenada por terceros cuando ya no sea necesaria para la finalidad original o cuando retiren su consentimiento.

Este derecho, fundamentado en el principio de autodeterminación informativa, otorga a los titulares de la información, el control sobre la permanencia de sus datos en entornos digitales. Esencialmente, posibilita que los titulares de datos gestionen activamente su información, evitando así el uso prolongado e innecesario de datos personales. La eliminación de datos en virtud de este derecho previene el riesgo de uso indebido, se adapta a cambios en las circunstancias de los individuos y respalda la protección de la privacidad y los derechos individuales en el contexto de la gestión de la información personal. Este derecho encuentra respaldo en diversas normativas de protección de datos a nivel internacional, reconociendo la importancia de equilibrar la utilidad de los datos con el respeto a la privacidad de los individuos. Es por ello que,

> *Por medio de este derecho se busca proteger el derecho al honor, a la privacidad del individuo; aunque, además se ven inmersas otras libertades y garantías inherentes del ser humano para su existencia y la titularidad del dato informático de calidad.* (Cano, 2018, p.6).

> *Es el derecho al olvido, el cual hace referencia al derecho que tiene los titulares de la información a "suprimir o eliminar sus datos personales" de cualquier sistema o base de datos en donde estén almacenados, salvo las excepciones establecidas por la ley o por un contrato.* (Decreto 1377, 2013, Artículo 9).

Este derecho no solo busca salvaguardar el honor y la privacidad del individuo, sino también otras libertades y garantías inherentes a la existencia humana y titularidad de datos informáticos de calidad, lo que realmente importante para que los individuos titulares de la información personal puedan ejercer un control efectivo sobre la información que reposa en Bases de Datos, además de que contribuye con ello a una protección más fuerte sobre la privacidad en el entorno digital.

El Derecho de Cancelación u Olvido en Colombia se presenta como un componente esencial dentro del marco de Protección de Datos Personales, estableciendo una conexión significativa con los principios fundamentales de privacidad y control sobre la información personal. Este derecho confiere a los titulares la facultad de solicitar la eliminación o supresión de sus datos personales cuando estos ya no sean necesarios para la finalidad para la cual fueron recopilados, hayan cumplido el propósito original, o existan razones legítimas para su revocación. Esta relación entre el derecho de cancelación y la protección de datos personales se basa en el principio de autodeterminación informativa, permitiendo a los individuos ejercer un mayor grado de control sobre la gestión y permanencia de sus datos en manos de terceros.

En este contexto, el Derecho de Cancelación actúa como una herramienta esencial para salvaguardar la privacidad y autonomía de los titulares, al permitirles decidir cuándo y cómo sus datos personales deben ser eliminados, contribuyendo así a mantener actualizada y relevante la información almacenada. Además, este derecho se alinea con los estándares

internacionales y la normativa colombiana de Protección de Datos Personales, como la Ley 1581 de 2012 y sus decretos reglamentarios, que buscan garantizar el respeto a los derechos fundamentales en el tratamiento de la información personal. En síntesis, el derecho de Cancelación u Olvido fortalece la Protección de Datos Personales en Colombia al proporcionar a los individuos un mecanismo efectivo para controlar la permanencia de su información en entornos digitales y garantizar que esta no sea utilizada de manera indebida o prolongada, en concordancia con los principios de privacidad y autodeterminación informativa.

Acerca del Derecho a la Portabilidad de Datos.

Este derecho no tiene una definición muy clara, sin embargo la Organización de los Estados Americanos (OEA) lo concibe como:

> *"Aquel derecho que le permite al titular obtener una copia de los Datos Personales que hubiere proporcionado al Responsable en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro Responsable sin impedimento, en caso de que lo requiera. El Titular podrá solicitar que sus Datos Personales se transfieran directamente de Responsable a Responsable, cuando sea técnicamente posible. El derecho a la portabilidad de los Datos Personales no afectará negativamente los derechos y libertades de otros."* (Principios actualizados sobre la privacidad y la protección de datos personales, Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos).

De lo anterior, se puede afirmar que es conveniente que los titulares de datos personales deben tener el derecho de obtener una copia estructurada electrónicamente de su información, dado que esto facilita su uso continuo y la posibilidad de transferirlos a otro responsable sin obstáculos cuando así lo deseen.

El Derecho a la Portabilidad de Datos, consagrado en el marco de la Protección de Datos Personales en Colombia, establece una relación fundamental que refuerza la salvaguarda de la privacidad y la autonomía del individuo sobre su información personal. Este derecho, respaldado normativamente por la Ley 1581 de 2012 y sus decretos reglamentarios, se erige como un pilar esencial para fortalecer la relación entre los titulares de la información y las entidades públicas o privadas que gestionan datos personales.

La conexión entre el Derecho a la Portabilidad de Datos y la Protección de Datos Personales en el territorio colombiano se manifiesta en su capacidad para facultar a los titulares de la información, permitiéndoles ejercer un control más significativo sobre su propia información. Al facilitar la transferencia segura y eficiente de datos entre distintas plataformas o proveedores de servicios, este derecho promueve la autodeterminación informativa, habilitando a los individuos para decidir cómo y cuándo desean compartir su información personal. Además, la implementación de la portabilidad de datos contribuye a consolidar y fortalecer los principios fundamentales de la normativa colombiana de

protección de datos, al promover la transparencia en el manejo de la información, reforzar la seguridad en las transferencias y fomentar la competencia en el mercado al permitir a los usuarios elegir servicios basándose en sus preferencias individuales.

El Derecho a la Portabilidad de Datos no solo potencia la capacidad de los titulares para gestionar su información, sino que también se alinea con los valores y principios esenciales de la Protección de datos personales en Colombia, consolidando un entorno más transparente, seguro y respetuoso de los derechos individuales en el tratamiento de la información personal.

Acerca del Derecho de oposición.

Como su nombre lo indica este derecho le confiere a las personas la facultad de contradecir, por razones legítimas y específicas, al procesamiento de datos personales, proporcionando así un mecanismo para mantener el control sobre la información. Por esta razón

> *"El Titular debe tener el derecho de oponerse, en razón de su situación particular, en cualquier momento al Tratamiento de sus Datos Personales cuando tenga una razón legítima para ello o cuando el Tratamiento de sus Datos Personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad. Cuando el Titular se oponga al Tratamiento con fines de mercadotecnia directa, sus Datos Personales deberían dejar de ser tratados para dichos fines."* (Principios actualizados sobre la privacidad y la protección de datos personales, Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos).

Este derecho concede al titular la facultad de contradecir en cualquier momento siempre que exista una razón legítima para ello. Contribuyendo así a establecer un marco normativo que busca salvaguardar la privacidad y autonomía de los individuos.

La interrelación entre el Derecho de Oposición y la Protección de Datos se establece como un mecanismo crucial para salvaguardar la privacidad y autonomía de los individuos en el tratamiento de su información personal. Este derecho otorga a los titulares la facultad de oponerse al procesamiento de sus datos en circunstancias específicas, brindando una capa adicional de control sobre el uso de su información. En el marco de la protección de datos colombiana, especialmente regulada por la Ley Estatutaria 1581 de 2012, el Derecho de Oposición se vincula estrechamente con el principio de consentimiento informado, permitiendo a los titulares retirar su aprobación en cualquier momento. Además, este derecho se manifiesta de manera significativa en contextos como decisiones automatizadas y actividades de marketing, donde los individuos pueden oponerse a ser sujetos de evaluaciones automáticas o a que sus datos se utilicen con fines publicitarios. La normativa colombiana reconoce la importancia de equilibrar el tratamiento de datos con el respeto a las preferencias y derechos fundamentales de los titulares, y el Derecho de Oposición emerge como un elemento esencial para lograr este equilibrio y garantizar una gestión de datos personalizada y respetuosa con la voluntad de los individuos.

Acerca del ámbito de aplicación de fundamento normativo.

El ámbito de aplicación del fundamento normativo, se basa específicamente en tres (3) disposiciones legales a saber,

Ley Estatutaria 1266 de 2008:

La **Ley Estatutaria 1266 de 2008** a través de la cual se dictan las disposiciones generales del Derecho fundamental de Hábeas Data y se regula el manejo de la información personal contenida en bases de datos, en especial la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y por la cual se dictan otras disposiciones relacionados con la materia.

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política de Colombia, así como el derecho a la información establecido en el artículo 20 de la Constitución Política de Colombia, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

Ley Estatutaria 1581 de 2012:

En este contexto, la **Ley Estatutaria 1581 de 2012** emerge como la principal normativa que regula el tratamiento de datos personales en el país. Esta ley establece los principios, derechos y obligaciones que deben regir en la recolección, almacenamiento, uso, circulación y supresión de la información personal. Su objetivo es conciliar el legítimo interés de las organizaciones en utilizar datos personales con la protección de la privacidad de los individuos, y a través de la cual se dictan disposiciones generales para la protección de datos personales.

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. Busca regular el manejo de la información personal y establecer principios y garantías para su tratamiento adecuado.

Algunos de los aspectos principales objeto de la regulación son definir los principios generales que deben regir el tratamiento de datos personales, como el principio de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, establecer las obligaciones de los responsables y encargados del tratamiento de datos personales, reconocer los derechos de los titulares de la información, como el derecho al conocimiento, acceso, actualización, rectificación y supresión de sus datos personales, regular el procedimiento para

el ejercicio de los derechos por parte de los titulares y establecer sanciones por el incumplimiento de las disposiciones de la ley, entre otros aspectos normativos.

Decreto Único Reglamentario 1074 de 2015:

A su vez, el **Decreto Único Reglamentario 1074 de 2015** complementa y reglamenta las disposiciones de la Ley Estatutaria, proporcionando directrices detalladas para su aplicación. Este decreto aborda aspectos prácticos, como el registro de bases de datos, la elaboración de políticas de tratamiento de datos y los procedimientos para atender consultas y reclamos, y por la cual tiene por objeto reglamentar las disposiciones de la Ley Estatutaria 1581 de 2012 y complementarlas con normas específicas que faciliten su aplicación.

Algunos de los aspectos principales objeto de la regulación son detallar las disposiciones relacionadas con el registro de las bases de datos ante la Superintendencia de Industria y Comercio (SIC), establecer pautas para la elaboración y adopción de políticas de tratamiento de datos personales, definir los procedimientos para la atención de consultas y reclamo, y regular la función de la Superintendencia de Industria y Comercio como autoridad de inspección, control y vigilancia en materia de protección de datos personales, entre otros aspectos normativos.

En breve, el fundamento normativo colombiano en materia de protección de datos refleja un equilibrio entre la necesidad de utilizar información personal para diversos fines legítimos y la protección de los derechos fundamentales de los ciudadanos. En este contexto, la Superintendencia de Industria y Comercio (SIC) cumple un papel crucial como entidad encargada de supervisar y garantizar el cumplimiento de estas normativas, asegurando así un adecuado manejo de la información personal en el ámbito público y privado.

En cuanto a la especificidad de los sujetos investigados respecto del domicilio de la sociedad, compañía o persona natural.

En Colombia, según la Sentencia de la Corte Constitucional C-049 de 1997, el domicilio se define como la sede jurídica de la persona o su asiento legal. Es el lugar en el cual la ley supone que siempre está la persona presente para los efectos jurídicos. En efecto, el domicilio es la información pública y oficial del asiento legal de empresa para fines legales y administrativos, el cual puede ser utilizado para notificaciones judiciales, correspondencia oficial y como punto de contacto con las autoridades gubernamentales del territorio.

Conforme a las Resoluciones Sanción, emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de Datos Personales, para el año 2022, que en su conjunto forman el objeto de estudio de la presente investigación, el domicilio de los sujetos investigados, es un criterio a mencionar, en cuanto, la Superintendencia de Industria y Comercio tiene jurisdicción para sancionar a las personas naturales y/o personas jurídicas que operan en el territorio colombiano y que incumplen las normativas relacionadas con la Protección de Datos Personales. Por lo tanto, la ubicación del domicilio de la empresa en

territorio colombiano es crucial, ya que establece la conexión con la jurisdicción de la Superintendencia de Industria y Comercio, así como que puede ser un factor crucial para determinar qué región del país presenta el mayor número de conductas vulneratorias al Régimen de Protección de Datos Personales.

En este orden de ideas, la frecuencia con la que Superintendencia de Industria y Comercio impone sanciones administrativas, multas, entre otras medidas correctivas por infracciones al Régimen de Protección de Datos Personales puede depender de varios factores, y estos a su vez, pueden variar según el contexto y las circunstancias específicas de cada sector, industria o región del país. Algunos de los factores que pueden influir en mayor frecuencia al momento de sancionar a los sujetos como consecuencia de conductas vulneratorias, en algunos sectores con mayor reincidencia en comparación con otros, son los siguientes:

Acerca de la sensibilidad de los datos personales objeto del Tratamiento.

Esta condición depende de que existen ciertos sectores particulares del mercado, que manejan información más sensible que otra de carácter general, como datos médicos o información financiera, entre otros aspectos personales que se reservan en la esfera privada del individuo, que pueden estar más expuestos a riesgos de violaciones de datos, lo que podría resultar en una mayor atención por parte de las autoridades y en la imposición de multas más frecuentes.

Acerca de la cantidad y tipo de datos procesados.

Esta condición depende de que existen con mayor frecuencia, ciertos sectores de la economía del país, que procesan grandes cantidades de datos personales o que utilizan datos para propósitos particulares, como los Servicios Públicos y las Telecomunicaciones, que pueden estar sujetas a un mayor nivel de control, supervisión y vigilancia por parte de las autoridades reguladoras, y a su vez, están más expuestas a ser objeto de investigación y como consecuencia a ser sancionadas por el indebido manejo de datos personales.

Acerca de la cultura del cumplimiento normativo.

La cultura de cumplimiento normativo puede influir en la frecuencia de la imposición de sanciones administrativas, puesto que, sectores que están más conscientes y comprometidos con el cumplimiento de las leyes de protección de datos pueden tener menos infracciones y, por lo tanto, menos multas. De esta manera, si la entidad exhibe una cultura organizacional arraigada en la conciencia y el compromiso con el cumplimiento de las leyes de protección de datos, se establece una sólida barrera contra posibles infracciones. En este contexto, las organizaciones no sólo reconocen la importancia de respetar las normativas vigentes, sino que también adoptan medidas proactivas para asegurar el cumplimiento normativo en todas las facetas de sus operaciones. Esta mentalidad preventiva y centrada en la adhesión a las regulaciones no solo reduce la probabilidad de violaciones de datos, sino que aumenta la confianza del Titular de la Información.

De igual forma, dentro de la cultura del cumplimiento normativo, está inmerso el nivel de conciencia y educación, ya que, sectores que tienen un mayor nivel de conciencia sobre la importancia de la protección de datos personales y que invierten en programas educativos de carácter preventivo para las operaciones empresariales en sus organizaciones pueden tener menos probabilidades de cometer infracciones.

Acerca del historial de incidentes.

Esta condición dispone que hay ciertos sectores, y particularmente, sujetos investigados que con anterioridad han estado involucrados en conductas vulneratorias previas de violación de datos, por lo cual, han sido requeridas previamente para que adopten medidas correctivas en la manera en cómo están realizando el tratamiento de datos personales, por lo tanto, pueden estar bajo un mayor control, supervisión y vigilancia, como resultado, pueden enfrentar sanciones administrativas más frecuentes, como consecuencia de no atender los requerimientos en los términos previstos por la Ley, o por no adecuar su conducta.

Para el caso en concreto, de conformidad con el criterio que atiende al domicilio del sujeto investigado, a continuación, se presentan las siguientes cifras estadísticas, a saber,

Domicilio del Sujeto Investigado.		
Descripción	**Cantidad**	**Porcentaje**
Bogotá, D.C.	36	55,38
Barranquilla, Atlántico.	4	6,15
Ibagué, Tolima.	1	1,54
Sincelejo, Sucre.	1	1,54
Cúcuta, Norte de Santander.	1	1,54
Bucaramanga, Santander.	3	4,62
Medellin, Antioquia.	3	4,62
Manizales, Caldas.	3	4,62
Santiago de Cali, Valle del Cauca.	3	4,62
Soledad, Atlántico.	1	1,54
Pasto, Nariño.	1	1,54
Cucunubá, Cundinamarca.	1	1,54
Cota, Cundinamarca.	1	1,54
Pereira, Risaralda.	1	1,54
Neiva, Huila.	1	1,54
Soacha, Cundinamarca.	1	1,54
Girardot, Cundinamarca.	1	1,54
Chia, Cundinamarca.	2	3,08
Total	65	100,00

Tabla No. 1 Para el Domicilio del Sujeto Investigado.

Gráfico No. 1 Para el Domicilio del Sujeto Investigado.

A partir de los datos estadísticos presentados con respecto al domicilio del sujeto investigado, se evidencia, que la mayor cantidad de las Resoluciones emitidas por la Superintendencia de Industria y Comercio, los sujetos investigados, ya sean personas naturales y/o personas jurídicas, en el rol de Responsable y/o Encargado del Tratamiento, tienen su domicilio en la ciudad de Bogotá D.C, que tienden a su vez, a ser las más sancionadas, toda vez que de acuerdo con las cifras estadísticas mostradas con anterioridad, de un total de sesenta y cinco (65) Resoluciones objeto de estudio para la presente investigación, con un total de treinta y seis (36) son las sociedades sancionadas ubicadas en la capital del país. De lo cual, se puede afirmar que, al ser Bogotá D.C al ser el centro económico y empresarial del país, tiene un mayor volumen de datos personales para procesar en comparación con otras regiones del territorio, y a su vez, con una relación directa, el manejo de grandes cantidades de información personal aumenta la probabilidad de errores o incumplimiento en el tratamiento de datos. Por otro lado, la restante cantidad considerable de sujetos sancionados se encuentran en otras regiones del país, que son, veintinueve (29) actos administrativos, se distribuyen a lo largo y ancho del país, en puntos estratégicos, como lo son, Barranquilla, Atlántico; Medellín, Antioquia; Santiago de Cali, Valle del Cauca, entre otras.

En cuanto a los derechos de los titulares de la información.

Para mencionar cuáles son los derechos de los titulares de la información se debe conocer previamente qué se entiende por titular de la información y para ello, es importante indicar la definición de la Superintendencia de Industria y Comercio,

"Aquella persona a quien se refiere la información que reposa en un banco de datos, razón por la cual, es quien puede ejercer el derecho de hábeas data". (Aspectos básicos sobre el derecho de Hábeas Data, Superintendencia de Industria y Comercio).

Esto quiere decir que cada uno de los individuos, que a su vez, en el Tratamiento de Datos, son titulares de la información, tienen la facultad de proteger su privacidad, e intimidad y tomar control sobre la información personal que se encuentra almacenada en diversas bases de datos.

Una vez abordada la definición de titular de la información, se proceder a explicar en qué consiste los Derechos de los titulares de la información, de conformidad con los dispuesto en el Artículo 8 de la Ley 1581 de 2012, que de manera literal estipula lo siguiente, a saber,

El Titular de los datos personales tendrá los siguientes derechos:

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

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el Artículo 10 de la presente ley;

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

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

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Para el caso en concreto, de conformidad con el Artículo 8 de la Ley 1581 de 2012 y acorde al objeto de estudio de la presente investigación, a continuación se detalla de manera breve y sencilla cada uno de los derechos que le asisten al titular de la información objeto del Tratamiento de Datos Personales,

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

La disposición se refiere al derecho con que cuentan los titulares de la información sobre sus datos personales en el contexto del tratamiento de datos llevado a cabo por el Responsable y/o Encargado del Tratamiento. Este derecho permite al titular de la información tomar el

control sobre la exactitud de los datos, en cuanto, el individuo puede conocer, actualizar y corregir la información que se tiene de ellos. Este derecho puede ejercerse en situaciones donde los datos sean parciales, inexactos, incompletos, fraccionados o puedan inducir a error. Además, abarca aquellos casos en los que el tratamiento de los datos esté expresamente prohibido o no haya sido autorizado previamente por la persona titular de los datos.

Por ejemplo, si un individuo encuentra que la información sobre su dirección de residencia o número de teléfono que reposa en una base de datos es inexacta o está desactualizada, tiene el derecho de solicitar la corrección de esos datos. De igual manera, si la información está fraccionada, incompleta o puede inducir a error, el titular de los datos tiene el derecho de rectificar aquella información. Este derecho busca garantizar que la información personal sea precisa y refleje fielmente la realidad, proporcionando a las personas un mayor control sobre sus datos personales.

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;

Este segundo literal del artículo se refiere al derecho con que cuenta el titular de la información para solicitar prueba de la autorización que ha otorgado al Responsable del Tratamiento de datos, lo cual prueba que cuenta con la autorización necesaria para llevar a cabo el tratamiento de la información personal del solicitante.

Por ejemplo, si una empresa recopila y procesa datos personales de sus clientes, cualquiera de los individuos involucrados en esta operación, puede ejercer este derecho, por medio de una petición, donde solicita la respectiva prueba que respalda la autorización legal con que cuenta la empresa para realizar dicho tratamiento. Esto puede incluir documentos, acuerdos de consentimiento u otros registros que demuestren que la entidad cuenta con el permiso adecuado para gestionar los datos personales de los usuarios. Este principio busca garantizar que el tratamiento de datos personales se realice de manera legal y transparente, proporcionando a los individuos la confianza de que sus datos se manejan de acuerdo con las normas de privacidad y protección de datos.

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

Esta disposición normativa se refiere al derecho con que cuenta el titular de la información, a ser informado, previa solicitud, por parte del Responsable del Tratamiento o el Encargado del Tratamiento, acerca del uso que se ha dado a sus datos personales. Por ejemplo, si una empresa es la Responsable del tratamiento de datos personales de sus clientes, cualquiera de los titulares de la información, involucrados en la operación, puede solicitar detalles sobre cómo se están siendo utilizados sus datos personales. Este derecho busca proporcionar transparencia y permitir que los individuos conozcan claramente cómo se maneja y utiliza su información personal, permitiéndoles tomar decisiones informadas sobre la privacidad y protección de su información.

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

La disposición normativa se refiere al derecho con que cuentan los titulares de la información para presentar quejas ante la Superintendencia de Industria y Comercio en caso de que se hayan cometido infracciones a lo establecido en la ley de protección de datos personales y otras normas relacionadas.

Por ejemplo, si una entidad, ya sea, Responsable y/o Encargada del Tratamiento de Datos, no cumple con las prerrogativas establecidas en la ley de protección de datos, ya sea, en cuanto a la privacidad, la falta de autorización expresa por parte del titular para el tratamiento de datos o la divulgación no autorizada de información personal, un individuo puede elevar una queja ante la Superintendencia de Industria y Comercio, por la presunta infracción.

Este derecho brinda a las personas la posibilidad de intervenir y presentar acciones en situaciones en las que se consideren que los derechos en cuanto a la privacidad y protección de la información personales han sido vulnerados, contribuyendo así a la supervisión y cumplimiento de las leyes de protección de datos.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

Este literal establece el derecho de una persona a revocar la autorización que ha otorgado para el tratamiento de sus datos personales y solicitar la supresión de dicha información en casos en los que se evidencie un incumplimiento de los principios, derechos y garantías constitucionales y legales relacionados con la protección de datos. Para que proceda la revocación o supresión, la Superintendencia de Industria y Comercio debe previamente determinar que el Responsable o Encargado del tratamiento ha incurrido en conductas contrarias a la ley de protección de datos personales y a la Constitución Política de Colombia.

En otras palabras, este numeral otorga a las personas la facultad de retirar su consentimiento y eliminar sus datos personales cuando se hayan violado las normativas y principios establecidos para la adecuada protección de la privacidad. La intervención de la Superintendencia garantiza una evaluación imparcial y legal de las conductas inadecuadas en el tratamiento de datos, que refuerza la protección de privacidad y permite a los individuos tomar medidas contra el uso indebido de sus datos personales.

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Este literal se refiere al derecho del titular de la información para acceder de forma gratuita a la información personal que ha sido objeto de tratamiento por parte de una entidad Responsable y/o Encargada del Tratamiento.

Por ejemplo, si una empresa ha recopilado y procesado datos personales de un cliente, este último tiene el derecho de solicitar y recibir de manera gratuita detalles sobre la información que la empresa tiene almacenada sobre él. Este derecho promueve la transparencia y la capacidad del individuo para conocer y verificar qué información poseen las entidades sobre ellos, permitiéndoles tomar decisiones informadas sobre su privacidad.

A modo de detalle, y de conformidad con el análisis investigativo del presente estudio de las Resoluciones emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de datos personales, para el año 2022, los literales del Artículo 8 de la Ley 1581 de 2012, que con frecuencia, los titulares de la información utilizan para hacer valer sus derechos, son los siguientes,

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

Dentro del marco de la investigación, se evidencia la aplicación del primer literal del Artículo de la Ley 1581 de 2012, en cuanto los titulares de la información, en el ejercicio del Derecho Fundamental de Hábeas Data y otros derechos conexos, tienen el derecho de Conocer, actualizar y rectificar sus datos personales, sujetos al Tratamiento de Datos, por tanto, un porcentaje de las investigaciones realizadas por la Superintendencia de Industria y Comercio, se enmarcaron en las quejas presentadas por los titulares de la información que consideraron que sus derechos estaban siendo vulnerados por conductas desplegadas por el Responsable del Tratamiento o Encargado del Tratamiento, respectivamente, y en su mayoría en casos donde el Tratamiento de Datos no ha sido autorizado, o en circunstancias en que está expresamente prohibido, como lo es, respecto de los datos sensibles.

De manera detallada, se presenta una muestra del total de resoluciones objeto de estudio que respaldan la justificación del Literal A del Artículo 8 de la Ley 1581 de 2012,

Por un lado, la Resolución 73807 de 2022, en donde, el Sindicato de Trabajadores del Hospital San Juan de Dios, en su calidad de Responsable del Tratamiento, realizó el tratamiento de los datos personales sensibles del titular sin contar con su autorización previa, expresa e informada, de igual forma, en este caso no resulta aplicable la excepción legal contenida en el Literal C del Artículo 6 de la Ley 1581 de 2012, puesto que la misma aplica exclusivamente respecto de los miembros del sindicato o respecto de las personas que mantengan contactos regulares por razón de su finalidad, lo cual no era el caso.

Por un lado, la Resolución 51177 de 2022, en donde, la Clínica de la Visión del Valle S.A.S, en su calidad de Responsable del Tratamiento, envió a la dirección electrónica del Titular los datos sensibles relativos a la historia clínica de once (11) Titulares, sin ser un tercero autorizado.

Por un lado, la Resolución 86797 de 2022, en donde, la sociedad Master Travel Sale S.A.S, en su calidad de Responsable incumplió con el deber de solicitar la autorización previa,

expresa e informada del titular para realizar el tratamiento de sus datos personales mediante llamadas telefónicas para el ofrecimiento de servicios comerciales.

Por un lado, la Resolución 85259 de 2022, en donde, la sociedad Gourmet & Vacation People S.A.S, en su calidad de Responsable no cuenta con la autorización previa para el tratamiento de los datos personales otorgada por la Titular para el envío de ofertas comerciales vía Whatsapp.

Por un lado, la Resolución 55739 de 2022, en donde la Caja Colombiana de Subsidio Familiar Colsubsidio, en su calidad de Responsable, trató el número de celular del titular sin contar con su autorización para ello, ya que la autorización obtenida fue suministrada por un tercero, por lo que incumplió el deber de solicitar la autorización previa, expresa e informada del titular.

Por un lado, la Resolución 40839 de 2022, en donde la Universidad Católica de Colombia, en su calidad de Responsable, realizó el envío de un correo electrónico de carácter publicitario a la dirección electrónica institucional del denunciante, el cual es un dato semiprivado, sin contar con su autorización previa, expresa e informada para el tratamiento de sus datos personales.

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;

Principalmente, la aplicación de este literal del Artículo 8 de la Ley 1581 de 2012, se presenta, en cuanto, los titulares de la información, están facultados para solicitar prueba de la autorización otorgada al Responsable del Tratamiento, de conformidad con el análisis investigativo del presente estudio, se evidencian los siguientes casos que respaldan la forma en cómo los usuarios dieron aplicación a esta prerrogativa, a saber,

Por un lado, la Resolución 85241 de 2022, en donde la sociedad Colombia Móvil S.A E.S.P, como Responsable del tratamiento de datos, incumplió el deber de solicitar y conservar la copia de la autorización previa para el tratamiento de la información personal del titular.

Por un lado, la Resolución 73813 de 2022, en donde la sociedad Hotel Termales El Otoño S.C.A, en su calidad de Responsable, incumplió con el deber de solicitar y conservar copia de la autorización de los titulares, respecto de la información recaudada a través de la página Web.

Por un lado, la Resolución 72784 de 2022, en donde la sociedad Dicomercial de Inversiones y CIA S.C.A, en su calidad de Responsable, incumplió con el deber de solicitar y conservar copia de la autorización de los titulares, en las condiciones prevista en la Ley 1581 de 2012.

Por un lado, la Resolución 60419 de 2022, en donde la sociedad Integral Business Center S.A.S, en su calidad de Responsable, incumplió con el deber de solicitar y conservar la autorización previa, expresa e informada del titular de la información.

Por un lado, la Resolución 51179 de 2022, en donde la sociedad Efrata International S.A.S, en su calidad de Responsable, incumplió con el deber de solicitar y conservar la autorización previa, expresa e informada del titular de la información.

Por un lado, la Resolución 50206 de 2022, en donde la sociedad TSQ S.A.S, en su calidad de Responsable, incumplió con el deber de solicitar y conservar la autorización previa, expresa e informada del titular de la información.

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

El Literal D del Artículo 8 de la Ley 1581 de 2012, faculta a los individuos para presentar ante la autoridad competente, particularmente, la Superintendencia de Industria y Comercio, quejas cuando se evidencie una posible vulneración a las infracciones a las prerrogativas dispuestas en el Régimen de Protección de Datos Personales y las demás normas que lo modifiquen, adicionen o complementen.

En este sentido, de conformidad con los parámetros establecidos como objeto de estudio para la presente investigación, uno de los criterios relevantes es considerar si la investigación al Responsable y/o Encargado del Tratamiento se presentó de oficio por parte del órgano competente o a petición de partes.

De manera detallada, la presentación de los siguientes datos estadísticos, obtenidos como resultado de lo investigado, permiten concluir el número total de veces que se iniciaron los procesos administrativos por parte de la Superintendencia de Industria y Comercio, como consecuencia de una queja presentada a petición de parte o de oficio.

Inicio del Proceso de Investigación.	
Descripción	**Cantidad**
De oficio por parte de la entidad.	29
A petición de parte.	36
Total	65

Tabla No. 2 Para el Inicio de la Investigación.

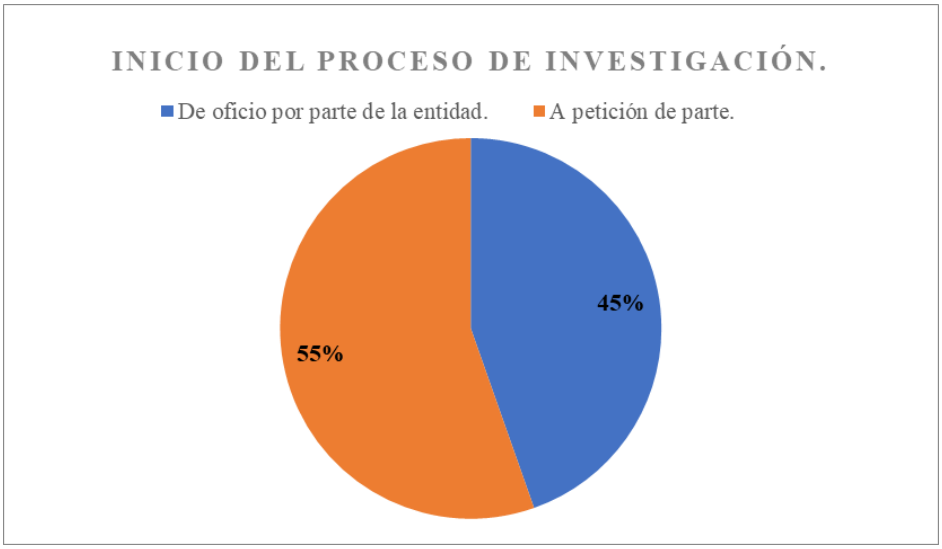


Gráfico No. 2 Para el Inicio de la Investigación.

De las anteriores gráficas estadísticas presentadas, se pueden afirmar las siguientes conclusiones, de modo que, de la cantidad total de Resoluciones emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de datos personales, para el año 2022, que son objeto de estudio de la presente investigación, se observa que un número total de veintinueve (29) fueron iniciadas de oficio por parte de la Superintendencia de Industria y Comercio para la apertura de una investigación por infracciones a las normas sobre protección de datos personales, mientras que, un número total, de treinta y seis (36) fueron iniciadas a petición de parte, lo cual representa en términos porcentuales el cincuenta y cinco por ciento (55%) del total, lo que es más de la mitad.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

El Literal E del Artículo 8 de la Ley 1581 de 2022, establece que la intervención de la autoridad regulatoria es necesaria para confirmar que ha habido un incumplimiento grave de las normativas de protección de datos, y bajo el supuesto de que se demuestre que el Responsable o Encargado ha incurridos en un conducta vulneratoria al Régimen de Protección de Datos Personales, procede la revocatoria y/ supresión de los datos personales.

Particularmente, ante una conducta que esté en contravención de las disposiciones normativas de la Protección de Datos Personales en Colombia, sobre la cual se adelanta una investigación por parte de la Superintendencia de Industria y Comercio, es común observar que el Titular de la Información, quién se ha visto afectado, solicite la revocatoria de la autorización previamente otorgada al Responsable y/o Encargado del Tratamiento, así como, ordenar que se suprima y eliminen los datos personales que recaen sobre él, y que estaban siendo tratados por la entidad; esto tiene fundamento en que, ante un incumplimiento grave,

los derechos del titular se están viendo vulnerados y lo que se busca es buscan garantizar la privacidad y seguridad de los datos de los individuos, y ante este supuesto, requieren una sanción por parte de la autoridad competente.

De manera detallada, este es un ejemplo de las sanciones emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de datos personales, que se enmarcan en el Literal E del Artículo 8 de la Ley 1581 de 2012,

Por un lado, la Resolución 85241 de 2022, en donde la sociedad Colombia Móvil S.A E.S.P, en su calidad de Responsable del Tratamiento, faltó al deber de garantizar a la Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, al no acceder a su pretensión de suprimir sus datos personales con el fin de no recibir mensajes de texto y correos electrónicos.

En cuanto a la especificidad de los sujetos investigados respecto de la actividad empresarial que ejecuta en el territorio colombiano.

A través del Derecho de Petición con Radicado No. 23-474320-2 enviado por los autores del presente Proyecto de Grado, a la Superintendencia de Industria y Comercio, con fines informativos relacionados con el objeto del estudio de investigación, el director de investigación de Protección de Datos Personales en Colombia, el señor Carlos Enrique Salazar Muñoz, permite indicar que,

Para el año 2022, la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio, entre el 01 de enero de 2022 y el 31 de diciembre de 2023, expidió un total de 124 sanciones, por vulneración a la *"Ley de Hábeas Data Financiero"* y setenta (70) por vulneración a la Ley 1581 de 2012 *"Régimen General de Protección de Datos Personales"*.

A la fecha, las conductas más sancionadas por la Superintendencia de Industria y Comercio son: Las fallas en la seguridad de la información, la falta de autorización previa, expresa e informada por parte del titular para el tratamiento de los datos personales, no informar la finalidad para la cual hacen la recolección de la información personal, no atender las consultas y reclamaciones de los ciudadanos y no atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio.

Por otro lado, hay ciertas actividades empresariales de los Responsables y/o Encargados del Tratamiento, sobre las cuál se emiten más sanciones por parte de la Superintendencia de Industria y Comercio, algunas de ellas son, Telecomunicaciones, Comercio Electrónico, Turismo, y Portales de Comercio Electrónico, que en su mayoría se encargan de la gestión y atención de usuarios y/o clientes.

En cuanto a los principios del Régimen de Protección de Datos Personales que están comprometidos en la vulneración.

El Artículo 4 de la Ley 1581 de 2012 establece los principios que rigen el Tratamiento de Datos Personales en Colombia, que reflejan el eje central de la protección de los datos personales, entre ellos, abarcan temas fundamentales en el Tratamiento, como, la autorización previa, expresa e informada del consentimiento del Titular, las finalidades y los medios para la captación y tratamiento de los datos personales, la privacidad, la seguridad de la información, la protección especial de los datos sensibles, y el ejercicio del derecho fundamental de Hábeas Data, respecto al acceso, rectificación, cancelación, oposición y portabilidad en cabeza del titular.

De igual forma, los principios que rigen el Régimen de Protección de Datos Personales sobre la privacidad y la protección de datos personales, son un instrumento que la Superintendencia de Industria y Comercio adopta como punto de referencia para el fortalecimiento del cumplimiento del marco jurídico, la protección armónica y efectiva de los datos personales, en cuanto ejerce la función de control y vigilancia de las conductas desplegadas por los Responsables y/o Encargado del Tratamiento para evitar infracciones que se enmarquen en el indebido manejo de datos personales, y sancionar aquellas que violan las disposiciones legales.

Acerca del Principio de legalidad en materia de Tratamiento de datos.

El Artículo 4 de la Ley 1581 de 2012, consagra la siguiente disposición en cuanto al principio de legalidad en materia de Tratamiento de datos.

El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

Según la Corte Constitucional de Colombia, en Sentencia C-748 de 2011, el principio de Legalidad en Materia de Tratamiento de Datos, "*Encierra el principal objetivo de la regulación estatutaria: someter el tratamiento de datos a lo establecido en las normas, fijar límites frente a los responsables y encargados del tratamiento y garantizar los derechos de los titulares de los mismos".* (Corte Constitucional, Sala Plena, C-748,2011).

Teniendo en cuenta el pronunciamiento jurisprudencial, se puede detallar que es crucial adecuar las prácticas de manejo de información a las normas vigentes, establecer límites precisos en el actuar de los sujetos Responsables y/o Encargados del tratamiento, y asegurar de manera efectiva los derechos inherentes a los titulares de los datos. Además de garantizar una gestión ética, transparente y legal de la información personal, contribuyendo así a proteger la privacidad y los intereses de los individuos en el contexto del entorno digital actual.

Este principio asegura que todas las acciones relacionadas con la recopilación, almacenamiento, la disposición y transmisión de datos personales, deben de adecuarse y ajustarse conforme a las regulaciones en materia de protección y seguridad de la información

vigentes. En el contexto de la protección de datos personales en Colombia, el principio de legalidad actúa como un marco normativo que garantiza que los procesos de tratamiento de datos cumplan con las leyes de privacidad y protección de la información resguardando así los derecho y la privacidad de los individuos.

Acerca del Principio de finalidad.

El Artículo 4 de la Ley 1581 de 2012, consagra la siguiente disposición en cuanto al principio de finalidad en materia de Tratamiento de datos.

El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

De acuerdo con este principio la recopilación y el uso de datos personales debe atender a propósitos específicos y legales, evitando el procesamiento indiscriminado o no autorizado de la información. En esencia, busca garantizar la transparencia y la protección de los derechos de los titulares de datos al asegurar que la información recopilada sea utilizada únicamente para los fines informados y consentidos.

La aplicación efectiva del principio de finalidad contribuye a fortalecer la confianza de los ciudadanos en los procesos de manejo de datos, promoviendo así una cultura de respeto y seguridad en el ámbito de la privacidad, seguridad y protección de la información.

De ahí que, los datos personales deben de ser recopilados únicamente para finalidades legítimas y a través de medios leales y legítimos, dado que la recopilación de datos personales implica la recolección de información personal que puede tener un impacto directo a la privacidad y la autonomía de los individuos. Por lo tanto, la Organización de Estados Americanos (OEA) en la publicación Principios actualizados sobre la privacidad y la protección de datos personales, a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos, destaca la importancia de que la recopilación de la información personal se ajuste a parámetros éticos y legales, toda vez que recopilar datos únicamente para finalidades legítimas significa que la información personal solo debe ser recabada con propósitos que sean legales y que respeten tanto los derechos y libertades de los individuos. Esta restricción busca evitar el uso indebido de la información recopilada, como el riesgo de vigilancia injustificada o discriminación.

Acerca del Principio de libertad.

El Artículo 4 de la Ley 1581 de 2012, consagra la siguiente disposición en cuanto al principio de libertad en materia de Tratamiento de datos.

El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

La relación entre el principio de libertad y la protección de datos personales radica en la salvaguarda de la privacidad individual, garantizando que la obtención, divulgación y procesamiento de los datos personales sólo ocurran con la autorización previa, expresa e informada del titular que otorga su consentimiento para el tratamiento de su información personal.

La Corte Constitucional de Colombia, en la Sentencia T-022 de 1993, ha relacionado el principio de libertad, con la prohibición del manejo de la información adquirida de manera ilícita, por está razón entiende la misma que: "*Se encuentra prohibida la obtención y divulgación de los mismos, sin la previa autorización del titular o en ausencia de mandato legal o judicial."*(Corte Constitucional, Sala Primera de Revisión, T-022,1993).

La prohibición expresa de obtener y divulgar información sin la autorización previa del titular, a menos que exista un mandato legal o judicial, subraya la importancia de respetar la autonomía y privacidad de los individuos en el tratamiento de sus datos personales. Esta restricción destaca la necesidad de obtener el consentimiento informado y consciente antes de recopilar o compartir información personal, reforzando así la protección de los derechos fundamentales de los titulares para salvaguardar la integridad y la seguridad de los datos personales, promoviendo un tratamiento que se ajuste a parámetros éticos y legales de la información en concordancia con los principios de la protección de datos.

Acerca del Principio de veracidad o calidad.

El Artículo 4 de la Ley 1581 de 2012, consagra la siguiente disposición en cuanto al principio de veracidad o calidad en materia de Tratamiento de datos.

La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

Según la Corte Constitucional de Colombia, en Sentencia C-748 de 2011, el principio de veracidad corresponde a *"Datos personales que obedezcan a situaciones reales y ciertas, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos."* (Corte Constitucional, Sala Plena, C-748,2011). Lo que refleja la importancia de mantener la integridad y exactitud de la información personal, contribuyendo a la protección de los derechos fundamentales de los individuos y asegurando prácticas de tratamiento de datos que sean éticas, confiables y acordes con los estándares constitucionales.

Este principio tiene conexión directa con la integridad de los datos y busca asegurar que la información utilizada sea fidedigna y refleje con precisión la realidad. Al promover la veracidad y calidad de los datos, se fortalece la confianza en los sistemas de manejo de información y se evita la toma de decisiones basadas en datos imprecisos o desactualizados. Además, este principio se relaciona estrechamente con la protección de la privacidad al prevenir el tratamiento de datos parciales, incompletos o que puedan inducir a error, contribuyendo así a garantizar el respeto a los derechos de los titulares de la información en el contexto de la regulación de datos personales en Colombia.

Acerca del Principio de transparencia.

El Artículo 4 de la Ley 1581 de 2012, consagra la siguiente disposición en cuanto al principio de transparencia en materia de Tratamiento de datos.

En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

El principio de transparencia refleja la importancia de informar a las personas sobre las prácticas y políticas que utilizan las entidades Responsables y/o Encargadas que recopilan los Datos Personales, con el fin de que los titulares de la información puedan tomar una decisión fundamentada respecto al suministro de los datos personales. Si no existe claridad en cuanto a la finalidad del tratamiento, el consentimiento de la persona para el tratamiento de sus datos no puede ser válido, porque la información que sea proporcionada al Titular debe ser en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, que permita su entendimiento.

Este principio se fundamenta en la necesidad de proporcionar claridad y accesibilidad a los individuos sobre cómo se recopilan, disponen y gestionan sus datos personales. Al fomentar la transparencia y el acceso a la información en las distintas instancias del tratamiento, se fortalece la confianza de los titulares en las entidades que procesan sus datos e información personal, permitiéndoles tomar decisiones informadas sobre la forma en cómo se maneja el tratamiento de su información procurando salvaguardar la claridad de la gestión de la información personal y el respeto a la privacidad individual en el contexto legal colombiano.

De acuerdo con el pronunciamiento de la Organización de Estados Americanos (OEA) el principio de transparencia involucra que siempre,

"Antes o al momento de recopilarse los Datos Personales, deberían especificarse claramente: i) la identidad y datos de contacto del Responsable; ii) las finalidades del Tratamiento; iii) el fundamento jurídico de su Tratamiento; iv) los destinatarios o categorías de destinatarios a los cuales los Datos Personales serán comunicados; v) la información a serles transmitida, y vi) la existencia, forma y mecanismos o procedimientos a través de los cuales los Titulares de Datos Personales podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad". (Principios actualizados sobre la privacidad y la protección de datos personales, Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos).

Acerca del Principio de acceso y circulación restringida.

El Artículo 4 de la Ley 1581 de 2012, consagra la siguiente disposición en cuanto al principio de acceso y circulación restringida en materia de Tratamiento de datos.

El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

Este principio destaca la importancia de restringir el acceso a los datos personales a personas autorizadas por el titular y aquellas permitidas por la ley. Además, establece que, salvo la información pública, los datos personales no deben estar disponibles en internet u otros medios de divulgación masiva, a menos que se pueda controlar técnicamente el acceso para limitarlo a los titulares o terceros autorizados.

El principio de acceso y circulación restringida se relaciona directamente con la protección de la privacidad al establecer salvaguardas para evitar la divulgación no autorizada de información personal, contribuyendo así a preservar la confidencialidad y seguridad de los datos en el entorno digital colombiano.

Según la Corte Constitucional de Colombia, en Sentencia C-748 de 2011, el principio de acceso y circulación restringida: *"Sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Además, se prohíbe que los datos personales, salvo información pública, se encuentren disponibles en Internet, a menos que se ofrezca un control técnico para asegurar el conocimiento restringido."*(Corte Constitucional, Sala Plena, C-748,2011).

La cita jurisprudencial respalda el pronunciamiento normativo en cuanto lo que se busca con el principio de acceso y circulación restringida a es el compromiso con la protección de la privacidad y la gestión responsable de los datos personales, asegurando que el acceso a la información esté sujeto a controles que respeten los derechos individuales y prevengan posibles usos indebidos o violaciones de la seguridad de la información.

Acerca del Principio de seguridad.

El Artículo 4 de la Ley 1581 de 2012, consagra la siguiente disposición en cuanto al principio de seguridad en materia de Tratamiento de datos.

La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

Este principio se relaciona directamente con la integridad y confidencialidad de los datos, siendo esencial para resguardar la privacidad de los individuos. En un contexto digital en

constante evolución, la implementación efectiva de medidas de seguridad contribuye a mitigar riesgos y proteger la información personal de posibles amenazas cibernéticas, asegurando así el cumplimiento de las normas de protección de datos en Colombia y fortaleciendo la confianza en el tratamiento adecuado de la información personal.

Según la Corte Constitucional de Colombia, en Sentencia C-748 de 2011, el principio de seguridad respecto a la protección de datos personales.

"*Debe adoptar medidas necesarias para proteger los ficheros contra riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático."* (Corte Constitucional, Sala Plena, C-748,2011).

Se puede afirmar que la implementación de medidas de seguridad es esencial para mitigar riesgos y garantizar la integridad, confidencialidad y disponibilidad de la información, contribuyendo así a una gestión responsable y segura de los datos en el ámbito digital.

Acerca del principio de confidencialidad.

El Artículo 4 de la Ley 1581 de 2012, consagra la siguiente disposición en cuanto al principio de confidencialidad en materia de Tratamiento de datos.

Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma;

Este principio se fundamenta en la necesidad de conservar bajo medidas de seguridad la privacidad de los individuos y se relaciona directamente con la seguridad y privacidad en el manejo de la información personal. Asegurar la confidencialidad contribuye a evitar la divulgación no autorizada de datos y a proteger la integridad de la información, elementos esenciales para el cumplimiento de las normas de protección de datos en Colombia y para el respeto de los derechos fundamentales de los titulares de la información.

Por ello, la Organización de los Estados Americanos (OEA) se ha pronunciado al respecto del principio de confidencialidad afirmando que: "*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."* (Principios actualizados sobre la privacidad y la protección de datos personales, Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos).

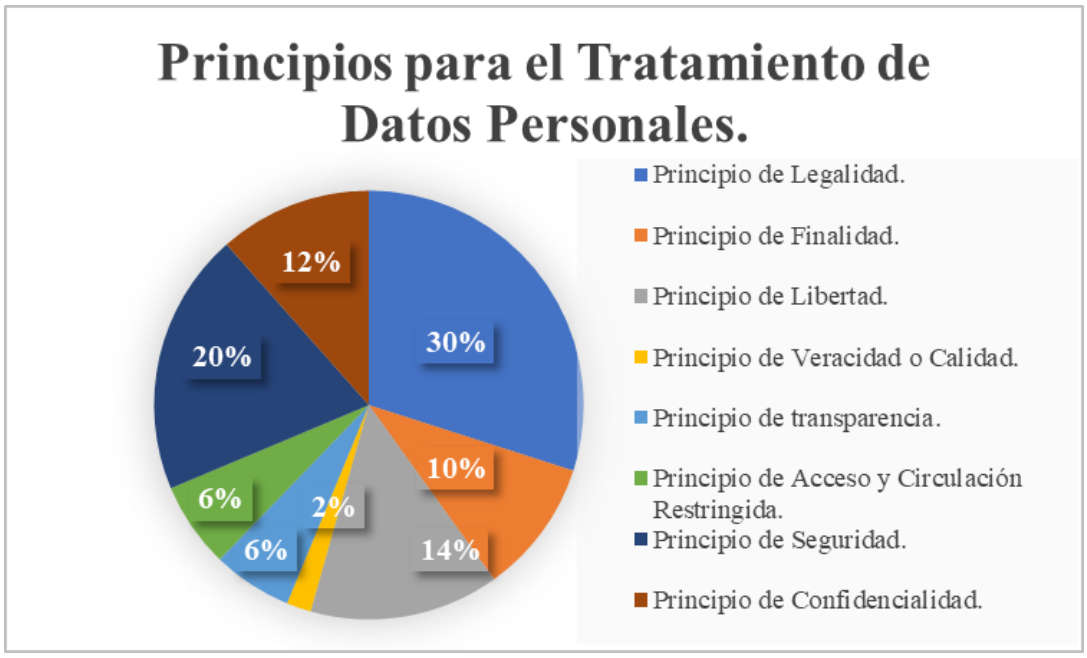
La restricción de divulgación y uso de datos personales limitándose a las finalidades para las cuales fueron recopilados, refuerza la importancia de respetar la privacidad y la voluntad de

los individuos. El pronunciamiento anterior, resalta que sin el consentimiento de la persona afectada o en cumplimiento de la ley, los datos personales no deben ser divulgados ni puestos a disposición de terceros para fines diferentes a los originalmente establecidos. Aquí se refleja el compromiso con el control y la protección de la información personal, asegurando que su utilización se realice de manera ética, legal y conforme a los derechos de cada uno de los titulares.

Por otro lado, es relevante para el presente estudio de investigación, identificar la cantidad de veces que la Superintendencia de Industria y Comercio evidenció alguna conducta por parte de los sujetos investigados, Responsable y/o Encargado del Tratamiento, que fuera en contra de los principios para el Tratamiento de Datos, por ello, se presentan los siguientes gráficos que reflejan los resultados obtenidos.

Principios para el Tratamiento de Datos Personales.	
Descripción	**Cantidad**
Principio de Legalidad.	65
Principio de Finalidad.	22
Principio de Libertad.	31
Principio de Veracidad o Calidad.	4
Principio de transparencia.	13
Principio de Acceso y Circulación Restringida.	14
Principio de Seguridad.	43
Principio de Confidencialidad.	25

Tabla No. 3 Para los Principios comprometidos en el indebido manejo de datos personales.



Gráfica No. 3 Para los Principios comprometidos en el indebido manejo de datos personales.

De los resultados obtenidos en relación a los principios para el Tratamiento de Datos Personales, se puede afirmar que la totalidad de actos administrativos emitidos por la Superintendencia de Industria y Comercio, por indebido manejo de datos personales, involucran el principio de legalidad, toda vez que, los hechos constitutivo de las infracciones al Régimen General de Protección de Datos Personales no son actividades regladas que se ajusten a las disposiciones normativas, en esta misma línea, se evidencia el número total de veces que cada uno de los principios del Artículo 4 de la Ley 1581 de 2012 estuvo comprometido en la vulneración, así las cosas, se observa que sin distinción alguna, en un solo acto administrativo se pueden aplicar varios de los literales consagrados en el Artículo 4 de la Ley 1581 de 2012, en cuanto los hechos constitutivos de la infracción pueden involucrar un número plural de principios afectados.

A continuación, se presenta el Capítulo Dos (2) de la Tesis de Grado respecto al Indebido Manejo de Datos Personales con un enfoque en el análisis cuantitativo, cualitativo y teórico de los resultados obtenidos de las Fichas de Investigación de las Resoluciones-Sanción, por medio de gráficos estadísticos que permitan la comparación entre la teoría y los hallazgos de investigación en cuanto a los parámetros para establecer la cuantía.

Las cifras y datos recogidos se presentan al lector a partir del siguiente análisis:

En cuanto al total del número de Resoluciones Sanción emitidas por la Superintendencia de Industria y Comercio para el año 2022.

En primer lugar, la Superintendencia de Industria y Comercio, autoridad competente para la función de inspección, vigilancia y control del Derecho Fundamental de Habeas Data amparado en la Ley 1266 de 2008, y la protección de Datos Personales consagrada en la Ley 1581 de 2012, a través de la Dirección de Investigación de Protección de Datos Personales, ejercerá la vigilancia de los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países de la misma naturaleza, en cuanto se refiere a la actividad de administración de datos personales de los titulares de la información. Además, podrá ordenar la corrección, actualización o retiro de datos personales de una base de datos, cuando así se determine dentro de la investigación y, administrará el Registro Nacional Público de Bases de Datos. Específicamente, para el año 2022, la Superintendencia emitió setenta (70) Resoluciones por el Indebido Manejo de Datos Personales, aunque el presente análisis se limita a la información de carácter pública que brinda la entidad, por tanto, la investigación se centra en sesenta y cinco (65) Resoluciones de carácter público que suministra la entidad, a través de su Página Web y por medio de la presentación de un derecho de petición.

Del conjunto de Resoluciones, se evidencia que, respecto al estado de la resolución y los recursos que el investigado puede presentar según la ley, la mayoría de las resoluciones, con un total de cincuenta y cinco (55) de ellas, se encuentran en firme, aunque solamente once (11) de los actos administrativos estuvo sujeto a recursos confirmando la decisión adoptada por la Superintendencia de Industria y Comercio, mientras que solo una fue modificada en su parte resolutiva; por otro lado, se observa que, un total de diez (10) resoluciones, están en trámite administrativo por parte de la autoridad, la clasificación atiende a un criterio diferenciador de la información disponible para la investigación, puesto que, se encuentra que para un grupo de las resoluciones no hay información pública del acto administrativo que resuelve el recurso, puesto que no se cuenta con acceso, aunque este haya sido concedido.

Estado de la Resolución.	
Descripción	**Cantidad**
En firme (No se presentaron recursos).	43
En firme (Se presentaron los Recursos de Reposición y Apelación).	11
En trámite (Se presentó el Recurso de Reposición, sin información del Recurso de Apelación).	6
En trámite (Sin evidencia de los actos administrativos de los recursos).	2
Modificada (Se presentaron los Recursos de Reposición y Apelación).	1
Modificada (Se presentó el Recurso de Reposición, sin información del Recurso de Apelación).	2
Total	65

Tabla No. 4 Para el Estado de las Resoluciones Sanción.

En cuanto a la formulación de cargos para las Personas Jurídicas y Personas Naturales investigadas por Indebido Manejo de Datos Personales.

En el Acto administrativo se adelanta el procedimiento sancionatorio con el fin de establecer las posibles violaciones a las normas, a las órdenes y/o instrucciones que están bajo inspección, control y vigilancia de la Superintendencia de Industria y Comercio. En esta parte, se detalla con precisión y claridad los hechos o conductas violatorias que originan la investigación por Indebido Manejo de Datos Personales, las personas naturales o jurídicas objeto de la investigación, las disposiciones presuntamente vulneradas y las sanciones o medidas que serían procedentes, para el caso en particular, se evidencian los siguientes hallazgos en el marco de la investigación;

Conforme al número de cargos imputados en los actos administrativos a cada uno de los sancionados, se observa de manera estadística, que para la mayor parte las Resoluciones se formula un único cargo, con un total de treinta y tres (33) resoluciones, y en ese mismo orden, de mayor a menor, en la cantidad de cargos para el número de cargos dos y tres, se encuentra similitud, dicha condición también se encuentra equiparada para el número de cargos cuatro y cinco, mientras que, solamente en una resolución se imputaron siete cargos.

Número de Cargos.	
Descripción	**Cantidad**
Cargo único.	33
Dos cargos.	13
Tres cargos.	12
Cuatro cargos.	3
Cinco cargos.	3
Siete cargos.	1
Total	65

Tabla No. 5 Para el Número de cargos de las Resoluciones Sanción.

En términos porcentuales, se presenta el siguiente gráfico para la cantidad de resoluciones frente al número de cargos.

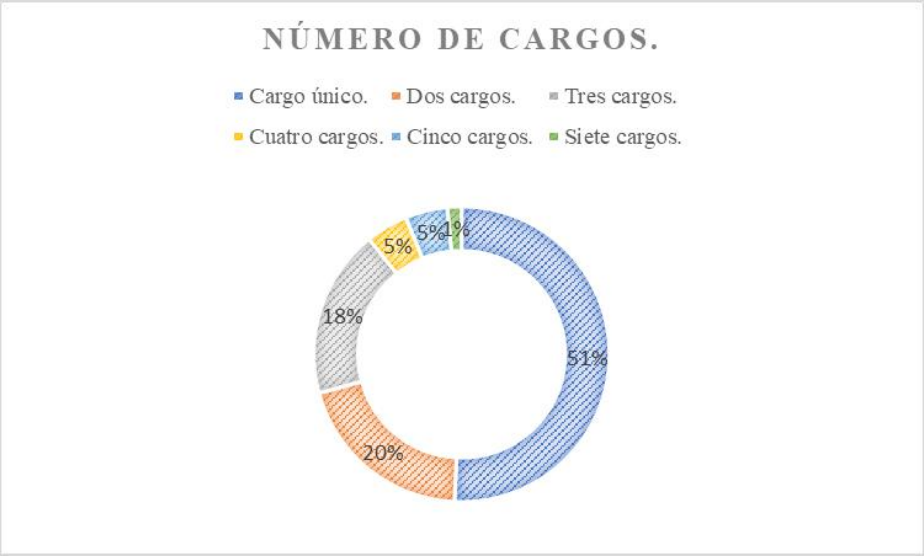


Gráfico No. 4 Para el Número de Cargos de la Resoluciones Sanción.

De conformidad con lo establecido en los Artículos 19 y 21 de la Ley 1581 de 2012 la Dirección de Investigación de Protección de Datos Personales es competente para investigar e imponer las sanciones pertinentes a los Responsables y Encargados del Tratamiento de datos una vez verifique el incumplimiento de las disposiciones en materia de protección de datos, en este punto, cuando se resuelve iniciar investigación administrativa, se procede a formular los cargos, que son por concepto de la presunta violación a lo dispuesto en las disposiciones normativas.

La presunta violación a las disposiciones normativas contenidas en el Régimen de Protección de Datos Personales parte desde la etapa actual en el marco del desarrollo tecnológico, los desarrollos y progresos informáticos, que propician aún más la trasgresión a los derechos y libertades de miles de usuarios, por ello, estos antecedentes han proporcionado a través de la doctrina jurídica y el desarrollo jurisprudencial dentro de los ordenamientos jurídicos, el reconocimiento al Derecho a la información y la autodeterminación informativa, que tienen su principal instrumento de garantía en el Derecho Fundamental de Hábeas Data, es decir, la facultad que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada según el Artículo 15 de la Constitución Política de Colombia, el cual comprende tres facultades concretas en cuanto al derecho a conocer las informaciones que a su titular se refieren, el derecho a actualizar tales informaciones, y el derecho a rectificar las informaciones que no correspondan a la verdad.

En Colombia, el Derecho Fundamental de Hábeas Data consagrado tanto en la Constitución Política de Colombia en su Artículo 15 y en la Ley 1266 de 2008 es la base del Régimen de Protección de Datos Personales, a partir de este derecho fundamental, se desarrollan todos los elementos relacionados con el Régimen de Protección de Datos Personales en Colombia,

específicamente, en la Ley Estatutaria 1581 de 2012 que tiene por objeto garantizar los derechos de las personas sobre el control de su información personal y sobre la confidencialidad, integridad y disponibilidad de esta en bases de datos, y sus decretos reglamentarios establecen las normas regulatorias específicas para garantizar la Protección de los Datos Personales en el territorio Colombiano bajo parámetros delimitados como la autorización expresa del titular, el consentimiento previo del titular, la finalidad legítima del tratamiento de Datos Personales, el acceso restringido a la información personal del titular, la seguridad y la confidencialidad de los datos personales, entre otros aspectos relevantes.

Por tal motivo, en ese orden de ideas, cuando surge una situación en donde existe una vulneración a los derechos salvaguardados a los titulares de la información a través de conductas como prácticas incorrectas, inadecuadas, vulneratorias o contrarias a las normativas de protección de datos en el tratamiento de la información personal de los individuos, las cuales transgreden el derecho a la privacidad y los derechos de las personas en relación con sus datos personales, se presenta la imperiosa necesidad, de que la entidad competente, particularmente, la Superintendencia de Industria y Comercio, respaldada en sus facultades sancionatorias, inicie la correspondiente investigación por medio de Delegatura para la Protección de Datos Personales para formular los debidos cargos e imponer la sanción a que haya a lugar. Lo anterior, resalta la importancia de la formulación en el número de cargos frente a las conductas desplegadas por el investigado, como se presentó en las ilustraciones estadísticas.

En cuanto a la calidad del sujeto investigado por la Superintendencia de Industria y Comercio por Indebido Manejo de Datos Personales.

La calidad del sujeto investigado por la Superintendencia de Industria y Comercio (SIC) por indebido manejo de datos personales hace referencia a la clasificación jurídica de la entidad, persona o entidad responsable del tratamiento de datos personales que está siendo objeto de una investigación por presuntas violaciones a las normativas de protección de datos en Colombia. En el contexto de las indagaciones e investigaciones llevadas a cabo por la Superintendencia de Industria y Comercio, la calidad del sujeto investigado adquiere relevancia en relación con su responsabilidad en el manejo adecuado y legal de la información personal de los individuos titulares.

En este orden de ideas, se destaca fundamentalmente la importancia de la calidad del sujeto investigado como factor determinante en la evaluación de posibles infracciones a la normativa al Régimen de Protección de Datos Personales, subrayando la diferenciación entre la calidad del sujeto investigado, lo cual permite determinar con mayor concreción y exactitud la responsabilidad de las entidades privadas, públicas y personas naturales en el manejo legal y ético de la información personal en el contexto del ordenamiento jurídico colombiano.

En el ordenamiento jurídico colombiano, particularmente, en el Régimen General de Protección de Datos Personales, de conformidad con lo establecido en la Ley 1581 de 2012, el sujeto investigado, puede ser una persona, según el Artículo 73 del Código Civil

Colombiano, *"Las personas son naturales o jurídicas"*, así las cosas, se entiende que una persona natural es un individuo humano, es decir, un ser humano con existencia física, que tiene capacidad jurídica para adquirir derechos y contraer obligaciones desde su nacimiento hasta su muerte, sin embargo, la capacidad jurídica puede estar sujeta a restricciones específicas, como la capacidad de obrar, que puede variar según la edad y otras circunstancias; por otro lado, la persona jurídica es una ficción legal que, aunque no tiene existencia física, es reconocida por la ley como sujeto de derechos y obligaciones, puede ser una entidad de derecho público o de derecho privado, que se crea y reconoce de acuerdo con las leyes y regulaciones colombianas. Algunas de las figuras societarias más comunes de las personas jurídicas incluyen sociedades, fundaciones, asociaciones, entre otras, y así como las personas naturales, pueden realizar actividades legales, adquirir bienes, contraer deudas y participar en transacciones legales en su propio nombre a través del representante legal.

Dentro de la presente investigación, de las sesenta y cinco (65) Resoluciones emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de datos personales, se observa que,

Calidad del Sujeto Investigado.	
Descripción	**Cantidad**
Persona Natural.	1
Persona Jurídica.	64
Total	65

Tabla No. 6 Para la Calidad del Sujeto Investigado de las Resoluciones Sanción.

Gráfico No. 5 Para la Calidad del Sujeto Investigado de las Resoluciones Sanción.

Según las estadísticas, del número total de Resoluciones emitidas por la Superintendencia de Industria y Comercio, para el año 2022, por indebido manejo de datos personales, de ellas, en sesenta y cuatro (64) Resoluciones Sanción, la calidad de sujeto investigado fue ocupada por una persona jurídica, en su totalidad, personas jurídicas de Derecho Privado, de las cuales

se destacan figuras societarias, tales como, Sociedades por Acciones Simplificadas, Sociedades Anónimas, Sociedades Limitadas, Sociedades en Comanditas por Acciones, Propiedades Horizontales, Bancos, Empresas de Servicios Públicos, Universidades, Liceos, Academias de Educación, Cajas de Compensación Familiar, Sindicatos, Hoteles, y Clínicas.

Por otro lado, solamente una (1) de las Resoluciones Sanción emitidas por la Superintendencia de Industria y Comercio, para el año 2022, por indebido manejo de datos personales, a saber, la autoridad competente, sancionó al señor Diego Fernando Pino Paredes, como consecuencia a que, gestionó procesos de venta de bases de datos en línea sin obtener la autorización previa, expresa e informado del titular y a su vez, tal autorización debe estar ligada a la finalidad del tratamiento o conexa a ésta.

En efecto, la evidencia de las figuras de Derecho Privado que ocupa el sujeto investigado demuestra que sin discriminación alguna, los agentes del mercado presentes en la sociedad se pueden ver involucrados en procesos como el indebido manejo de dato personales, en específico, por ello, la importancia de que la autoridad competente, esté comprometida, por medio de la función de vigilancia y control a velar por verificar que las entidades estén cumpliendo con las disposiciones normativas que le son aplicables, particularmente, con especial detalle y cuidado, si dentro del ejercicio de sus operaciones comerciales se encuentran manejando datos personales de los ciudadanos, que a su vez, son parte de una ésfera que requiere de debida diligencia, en cuanto a la imperiosa protección que los datos personales precisan.

Las personas naturales y las personas jurídicas involucradas en el manejo de datos personales, dentro del ejercicio de las operaciones y gestión del tratamiento de datos personales, pueden adquirir dos (2) posturas, a saber, ocupar la posición de Responsable del Tratamiento de Datos Personales y/o Encargado del Tratamiento de Datos Personales.

Conceptualmente, el Responsable del Tratamiento de los Datos Personales es la persona natural o jurídica que decide sobre las finalidades del tratamiento y los medios empleados para el efecto, por ejemplo, para ponerlos en circulación, usarlos de alguna manera o determinar su acceso.

Por su parte, el Encargado del Tratamiento de los Datos Personales o subencargado es la persona natural o jurídica que realiza el tratamiento de los datos personales por instrucción o delegación del responsable y está sujeto a las obligaciones contempladas en la Ley 1581 del 2012, sus decretos reglamentarios y las instrucciones impartidas por la Superintendencia de Industria y Comercio. Por lo tanto, le corresponde garantizar al titular en todo tiempo el pleno y efectivo ejercicio del Derecho Fundamental de Hábeas Data; conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; realizar oportunamente la actualización, rectificación o supresión de los datos.

Tomando en cuenta la cantidad total de Resoluciones Sanción, objeto de estudio, analizadas en el transcurso de la investigación, se concluye que, de sesenta y cinco (65) Resoluciones emitidas por la Superintendencia de Industria y Comercio respecto al indebido manejo de

datos personales, únicamente una (1) de ellas, la calidad de sujeto investigado, fue ocupada por un Encargados del Tratamiento de Datos Personales. En consecuencia, sesenta y cuatro (64) de las Resoluciones expedidas por la Superintendencia de Industria y Comercio, acerca del indebido manejo de datos personales, sancionan a Responsables del Tratamiento de Datos Personales.

A continuación, de manera detallada, se menciona el acto administrativo que abarca el tema en específico del Encargado del Tratamiento de Datos Personales,

Por medio de la Resolución No. 77643 de 2022, la Superintendencia de Industria y Comercio, en el ejercicio de las funciones de de vigilancia y control respecto de los Responsables y Encargados del tratamiento de Datos Personales, sanciona a la sociedad, Seguridad El Progreso LTDA, toda vez que, en su calidad de Encargado del tratamiento de datos personales, no acreditó haber atendido los requerimientos realizados por la autoridad nacional de protección de datos.

Para contextualizar, la infracción por parte del Encargado del Tratamiento de Datos Personales, quién opera actividades de seguridad privada, se presentó en el entendido en que, no atendió los requerimientos impartidos por la Superintendencia de Industria y Comercio de conformidad con el Literal O del artículo 17 de la Ley 1581 de 2012, en el transcurso de la investigación adelantada hacía el Conjunto Residencial Los Arrayanes De Sauzalito P.H, que es el directamente responsable del tratamiento de datos personales de sus residentes y propietarios y que es dicho conjunto el que tiene el deber de obtener las respectivas autorizaciones de sus copropietarios, sin embargo, probatoriamente, nada dijo sobre su deber de atender los requerimientos realizados por la Superintendencia.

Por otro lado, la sanciones impuestas por la Superintendencia de Industria y Comercio, en cuanto al indebido manejo de datos personales a los Responsables del Tratamiento de Datos, recae primordialmente sobre figuras societarias de derecho privado. Algunas de las que se destacan son,

La sociedad Hotel Termales del Otoño S.C.A, en su calidad de Responsable del Tratamiento de Datos Personales, faltó al deber de solicitar y conservar copia de la autorización de los Titulares, respecto a la información recaudada a través de su página web en el apartado *"Reservas"*, igualmente pese a contar con un aviso de privacidad, no acreditó que se encontraba implementado y puesto a disposición de los titulares. Tampoco implementó un Manual de Políticas de seguridad, ni contestó los requerimientos de este despacho, obstaculizando las facultades de vigilancia y control, por tanto, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

La sociedad Sindicato de Trabajadores del Hospital San Juan de Dios, en su calidad de Responsable del Tratamiento de Datos Personales, realizó el tratamiento de los datos personales sensibles del titular sin contar con su autorización previa, expresa e informada. En este caso no resulta aplicable la excepción legal contenida en el literal c) del artículo sexto de la Ley 1581 de 2012, puesto que la misma aplica exclusivamente respecto de los miembros del sindicato o respecto de las personas que mantengan contactos regulares por razón de su

finalidad. Así mismo, debe implementar la Política de Tratamiento de Datos Personales y un manual de procedimiento para la atención de consultas y reclamos, de seguridad y ciclo del dato, por tanto, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

La sociedad Comunicación Celular S.A COMCEL S.A, en su calidad de Responsable del Tratamiento de Datos Personales, continuó enviando mensajes publicitarios, comerciales y promocionales a la línea móvil del Titular a través de códigos cortos aun después de que éste solicitara que no le enviaran esta información, obstaculizando el ejercicio del derecho de hábeas data, así mismo, incumplió con la orden administrativa impartida por esta Dirección por cuanto continuó con el envío de mensajes publicitarios, comerciales y promocionales en el año 2021 a la línea móvil del Titular, por tanto, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

La sociedad MercadoLibre Colombia LTDA, en su calidad de Responsable del Tratamiento de Datos Personales, incumplió con el deber legal, con los Titulares de la Información, de salvaguardar la información bajo medidas de seguridad adecuadas, procurando siempre la protección de los datos personales de cada uno. En consecuencia, si la sociedad divulga y/o expone datos personales a terceros no autorizados, así sea solo la dirección de correo electrónico, se genera un incumplimiento del deber de impedir la consulta, uso o acceso no autorizado o fraudulento de los datos personales de los Titulares, por tanto, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

La Universidad Católica de Colombia, en su calidad de Responsable del Tratamiento de Datos Personales, realizó el envío de un correo electrónico de carácter publicitario a la dirección electrónica institucional del denunciante, el cual es un dato semiprivado, sin contar con su autorización previa, expresa e informada para el tratamiento de sus datos personales; así como tampoco le informó sobre la finalidad de la recolección de sus datos y los derechos que le asisten. Por otra parte, la sociedad, pese a tener implementadas algunas medidas tendientes a proteger el Derecho de Hábeas Data, estas no fueron suficientes, y las funcionarias que enviaron el correo publicitario al titular no fueron debidamente capacitadas sobre el Régimen de protección de datos personales, por tanto, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

La entidad financiera Banco Pichincha S.A, en su calidad de Responsable del Tratamiento de Datos Personales, actuó de manera negligente frente al tratamiento de los datos personales del titular, al no cumplir con su deber de garantizar en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, al continuar enviando notificaciones a su dirección de correo electrónico, después de recibir la solicitud de supresión de dicho dato por parte del titular. De igual forma incumplió con el deber de atender los requerimientos de esta Superintendencia con el fin de esclarecer los hechos de la investigación, por tanto, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

La Academia de Pilotos De Aviación S.A, en su calidad de Responsable del Tratamiento de Datos Personales, tienen el deber de atender las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, especialmente la instrucción de registrar sus bases de datos en el Registro Nacional de Bases de Datos. De igual forma, los Responsables deben implementar, una Política de Tratamiento de Datos personales, un Manual con los procedimientos para la recolección, almacenamiento, uso, circulación y supresión de la información, un Manual Interno para la Atención de Consultas y Reclamos y un Manual Interno de Políticas de Seguridad, por tanto, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

La sociedad RAPPI S.A.S, en su calidad de Responsable del Tratamiento de Datos Personales, tiene el deber legal de cumplir con las instrucciones, en cuanto, se le ordena la corrección, actualización o retiro de los datos personales de una base de datos, cuando así se determine dentro de una investigación, por lo tanto, los Responsables, están en la obligación de acatar las órdenes impartidas y, demostrar el cumplimiento de los deberes a los que se encuentra obligados, por tanto, ante la situación de un incumplimiento, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

La Caja Colombiana de Subsidio Familiar Colsubsidio, en su calidad de Responsable del Tratamiento de Datos Personales, trató el número de celular del titular sin contar con su autorización para ello, ya que la autorización obtenida fue suministrada por un tercero, por lo que incumplió el deber de solicitar y conservar copia de la autorización previa, expresa e informada; así mismo, vulneró el deber de informarle la finalidad de la recolección de sus datos personales. Por otra parte, se evidencia que no dio una respuesta de fondo a la petición del Titular, ni dentro del término legal establecido, por tanto, la Superintendencia de Industria y Comercio sanciona con una multa de carácter administrativo e imparte órdenes.

Estadísticamente, lo anteriormente expresado respecto al Encargado y Responsable del Tratamiento se expresa cuantitativamente de la siguiente manera,

Calidad del Sujeto Investigado.	
Descripción	**Cantidad**
Encargado del Tratamiento de Datos Personales.	1
Responsable del Tratamiento de Datos Personales.	64
Total	65

Tabla No. 7 Para la calidad del Sujeto Investigado de las Resoluciones Sanción.

Gráfico No. 6 Para la calidad del Sujeto Investigado de las Resoluciones Sanción.

A modo de conclusión, porcentualmente se observa que respecto a la calidad del sujeto investigado con relación a sí es una persona natural o una persona jurídica, el noventa y ocho por ciento (98%) de la muestra objeto del estudio de investigación corresponde a que el sujeto investigado adquiere la calidad de persona jurídica, mientras que, aproximadamente, el dos por ciento (2%) corresponde a la calidad de persona natural. Siguiendo la misma línea, tanto las personas naturales, como las personas jurídicas, pueden estar inmersos en la posición de Responsable del Tratamiento de Datos Personales y/o Encargado del Tratamiento de Datos Personales, en términos de cifras estadísticas, el noventa y ocho por ciento (98%) de la muestra objeto del estudio de investigación corresponde a que el sujeto investigado es el Responsable del Tratamiento de Datos Personales, mientras que, únicamente, aproximadamente el dos por ciento (2%) corresponde al Encargado del Tratamiento de Datos Personales.

En cuanto a los deberes que le corresponden a los Responsables Del Tratamiento de Datos Personales y/o Encargados Del Tratamiento.

Acerca del cumplimiento normativo de los Deberes del Responsable y/o Encargado del Tratamiento de Datos Personales consagrados en la Ley 1581 de 2012.

En el contexto de la Protección de Datos Personales, los términos *"Responsable del Tratamiento"* y *"Encargado del Tratamiento" s*e refieren a roles específicos dentro del marco legal, como el Régimen de Protección de Datos Personales**.** A saber,

El Responsable del Tratamiento es la entidad u organización que determina los fines y medios del procesamiento de datos personales. En otras palabras, es la entidad que toma decisiones sobre cómo y por qué se recopilan, almacenan y procesan datos personales. El Responsable del Tratamiento tiene la responsabilidad principal de garantizar que el tratamiento de datos

cumpla con las leyes de protección de datos aplicables y que se respeten los derechos de los individuos cuyos datos se están procesando.

El Encargado del Tratamiento es una entidad u organización que procesa datos personales en nombre del Responsable del Tratamiento. Este rol implica llevar a cabo las instrucciones del Responsable del Tratamiento y garantizar que se implementen medidas adecuadas para proteger la privacidad y seguridad de los datos. Los Encargados del Tratamiento pueden ser proveedores de servicios externos contratados para realizar operaciones específicas de procesamiento de datos. También tienen la responsabilidad de cumplir con las leyes de protección de datos y de colaborar con el Responsable del Tratamiento para garantizar el respeto de los derechos de los individuos.

De lo expuesto, el Responsable del Tratamiento toma decisiones sobre el tratamiento de datos, mientras que el Encargado del Tratamiento realiza operaciones específicas de procesamiento de datos en nombre del Responsable del Tratamiento. Ambos deben trabajar en conjunto para garantizar el cumplimiento de las leyes de protección de datos y proteger la privacidad de las personas cuyos datos están siendo procesados.

Dentro de este orden de ideas, en el transcurso de la investigación, se advierte, que las normas vulneradas, atienden esencialmente al incumplimiento o infracción a los deberes que le asisten en la calidad de Responsable del Tratamiento de Datos Personales o Encargado del Tratamiento de Datos Personales, por ello, de las sesenta y cinco (65) Resoluciones emitidas por la Superintendencia de Industria y Comercio por Indebido Manejo de Datos Personales, se hace la siguiente diferenciación,

Los deberes que le corresponden al Responsable del Tratamiento de Datos Personales, están consagrados en el Artículo 17 de la Ley 1581 de 2012; la disposición normativa de manera literal estipula lo siguiente,

Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

f) 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 necesarias para que la información suministrada a este se mantenga actualizada;

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

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

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

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

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

m) Informar a solicitud del Titular sobre el uso dado a sus datos;

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

De manera detallada, y considerando que en la mayor cantidad de Resoluciones emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de Datos Personales, los sujetos investigados ostentan la calidad de Responsable del Tratamiento de Datos, se especifica de manera breve y concisa lo relacionado a cada uno de los literales del Artículo 17 de la Ley 1581 de 2012, a continuación,

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento tienen la obligación de asegurar y salvaguardar que los titulares de datos personales puedan ejercer plenamente y de manera efectiva el Derecho Fundamental de Hábeas Data, el cual implica que los titulares tengan la facultad de controlar la información que se recopila, almacena, utiliza y procesa sobre ellos en bases de datos, de acceder a la información que se ha recopilado sobre ellos, conocer su uso, solicitar su corrección si es incorrecta, y en general, tener control sobre sus datos personales. Al garantizar el ejercicio del Derecho de Hábeas Data, los Responsables del Tratamiento contribuyen a la protección integral de los derechos de los titulares de datos personales, promoviendo la transparencia y el respeto en cuanto a la

privacidad, la intimidad y la autodeterminación informativa de los individuos, promoviendo la autonomía y el control de los individuos sobre su propia información.

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen el deber de solicitar y conservar, de acuerdo con las condiciones establecidas por la ley, una copia de la autorización otorgada por el Titular de la información. Esto implica que las entidades Responsables del Tratamiento o personas encargadas de gestionar datos personales deben obtener por medio de una autorización otorgada por el titular, el consentimiento expreso de los individuos a quienes pertenece la información personal, y además, se les exige como prerrogativa que deben mantener una copia de dicha autorización en cumplimiento con las disposiciones legales aplicables, lo cual busca garantizar la transparencia y el respeto por la privacidad de los individuos cuyos datos están siendo procesados por la entidad.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, dentro de sus deberes tienen la obligación de informar de manera adecuada al Titular de los Datos Personales sobre la finalidad de la recolección y los derechos que le corresponden como consecuencia de la autorización otorgada. En otras palabras, las entidades o personas encargadas de gestionar datos personales deben comunicar claramente a los titulares la razón por la cual se están recopilando sus datos y también informarles sobre los derechos con los que cuentan en relación con dicha autorización. Esto busca garantizar la transparencia en el manejo de la información personal, permitiendo a los titulares de la información que conozcan de manera clara y precisa cómo se utilizarán sus datos y qué prerrogativas tienen en relación con su privacidad y seguridad.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de conservar la información personal bajo condiciones de seguridad adecuadas, lo cual implica tomar medidas para prevenir la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos. En otras palabras, las entidades o individuos encargados de gestionar información personal deben implementar medidas de seguridad efectivas para proteger los datos contra posibles amenazas o riesgos que puedan comprometer su integridad y confidencialidad. Estas medidas pueden incluir controles de acceso, encriptación, copias de seguridad regulares y otras prácticas de seguridad informática, en cuanto, a que el objetivo es garantizar la privacidad y la protección de los datos personales, cumpliendo con las disposiciones legales y promoviendo la confianza de los titulares en el manejo responsable de su información.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de garantizar que la información proporcionada al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible. En términos simples, significa que aquellos que manejan datos personales deben asegurarse de que la información que comparten con terceros, es decir, el Encargado del Tratamiento, cumpla con ciertos estándares de calidad. La veracidad implica que la información sea precisa y real; el lleno de la información se refiere a que no falten datos relevantes; la exactitud se relaciona con la precisión de la información; la actualización implica que los datos estén al día; la con probabilidad se refiere a la posibilidad de verificar la información; y la comprensibilidad significa que la información sea clara y en términos comprensible. De ahí que, cumplir con estos requisitos sea un aspecto fundamental para mantener la integridad de los datos y asegurar que la información sea confiable y útil en el proceso de tratamiento.

f) 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 necesarias para que la información suministrada a este se mantenga actualizada;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de actualizar la información proporcionada al Encargado del Tratamiento de manera oportuna. Esto implica que si hay cambios o novedades en los datos que previamente se hayan suministrado, el Responsable del Tratamiento debe comunicar estos cambios al Encargado del Tratamiento de manera rápida y efectiva. Además, el Responsable del Tratamiento debe adoptar todas las medidas necesarias para asegurarse de que la información proporcionada al Encargado del Tratamiento se mantenga actualizada de manera continua. Este requisito es indispensable, en cuanto, busca garantizar la precisión y actualización de la información gestionada, contribuyendo así a la integridad de los datos y cumpliendo con los principios de protección de datos, que incluyen la actualización y corrección de la información personal.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tiene la obligación de rectificar la información cuando sea incorrecta y comunicar esta corrección al Encargado del Tratamiento. En otras palabras, si el Responsable del Tratamiento advierte que la información personal que maneja es inexacta o contiene errores, tiene la responsabilidad de corregirla. Además, debe informar a la entidad o individuo designado como Encargado del Tratamiento sobre esta rectificación para asegurarse de que la información corregida se refleje adecuadamente en los registros y sistemas pertinentes; lo anterior busca mantener la exactitud y veracidad de los datos personales, contribuyendo así a la integridad de la información y cumpliendo con los principios de protección de datos que destacan la importancia de garantizar que los datos sean correctos y estén actualizados.

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

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de suministrar al Encargado del Tratamiento, según corresponda, únicamente aquellos datos cuyo tratamiento haya sido previamente autorizado de acuerdo con lo establecido en la Ley de Protección de Datos. Esto significa que el Responsable del Tratamiento no puede compartir con el Encargado del Tratamiento información que no cuente con la debida autorización del titular de los datos o que no esté respaldada por las disposiciones legales aplicables. El proceso de autorización implica obtener el consentimiento explícito de los individuos cuyos datos serán tratados, asegurando así que el manejo de la información personal se realice de manera transparente y conforme a las regulaciones vigentes, lo cual busca proteger los derechos de privacidad de los titulares y garantizar que sus datos solo se utilicen de acuerdo con los términos y condiciones autorizados.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de exigir al Encargado del Tratamiento, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular. En otras palabras, el Responsable del Tratamiento debe asegurarse de que la entidad o persona designada como Encargado del Tratamiento cumpla rigurosamente con las medidas de seguridad y privacidad establecidas para proteger la información personal del titular.

Este requisito destaca la importancia de establecer y mantener altos estándares de seguridad para evitar la adulteración, pérdida, consulta, uso no autorizado o cualquier forma de acceso fraudulento a la información del titular. A través de esta exigencia, se busca garantizar que tanto el Responsable del Tratamiento como el Encargado del Tratamiento cumplan con las normativas de protección de datos y resguarden la confidencialidad y seguridad de la información personal.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de tramitar las consultas y reclamos formulados de acuerdo con lo establecido en la ley de Protección de Datos. Esto implica que las personas cuyos datos personales están siendo procesados tienen el derecho de realizar consultas o presentar reclamos sobre el tratamiento de su información personal, y el Responsable del Tratamiento está obligado a gestionar las peticiones de manera adecuada y oportuna conforme los términos señalados en el Régimen de Protección de Datos Personales.

El Responsable del Tratamiento de Datos Personales debe proporcionar los procedimientos y mecanismos necesarios para que los titulares de los datos puedan ejercer sus derechos, en cuanto, acceso, corrección, actualización, rectificación y supresión de la información

personal. Además, debe responder a las consultas y reclamos en los términos y plazos establecidos por la ley, garantizando así una comunicación efectiva y transparente con los titulares de los datos.

Esta prerrogativa busca salvaguardar los derechos de los Titulares de Datos, brindándoles la oportunidad de participar en el control y manejo de su información personal, así como asegurar que los Responsables del Tratamiento de Datos respondan de manera diligente y efectiva a sus inquietudes o solicitudes.

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

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de adoptar un manual interno de políticas y procedimientos. Este manual debe ser diseñado con el propósito de asegurar el adecuado cumplimiento de la Ley de Protección de Datos Personales, con un enfoque particular en la atención de consultas y reclamos. En otras palabras, el Responsable del Tratamiento debe desarrollar un documento interno que contenga políticas y procedimientos específicos relacionados con la gestión de datos personales. Estas políticas y procedimientos deben estar alineados con los requisitos y principios establecidos en la ley, y deben abordar de manera detallada la forma en que se gestionarán las consultas y reclamos de los Titulares de los Datos.

El objetivo de este precepto es establecer pautas claras y procesos internos para garantizar el cumplimiento normativo y la atención efectiva de las solicitudes de los Titulares de los Datos. Además, el manual interno ayuda a que los involucrados en el Tratamiento de Datos tengan un marco de referencia claro sobre cómo deben manejarse y protegerse los Datos Personales de acuerdo con la ley.

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de informar al Encargado del Tratamiento cuando cierta información esté en conflicto por parte del titular de los datos. Esto se aplica específicamente después de que el titular haya presentado una reclamación y el proceso aún no haya concluido. Es decir, si un titular de datos presenta un reclamo sobre la información que está siendo procesada, y el proceso de resolución de la reclamación aún no ha finalizado, el Responsable del Tratamiento debe comunicar esta situación al Encargado del Tratamiento. Esto asegura que el Encargado del Tratamiento tenga conocimiento de cualquier disputa en curso sobre la información que está siendo manejada, lo cual puede ser relevante para garantizar el adecuado tratamiento y resolución de la controversia.

Este requisito busca facilitar la comunicación y coordinación entre el Responsable del tratamiento y el Encargado del Tratamiento en situaciones en las que la información

procesada esté siendo objeto de disputa o reclamación por parte del titular, contribuyendo así a una gestión transparente y eficaz de las situaciones conflictivas.

m) Informar a solicitud del Titular sobre el uso dado a sus datos;

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de informar al titular, a solicitud de este, sobre el uso dado a sus datos personales. Esto significa que los individuos tienen el derecho de solicitar información acerca de cómo se están utilizando sus Datos Personales, y el Responsable del Tratamiento está obligado a proporcionar esta información de manera clara y completa. Este requisito promueve la transparencia y el control que los titulares de datos tienen sobre el manejo de su información personal, permitiéndoles conocer con precisión el propósito y alcance del tratamiento de sus datos.

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de informar a la autoridad de Protección de Datos, particularmente, a la Superintendencia de Industria y Comercio, cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares. En situaciones donde la seguridad de los Datos Personales se ve comprometida, como en casos de brechas de seguridad, intrusiones no autorizadas u otros incidentes similares, el Responsable del Tratamiento debe notificar de inmediato a la autoridad de protección de datos. Esta medida busca garantizar una respuesta rápida y efectiva ante posibles riesgos para la privacidad de los titulares, permitiendo que la autoridad de protección de datos tome las acciones necesarias para mitigar los impactos y proteger la información personal. Además, la oportuna notificación contribuye a la transparencia y responsabilidad en la gestión de datos personales.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Esta disposición normativa hace referencia a que, los Responsables del Tratamiento de Datos Personales, tienen la obligación de cumplir con las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio. En este contexto, la Superintendencia de Industria y Comercio es la entidad encargada de supervisar y regular el cumplimiento de las normas de Protección de Datos en Colombia. Por lo tanto, los Responsables del Tratamiento deben acatar las directrices, instrucciones y requisitos que emita esta entidad para asegurar el cumplimiento de las leyes y regulaciones de protección de datos. Este requisito refuerza la supervisión y control por parte de la autoridad competente, contribuyendo a la aplicación efectiva de las normas de privacidad y protección de datos en el país.

De conformidad con los resultados obtenidos en el transcurso de la investigación de las Resoluciones emitidas por la Superintendencia de Industria y Comercio para el año 2022, específicamente en materia de Indebido Manejo de Datos Personales,

se puede evidenciar que, las sanciones administrativas que impone la Superintendencia de Industria y Comercio se adoptan como consecuencia de la existencia de una conducta vulneratoria al Régimen de Protección de Datos Personales; por tanto, las infracciones cometidas se adecuan típicamente a los deberes del Responsable del Tratamiento de Datos, consagrados en los literales del Artículo 17 de la Ley 1581 de 2012, que en concurrencia son vulnerados.

Los gráficos estadísticos que se detallan a continuación reflejan los resultados obtenidos en cuanto a la cantidad de veces que la Superintendencia de Industria y Comercio evidenció que los sujetos investigados, bien sean Responsables y/o Encargados del Tratamiento, vulneraron alguna de las disposiciones normativas consagradas en el Artículo 17 de la Ley 1581 de 2012.

Deberes del Responsable del Tratamiento de Datos Personales.	
Descripción	**Cantidad**
Literal A del Artículo 17 de la Ley 1581 de 2012.	7
Literal B del Artículo 17 de la Ley 1581 de 2012.	21
Literal C del Artículo 17 de la Ley 1581 de 2012.	18
Literal D del Artículo 17 de la Ley 1581 de 2012.	10
Literal E del Artículo 17 de la Ley 1581 de 2012.	1
Literal F del Artículo 17 de la Ley 1581 de 2012.	0
Literal G del Artículo 17 de la Ley 1581 de 2012.	2
Literal H del Artículo 17 de la Ley 1581 de 2012.	0
Literal I del Artículo 17 de la Ley 1581 de 2012.	0
Literal J del Artículo 17 de la Ley 1581 de 2012.	10
Literal K del Artículo 17 de la Ley 1581 de 2012.	34
Literal L del Artículo 17 de la Ley 1581 de 2012.	0
Literal M del Artículo 17 de la Ley 1581 de 2012.	0
Literal N del Artículo 17 de la Ley 1581 de 2012.	2
Literal O del Artículo 17 de la Ley 1581 de 2012.	25

Tabla No. 8 Para los Deberes del Responsable del Tratamiento de Datos Personales.

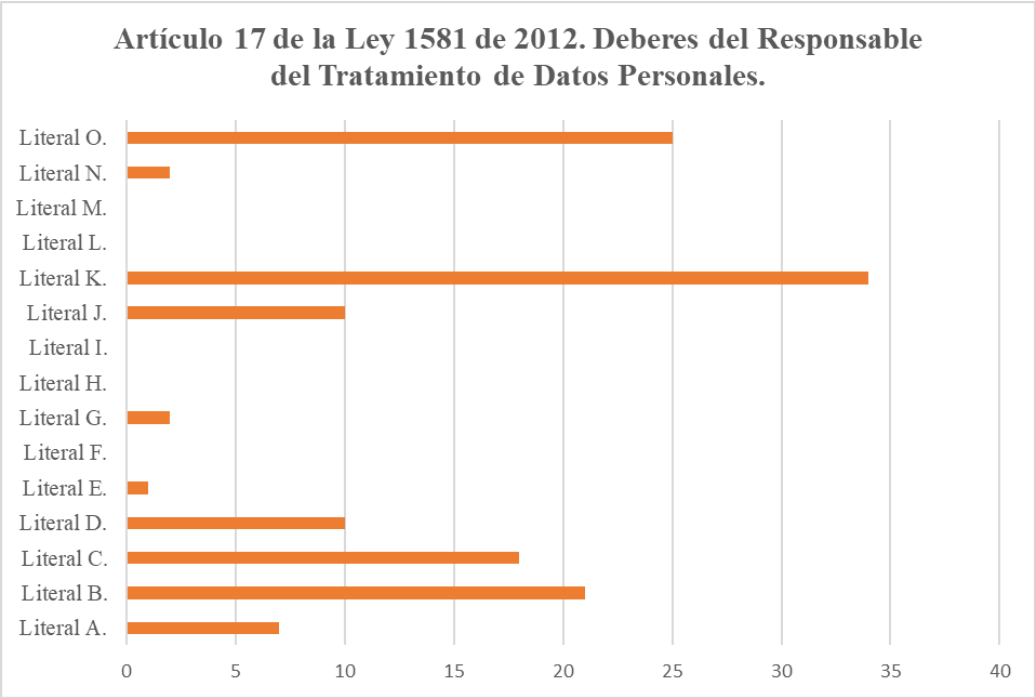


Gráfico No. 7 Para los Deberes del Responsable del Tratamiento de Datos Personales.

A partir de los datos estadísticos presentados en la Tabla No. 5 y en el Gráfico No. 4, se evidencia que, respecto al contenido del número total de las Resoluciones Sanción emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de datos personales, para el año 2022, por concepto de normas vulneradas, se tiene que,

El Literal K del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos; obtuvo un total de treinta y cuatro (34) veces, en que se evidenció su contravención por concepto de norma vulnerada.

El Literal O del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio; obtuvo un total de veinticinco (25) veces, en que se evidenció su contravención por concepto de norma vulnerada.

El Literal B del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular; obtuvo un total de veintiún (21) veces, en que se evidenció su contravención por concepto de norma vulnerada.

El Literal C del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización

otorgada; obtuvo un total de dieciocho (18) veces, en que se evidenció su contravención por concepto de norma vulnerada.

El Literal D del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; y, el Literal J del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben tramitar las consultas y reclamos formulados en los términos señalados en la presente ley; obtuvieron la misma cantidad cada uno, es decir, un total de diez (10) veces, en que se evidenció su contravención por concepto de norma vulnerada.

El Literal E del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible; obtuvo un total de una (1) vez, en que se evidenció su contravención por concepto de norma vulnerada.

El Literal F del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de 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 necesarias para que la información suministrada a este se mantenga actualizada;

El Literal H del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

El Literal I del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

El Literal L del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

El Literal M del Artículo 17 de la Ley 1581 de 2012, en cuanto a que los Responsables del Tratamiento, dentro de sus obligaciones, deben de informar a solicitud del Titular sobre el uso dado a sus datos;

Los anteriores literales, desde el Literal F hasta el Literal M, obtuvieron un total nulo (0) de veces, en que se evidenció su contravención por concepto de norma vulnerada. Lo cual tiene fundamento en que son deberes que el Responsable del Tratamiento delega al Encargado del

Tratamiento, lo cual no es una situación fáctica que se presenta en las Resoluciones objeto de estudio en la investigación.

Sin embargo, se hace la aclaración que el número total de veces en que se hace el conteo de cada uno de los numerales del Artículo en mención, no tiene relación con el número de Resoluciones objeto de estudio, toda vez que, indistintamente, cualquiera de los numerales pueden estar inmerso en varios de los cargos estudiados por la Superintendencia de Industria y Comercio en Resoluciones, y así las cosas, varios literales, de manera singular, pueden estar presentes en un solo cargo.

Las observaciones anteriormente presentadas, se muestran en el siguiente gráfico estadístico, que organiza la información en orden de mayor a menor, en cuanto a la cantidad de veces que cada uno de los literales del Artículo 17 de la Ley 1581 de 2012, se sancionó en los actos administrativos por concepto de norma vulnerada, a saber,

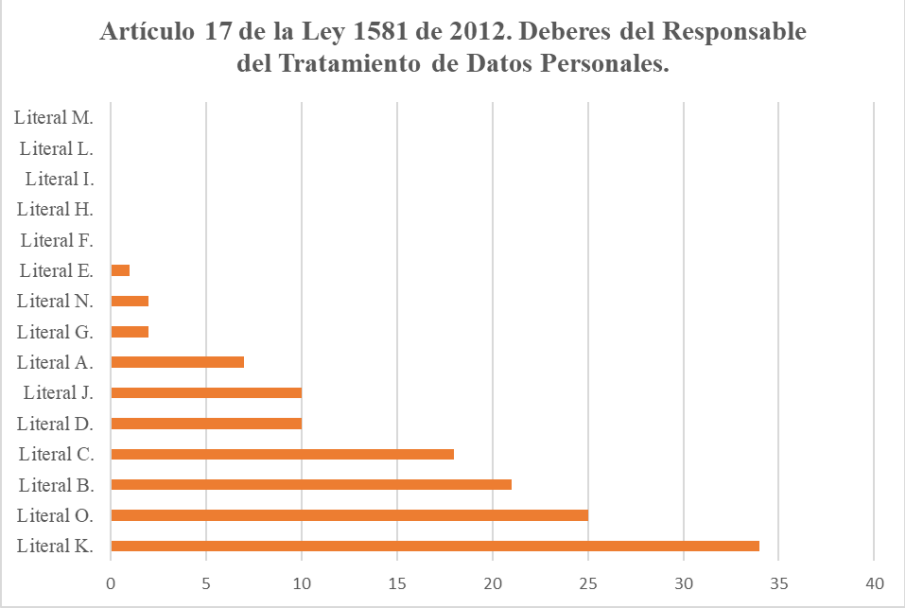


Gráfico No. 8 Para los Deberes del Responsable del Tratamiento de Datos Personales.

Por otro lado, los deberes que le corresponden al Encargado del Tratamiento de Datos Personales, están consagrados en el Artículo 18 de la Ley 1581 de 2012, la disposición normativa de manera literal estipula lo siguiente,

Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;

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

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;

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

g) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;

h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

PARÁGRAFO. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

Consecuentemente, solamente una de las Resoluciones objeto de estudio de la investigación, emitidas por la Superintendencia de Industria y Comercio, para el año 2022, sancionó a un Encargado del Tratamiento de Datos Personales, a saber, la empresa Seguridad El Progreso LTDA, específicamente, por concepto de la vulneración del Literal L del Artículo 18 de la Ley 1581 de 2012, en cuanto al incumplimiento en atender las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Acerca del tipo de infracción o violación cometida por parte del Responsable y/o Encargado del Tratamiento.

Frente a las sanciones que se imponen como consecuencia de la violación al Régimen de Protección de Datos, es preciso destacar que, de acuerdo con el principio de proporcionalidad

que guía el derecho administrativo sancionador, la autoridad administrativa, en este caso, la Superintendencia de Industria y Comercio está obligada a ejercer su facultad sancionadora de manera razonable, proporcionada y equitativa, de modo que este enfoque busca alcanzar un equilibrio proporcional y adecuado entre la sanción impuesta, y las prerrogativas de la normativa correspondiente, así como garantizar la proporcionalidad entre la conducta constitutiva de la infracción y la sanción aplicada. Sobre la aplicación de este principio, la Corte Constitucional ha señalado:

"En cuanto al principio de proporcionalidad en materia sancionatoria administrativa, éste exige que tanto la falta descrita como la sanción correspondiente a las mismas que resulten adecuadas a los fines de la norma, esto es, a la realización de los principios que gobiernan la función pública. Respecto de la sanción administrativa, la proporcionalidad implica también que ella no resulte excesiva en rigidez frente a la gravedad de la conducta, ni tampoco carente de importancia frente a esa misma gravedad" (Corte Constitucional, Sala Plena, Sentencia C-125 del 18 de febrero de 2003, Exp. Rad. D-4059, Magistrado Ponente Dr. Marco Gerardo Monroy Cabra).

De conformidad con la lectura de la disposición normativa consagrada en el Artículo 17 y el Artículo 18 de la Ley 1581, en concordancia con la aplicación del principio constitucional de proporcionalidad entre el hecho constitutivo de la sanción y la sanción aplicada, resulta claro que para que haya lugar a la imposición de una sanción por parte de la Superintendencia de Industria y Comercio, basta que la conducta desplegada por la investigada haya puesto en peligro los intereses jurídicos tutelados por la Ley 1581 de 2012, por tanto, ante el incumplimiento de los deberes por parte de los sujetos investigados, en el marco del indebido manejo de datos personales, es relevante adecuar la conducta atípica al hecho de cometer una infracción al Régimen de Protección de Datos, que vulnera los principios, derechos y garantías constitucionales y legales que rigen la materia. Por lo que respecta, se puede afirmar que, en cada una de las Resoluciones objeto de estudio de la presente investigación, queda demostrado el incumplimiento a los deberes que trata, en su mayoría, el Artículo 17 de la ley 1581 de 2012, y particularmente en un único procedimiento administrativo sancionatorio, el Artículo 18 de la Ley 1581 de 2012.

A modo de detalle, para contextualizar se presentan los siguientes ejemplos, en cuanto al tipo de infracción y/o violación cometida por los sujetos investigados, a saber,

Por un lado, la Resolución 25867 de 2022, por la cual se impone una sanción a la sociedad Rappi S.A.S por la infracción al deber de cumplir las instrucciones y los requerimientos que imparta la autoridad de protección de datos personales, consagrado en el Literal O del Artículo 17 de la Ley 1581 de 2012.

Por un lado, la Resolución 37200 de 2022, por la cual se impone una sanción a la entidad financiera Banco Pichincha S.A por la infracción al deber de contar con la autorización de manera previa expresa e informada del titular para el manejo de su información y el deber de cumplir con las instrucciones y requerimientos que imparte la Superintendencia de Industria y Comercio, consagrados en el Literal A del Artículo 17 de la Ley 1581 de 2012 y el Literal O del Artículo 17 de la Ley 1581 de 2012.

Por un lado, la Resolución 72798 de 2022, por la cual se impone una sanción a la sociedad Comunicación Celular S.A COMCEL S.A por la infracción al deber de garantizar al titular, en todo momento, el pleno y efectivo ejercicio del Derecho de Hábeas Data y el deber de cumplir con las instrucciones y requerimientos de la Superintendencia de Industria y Comercio, consagrados en el Literal A del Artículo 17 de la Ley 1581 de 2012 y el Literal O del Artículo 17 de la Ley 1581 de 2012.

Por un lado, la Resolución 54923 de 2022, por la cual se impone una sanción a la Clínica Vascular Navarra S.A, por la infracción al deber de conservar la información bajo las condiciones de seguridad necesarias para evitar su uso o acceso no autorizado, y el deber de informar a la autoridad cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares, consagrados en el Literal D del Artículo 17 de la Ley 1581 de 2012 y el Literal N del Artículo 17 de la Ley 1581 de 2012.

Por otro lado, la Resolución 60419 de 2022, por la cual se impone una sanción a la sociedad Integral Business Center S.A.S, por la infracción al deber de solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular, al deber de informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada, al deber de adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos, y al deber de Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio, consagrados en el Literal B del Artículo 17 de la Ley 1581 de 2012, el Literal C del Artículo 17 de la Ley 1581 de 2012, el Literal K del Artículo 17 de la Ley 1581 de 2015 y el Literal O del Artículo 17 de la Ley 1581 de 2015.

Por un lado, la Resolución 74662 de 2022, por la cual se impone una sanción a la sociedad Fitness People-Centro Médico Deportivo S.A.S, por la infracción al deber de informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada, consagrado en el Literal C del Artículo 17 de la Ley 1581 de 2015.

Por un lado, la Resolución 78501 de 2022, por la cual se impone una sanción a la sociedad Salud Actual IPS LTDA, por la infracción al deber de adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos, el deber de tramitar las consultas y reclamos formulados en los términos señalados en la presente ley, y el deber de cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio, consagrados en el Literal K del Artículo 17 de la Ley 1581 de 2012, Literal J del Artículo 17 de la Ley 1581 de 2012 y el Literal O del Artículo 17 de la Ley 1581 de 2012.

Por un lado, la Resolución 81963 de 2022, por la cual se impone una sanción a la sociedad Simba Software S.A.S, por la infracción al deber informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada, y al deber de tramitar las consultas y reclamos formulados en los términos señalados en la

presente ley, consagrados en el Literal C del Artículo 17 de la Ley 1581 de 2012 y el Literal J del Artículo 17 de la Ley 1581 de 2012.

En cuanto a la especificidad de los sujetos investigados respecto a la responsabilidad frente al proceso administrativo.

La responsabilidad del sujeto investigado implica evaluar si el Responsable y/ Encargado del Tratamiento que está siendo investigado por parte de la Superintendencia de Industria y Comercio ha cumplido o no con las obligaciones y responsabilidades establecidas en las prerrogativas sobre protección de datos personales en Colombia.

Esto incluye verificar condiciones, como, si se obtuvo la autorización previa, expresa e informada del titular, si se respetaron los principios para el tratamiento de datos personales, si se han implementado medidas correctivas para adecuar la conducta a la ley, si se cuenta con la Política de Tratamiento de Datos Personales y los demás manuales requeridos, si se han atendido los requerimientos de los titulares de la información, si se ha conservado la información personal del titular bajo las medidas de seguridad adecuadas para impedir el acceso por parte de terceros no autorizados a información sensible y semiprivada, si han atendido las instrucciones y requerimientos efectuados por la Superintendencia de Industria y Comercio, y si se acreditó haber adoptado e implementado un manual de políticas de seguridad de la información, entre otras.

En este punto, es relevante preguntarse *¿Qué consecuencias conlleva aceptar o no aceptar la responsabilidad en materia de conductas vulneratorias al Régimen de Protección de Datos Personales?* Para responder a este interrogante, se plantea lo siguiente,

Acerca de allanarse o aceptar los cargos formulados.

Ante el interrogante, se observa que esto va más allá de simplemente buscar la imposición de una sanción leve, bajo la circunstancia de que se aplique el criterio atenuante de la sanción consagrado en el Literal F del Artículo 24 de la Ley 1581 de 2012.

En teoría, cuando el sujeto investigado se allana a los cargos, significa que admite su responsabilidad en relación con los delitos que se le imputan sin presentar defensa alguna. Al allanarse, el acusado reconoce su culpabilidad y se somete a las consecuencias legales. Esto puede tener impacto en la sentencia final, ya que la cooperación y el reconocimiento de la responsabilidad pueden considerarse factores atenuantes.

Bajo otra perspectiva, aceptar los cargos que se imputan en materia de infracciones a la protección de datos personales, implica un compromiso con la transparencia y la responsabilidad. Al reconocer abiertamente los errores, se demuestra un fuerte compromiso con la ética y la honestidad, lo cual tiene un impacto significativo en el fortalecimiento de la confianza, tanto de los usuarios afectados como del público en general.

En este orden de ideas, cuando los sujetos investigados, en su calidad de infractores admiten la comisión de la conducta en contra del Régimen de Protección de Datos Personales,

facilitan el proceso de investigación y sanción, agilizando el procedimiento y mostrando disposición para trabajar en conjunto con la Superintendencia de Industria y Comercio. De igual forma, la aceptación de la responsabilidad en la comisión de la conducta, es una conducta que favorece el desarrollo del proceso, pero a su vez, tiene en la graduación de la sanción.

En síntesis, aceptar la responsabilidad respecto a la infracción de una conducta que va en contra a la Ley y las disposiciones normativas, puede ser parte de una estrategia de gestión de crisis, dado que la divulgación proactiva de la infracción y la asunción de responsabilidad ayudan a mitigar los daños reputacionales. Al reconocer rápidamente el problema y tomar medidas correctivas, las empresas pueden evitar potenciales pérdidas de confianza de sus clientes. Sin embargo, la aceptación de la responsabilidad en la investigación se puede examinar desde otra perspectiva como el resultado de un análisis de costos y beneficios, puesto que, generalmente suelen ser más bajos los costos legales, en cuanto a las sanciones, adopción de medidas correctivas, que ser objeto de la imposición de sanción más drásticas.

Acerca de no aceptar los cargos formulados.

En el otro extremo, *¿Qué consecuencias conlleva no aceptar la responsabilidad en materia de conductas vulneratorias al Régimen de Protección de Datos Personales?*

Ante este interrogante, se produce la postura contraría a la aceptación expresa de los cargos, puesto que, en ocasiones los sujetos investigados, no se allanan o aceptan a los cargos imputados.

En el sistema legal colombiano, la postura procesal de aceptar los cargos imputados implica que el sujeto investigado reconoce formalmente la veracidad de los cargos presentados en su contra. A diferencia del allanamiento total, donde el acusado admite su culpabilidad sin objeciones, al aceptar los cargos imputados, se permite al individuo participar activamente en su defensa. Esta posición se caracteriza por el reconocimiento de la acusación, pero se reserva el derecho de presentar argumentos y pruebas que puedan atenuar la responsabilidad dentro del transcurso de la diligencia procesal.

Al adoptar esta postura, el acusado reconoce la necesidad de enfrentar las acusaciones de manera directa, pero también busca ejercer su derecho a la defensa. Puede ser parte de una estrategia legal para colaborar de manera limitada con el proceso, admitiendo ciertos hechos mientras argumenta que existen circunstancias atenuantes que deben tenerse en cuenta al determinar la sentencia final. En este sentido, la aceptación de los cargos imputados permite una mayor flexibilidad en la presentación de defensas, permitiendo al acusado influir en el resultado del proceso de manera más activa que un simple allanamiento.

Acerca de guardar silencio ante los cargos formulados.

La decisión de guardar silencio, es un derecho que permite al acusado abstenerse de hacer declaraciones incriminatorias durante el proceso. Este derecho se fundamenta en el principio de no autoincriminación y busca proteger al sujeto investigado de proporcionar información

que pueda perjudicarlo. Sin embargo, la falta de declaración no detiene el curso del proceso legal, y en el momento oportuno, el acusado puede presentar defensas formales, o abstenerse de hacerlo.

De conformidad con el objeto de estudio de la investigación, y en cuanto a las posturas que puede asumir el sujeto investigado frente a la responsabilidad en la comisión de las conductas en contra del Régimen de Protección de Datos Personales, se presentan las siguientes gráficas para evaluar los porcentajes y cifras obtenidas en el estudio investigativo respecto a la responsabilidad del sujeto investigado.

Responsabilidad del Sujeto Investigado.	
Descripción	**Cantidad**
Acepta la responsabilidad frente a los cargos imputados.	12
No acepta la responsabilidad frente a los cargos imputados.	31
Guardó silencio frente a los cargos imputados.	22
Total	65

Tabla No. 9 Para la Responsabilidad del Sujeto Investigado.

Gráfico No. 9 Para la Responsabilidad del Sujeto Investigado.

De la anterior información gráfica presentada, y conforme a los parámetros establecidos en el objeto de la investigación, se puede afirmar que, de acuerdo al total del número de Resoluciones objeto de estudio en la presente investigación, la postura con una mayor reincidencia es que el investigado no acepta la responsabilidad frente a los cargos imputados, con una cantidad de treinta y un (31) Resoluciones, que en términos porcentuales es el

cuarenta y ocho por ciento (48%), mientras que; la siguiente postura, en términos de mayor a menor es la situación bajo la cual el sujeto investigado guarda silencio frente a los cargos imputados, con un total de veintidós (22) Resoluciones, que en términos porcentuales representa el treinta y cuatro por ciento (34%) del total; por último, la menor cantidad de cifras obtenidas es para la aceptación de la responsabilidad frente a los cargos imputados, con un total de doce (12) y en términos porcentuales es el dieciocho por ciento (18%).

Esta información refleja ciertos patrones de comportamiento que muestran patrones claros en las posturas adoptadas por los investigados en el transcurso de la investigación. La prevalencia de la no aceptación de responsabilidad podría indicar una estrategia común de defensa entre los sujetos, quienes deciden no impugnar la validez y la veracidad de los cargos imputados. Por otro lado, se observa la baja frecuencia en la aceptación de la responsabilidad donde el bajo porcentaje sugiere que los sujetos investigados tienden a no reconocer explícitamente su responsabilidad en las conductas vulneratorias del Régimen de Protección de Datos Personales, incluso cuando se enfrentan a pruebas o cargos en su contra. Por último, la postura adoptada más común es el silencio por parte de los sujetos investigados frente a los cargos imputados, representando la mayor cantidad porcentual, esto indica que un considerable porcentaje de la muestra opta por no pronunciarse o no adoptar una posición explícita durante el proceso, en cuanto, no presenta material probatorio, no presenta escrito de descargos y/o no ejerce el derecho a la defensa lo que puede tener implicaciones legales, como aceptar los hechos que se le imputan por ciertos.

En cuanto a las medidas sancionatorias que adopta la Superintendencia de Industria y Comercio para las conductas vulneratorias por Indebido Manejo de Datos Personales.

En Colombia, el Derecho fundamental de Habeas Data, consagrado en el Artículo 15 de la Constitución Política de 1991 protege la privacidad, la intimidad personal y familiar del individuo y, confiere el derecho a cada uno de los ciudadanos de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas, lo que permite que tomen el control pleno sobre la información personal que como Titulares disponen en bases de datos manejadas por el Responsable y/o Encargado del Tratamiento. Por ello, como garantía fundamental del Derecho de Hábeas Data, el Artículo 19 de la Ley 1581 de 2012 estipula de manera literal que:

"La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley."

Es menester mencionar que la Corte Constitucional de Colombia, en línea con las prerrogativas consagradas en el Artículo 15 de la Constitución Política de Colombia de 1991 y el Artículo 19 de la Ley 1581 de 2012, se ha pronunciado al respecto de la importancia de la Protección de los Datos Personales de los titulares de la información, y la creación de la

Delegatura encargada para la protección de Datos Personales, adscrita a la Superintendencia encargada, por tanto, de manera literal, se afirma lo siguiente,

Una Delegatura para la protección de datos personales, implica la creación dentro de la estructura de la superintendencia un despacho para un Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos [...] Las superintendencias, pese a que están en el ámbito de la rama ejecutiva del poder público y dependen del Presidente de la República poseen un carácter independiente y autónomo por tratarse de organismos técnicos con autonomía administrativa y obligados a satisfacer en ejercicio de sus competencias los principios que, en los términos del artículo 209 de la Constitucional, rigen la función administrativa, características éstas que garantizan el cumplimiento de los estándares internacionales fijados sobre las autoridades encargadas de la protección de datos. (Corte Constitucional, Sala Plena, C-748,2011).

De acuerdo con lo anterior, la Delegatura para la Protección de Datos Personales es un garante del cumplimiento de las disposiciones legales y constitucionales relacionadas el Tratamiento de Datos Personales, y el manejo de ellos, en la recolección, disposición, circulación y supresión de información personal, asegurando el ejercicio pleno del Derecho fundamental de Hábeas Data y velando que las entidades Responsables y/o Encargadas del Tratamiento limiten sus actuaciones a las prerrogativas legales y constitucionales establecidas para la gestión de datos personales en el ámbito del territorio nacional.

Paralelamente, un punto crucial radica en que para hacer respetar los principios, derechos, garantías y procedimientos expuestos anteriormente; la Superintendencia de Industria y Comercio debe cumplir cabalmente con las funciones establecidas en el Artículo 21 de la Ley 1581 de 2012, que con anterioridad han sido descritas de manera individual, en el apartado del documento, que se refiere a la facultad sancionatoria de la Superintendencia de Industria y Comercio frente al Indebido Manejo de Datos Personales.

En este orden de ideas, una vez explicadas las funciones de la Superintendencia de Industria y Comercio; se puede afirmar que es la misma autoridad administrativa competente, la encargada de sancionar las conductas que presentan a lo largo y ancho del territorio colombiano por el indebido tratamiento de datos personales, es así como, el Artículo 22 de la Ley 1581 de 2012, de manera literal pone de presente el trámite para las sanciones, y estipula lo siguiente,

"Una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes."

Conforme a la anterior disposición normativa, se tiene que, la Superintendencia de Industria y Comercio, en el ejercicio de sus facultades podrá adoptar las medidas correspondientes para impartir órdenes a los Responsables y/o Encargados del Tratamiento y que con ello, adecuen sus conductas a lo establecido por la ley, así como también podrá imponer sanciones administrativas a las conductas que considere infractoras del Régimen de Protección de Datos Personales.

Adicionalmente, el Artículo 23 de la Ley 1581 de 2012, establece las sanciones que podrán ser impuestas por la Superintendencia de Industria y Comercio a los sujetos infractores de naturaleza privada.

En cuanto a las sanciones que se podrán imponer a los Responsables y/o Encargados del Tratamiento, la disposición normativa de manera literal consagra lo siguiente, a saber,

La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

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

c) Cierre 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;

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

A continuación, se abordará de manera detallada cada uno de los literales que consagran las sanciones que puede imponer la Superintendencia de Industria y Comercio en el ejercicio de su función sancionatoria contra las sociedades infractoras del Régimen de Protección de Datos Personales,

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

La Ley Estatutaria 1581 de 2012 faculta a la Superintendencia de Industria y Comercio para imponer a los Responsables y Encargados del Tratamiento sanciones de carácter pecuniario, lo que subraya la facultad sancionatoria por parte de la entidad en el ámbito de protección de datos. Las multas de carácter personal e institucional, que a su vez, pueden convertirse en sucesivas si el incumplimiento que las originó persiste en el tiempo, constituyen un mecanismo legal convincente que está destinado a garantizar el cumplimiento efectivo de las disposiciones legales del Régimen de Protección de Datos Personales. La imposición de sanciones de carácter pecuniario proporciona a la Superintendencia de Industria y Comercio una herramienta efectiva para reforzar el cumplimiento y el respeto a las normas de privacidad y protección de datos, incentivando así a las partes involucradas en el tratamiento a adoptar medidas adecuadas y evitar prácticas que puedan comprometer la seguridad y privacidad de la información personal.

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

La facultad de la Superintendencia de Industria y Comercio para suspender las actividades relacionadas con el tratamiento de datos hasta por un término de seis meses refleja la capacidad de la autoridad regulatoria para aplicar sanciones más drásticas con el objetivo de corregir y prevenir incumplimientos graves de las normas de protección de datos, que comprometen y ponen en peligro la seguridad y la privacidad de la información personal.

La imposición de la sanción correspondiente a la suspensión de las actividades relacionadas con el Tratamiento, resalta la relevancia y prontitud con que la Superintendencia de Industria y Comercio debe de abordar las conductas que generan violaciones significativas a la protección de datos personales, ofreciendo un mecanismo más drástico y directo para inducir cambios inmediatos en las conductas vulneratorias que ponen en peligro el manejo adecuado de la información personal, así como, buscar que se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley. Además, al especificar los correctivos que deben adoptarse en el acto de suspensión, la Superintendencia de Industria y Comercio proporciona una guía clara sobre las medidas necesarias que deben ser adoptadas para poner fin a la suspensión y restablecer con normalidad las operaciones, incentivando la rápida adecuación a las normas establecidas.

c) 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;

La facultad de la Superintendencia de Industria y Comercio para ordenar el cierre temporal de las operaciones relacionadas con el tratamiento de datos una vez vencido el término de suspensión sin que se hayan adoptado los correctivos indicados refleja la firmeza de la autoridad administrativa en garantizar el cumplimiento efectivo de las disposiciones legales relacionadas con la protección de datos.

El mecanismo de cierre temporal de las operaciones relacionadas con el Tratamiento representa una sanción más severa y directa que las medidas estipuladas en los numerales anteriores; que está destinada abordar las situaciones de los incumplimientos persistentes o la falta de acciones correctivas por parte de los Responsables y/o Encargados del Tratamiento.

La imposición de una sanción que involucra el cierre temporal subraya la determinación de la Superintendencia de Industria y Comercio en asegurar el respeto a las normas de privacidad y protección de datos, mostrando que las consecuencias por omisión, negligencia o violaciones graves pueden llegar a ser drásticamente significativas, incluyendo con ello, el cese temporal obligatorio de las operaciones relacionadas con el tratamiento de datos.

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

La facultad de la Superintendencia de Industria y Comercio para ordenar el cierre inmediato y definitivo de operaciones que involucren el tratamiento de datos sensibles demuestra tanto la complejidad de la situación que vulnera la seguridad, la privacidad y la protección de lo datos personales, así como la veracidad con la que la autoridad administrativa encargada aborda las violaciones relacionadas con información de especial cuidado, en cuanto contiene información sensible, que es privada y confidencial para el titular de la información.

La medida del cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles, refleja la determinación de la Superintendencia de Industria y Comercio en proteger la privacidad y seguridad de los datos sensibles, mostrando que las consecuencias por el manejo negligente o inadecuado de esta categoría de información pueden resultar en la clausura inmediata y permanente de las operaciones respectivas.

La imposición de una sanción que involucra el cierre definitivo demuestra la relevancia de esta función asignada a la Superintendencia de Industria y Comercio en cuanto a la protección de datos sensibles y la necesidad de garantizar un manejo adecuado y ético de esta información que requiere de especial cuidado.

Así las cosas, de la muestra analizada en el presente estudio de investigación, de las Resoluciones emitidas por la Superintendencia de Industria y Comercio, para el año 2022, por indebido manejo de datos personales, se obtienen los siguientes datos estadísticos que reflejen el tipo de sanciones que impuso la Superintendencia de Industria y Comercio a los Responsables y/o Encargados del Tratamiento,

Sanción impuesta por la Superintendencia de Industria y Comercio a los Sujetos Investigados.	
Descripción	**Cantidad**
Únicamente la imposición de una sanción administrativa de carácter pecuniario.	31
Sanción administrativa de carácter pecuniario y la imposición de órdenes administrativas.	34
Total	65

Tabla No. 10 Para la medida adoptada por la Superintendencia de Industria y Comercio a los sujetos investigados.

Gráfico No. 10 Para la medida adoptada por la Superintendencia de Industria y Comercio a los sujetos investigados.

De la anterior información presentada, se puede afirmar que del número de total de Resoluciones estudiadas en el objeto de la presente investigación, se obtiene como resultado que para la descripción en donde la Superintendencia de Industria y Comercio impone solamente una sanción sanción administrativa de carácter pecuniario corresponde en términos porcentuales al cuarenta y ocho por ciento (48%) de los datos obtenidos, lo que numéricamente representa treinta y un (31) resoluciones emitidas bajo esta condición, mientras que, para la descripción en donde la Superintendencia de Industria y Comercio impone una sanción administrativa de carácter pecuniario junto con la imposición de órdenes administrativas que buscan adecuar las conductas de los Responsables y/o Encargados del Tratamiento a las disposiciones consagradas en la Ley, se obtiene como resultado en términos porcentuales la cifra de cincuenta y dos por ciento (52%), que en cifras numéricas representada un total de treinta y cuatro (34) resoluciones sancionadas bajo esta condición, lo cual representa más de la mitad de los datos obtenidos.

Por otro lado, es importante resaltar que de conformidad con el estudio realizado en la presente investigación, de la muestra de sesenta y cinco (65) Resoluciones objeto del estudio, se presentan los siguientes datos relacionados con el Artículo 23 de la Ley 1581 de 2012,

Respecto al Literal A del Artículo 23 de la Ley 1581 de 2012, que consagra la imposición de multas de carácter pecuniario para los sujetos investigados por conductas vulneratorias al Régimen de Protección de Datos Personales, en su mayoría, es decir, en el contenido del número total de los actos administrativos sancionados por la Superintendencia de Industria y Comercio se adoptó la imposición de una sanción administrativa que corresponde a una multa de carácter pecuniario.

Por otro lado, en lo que respecta al Literal B del Artículo 23 de la Ley 1581 de 2012, que consagra la posibilidad de ordenar la suspensión de las actividades relacionadas con el

Tratamiento hasta por un término de seis (6) meses; en cuanto a las Resoluciones estudiadas, solamente en tres (3) de ellas se ordena esta medida, a saber,

En la Resolución 60419 de 2022, se impone a la sociedad Integral Business Center S.A.S, la orden de suspensión de las actividades relacionadas con el Tratamiento de Datos Personales por un término de tres (3) meses.

En la Resolución 63771 de 2022, se impone a la sociedad Dataset Technologies S.A.S, la orden de suspensión de las actividades relacionadas con el Tratamiento de Datos Personales por un término de seis (6) meses.

En la Resolución 51179 de 2012, se impone a la sociedad Efrata International S.A.S, la orden de suspensión de las actividades relacionadas con el Tratamiento de Datos Personales por un término de tres (3) meses.

El literal C y el literal D del Artículo 23 de la Ley 1581 de 2022 no son medidas adoptadas por la Superintendencia de Industria y Comercio en el compendio de Resoluciones analizadas.

En cuanto a la existencia de requerimiento previo por parte de la Superintendencia de Industria y Comercio a los investigados.

Durante el transcurso de las investigaciones administrativas iniciadas por la autoridad competente en cuanto a conductas vulneratorias del Régimen de Protección de Datos Personales, la Superintendencia de Industria y Comercio emitió instrucciones a través de requerimientos previos a diversas entidades Responsables y/o Encargados del Tratamiento para que particularmente adoptaran dentro del manejo de la información personal, una serie de políticas y medidas tendientes a garantizar efectivamente la privacidad, la protección y la seguridad de la información.

De ahí que, la Superintendencia de Industria y Comercio exige el cumplimiento de los deberes consagrados en el Artículo 18 y Artículo 17 de la Ley 1581 de 2012, dependiendo del caso en concreto; algunos de los requerimientos más comunes se basan en exigir a las entidades adoptar una política integral para el manejo adecuado de la información personal, adoptar políticas específicas de seguridad de la información, informar los motivos por los cuales ha cometido infracciones a los deberes que sobre él recaen, acreditar la política de Tratamiento de Datos Personales y la inscripción de sus bases de datos con información personal en el Registro Nacional de Bases de Datos-RNBD, ordenar a las entidades a cumplir con medidas de seguridad y políticas necesarias para garantizar un tratamiento correcto de la información personal en todas las etapas del ciclo de vida del dato, incluyendo la recolección, circulación y disposición final, entre otras.

A pesar de las claras directrices y exigencias por parte de la Superintendencia de Industria y Comercio, en el transcurso de la investigación, se observa que gran parte de las entidades parecen haber hecho caso omiso a los requerimientos, lo que conlleva como consecuencia la imposición de una sanción directamente relacionado con la conducta infractora.

Generalmente, una de las posibles razones para no cumplir con las órdenes e instrucciones impartidas por la Superintendencia de Industria y Comercio, es la falta de conciencia o subestimación de la importancia de contar con políticas fuertes respecto al tratamiento de datos y seguridad de la información, donde, algunas entidades pueden no haber reconocido plenamente las amenazas potenciales y las implicaciones legales de no implementar adecuadamente estas medidas, lo que evidencia a una falta de compromiso con las directrices de la Superintendencia de Industria y Comercio, lo que implica que no se adopten las medidas adecuadas para preservar la privacidad y el derecho del hábeas data del titular y protegerlo de divulgaciones no autorizadas de su información personal.

Por otro lado, otra de las posibles razones para el incumplimiento podría ser la falta de recursos, tanto financieros como de personal, necesarios para llevar a cabo las implementaciones exigidas, puesto que, las empresas pueden haber considerado que la implementación de políticas y medidas de seguridad requeriría una inversión significativa en términos de tiempo y recursos, así también, se observa que dentro de las posibilidades en cuanto a la omisión está no hacerlo dentro de los términos establecidos en la ley.

De conformidad con el parámetro de la existencia de requerimiento previo a los sujetos investigados por parte de la Superintendencia de Industria y Comercio, y atendiendo a los objetivos de la investigación, se presentan las siguientes gráficas estadísticas que evidencian los resultados obtenidos,

La existencia de requerimiento previo a la entidad por parte de la SIC.	
Descripción	**Cantidad**
Si hubo requerimiento previo a la entidad por parte de la SIC.	45
No hubo requerimiento previo a la entidad por parte de la SIC.	20
Total	65

Tabla No. 11 para la existencia de requerimiento previos a los sujetos investigados por parte de la Superintendencia de Industria y Comercio.

Gráfica No. 11 para la existencia de requerimiento previos a los sujetos investigados por parte de la Superintendencia de Industria y Comercio.

De los gráficos estadísticos presentados con anterioridad, se puede concluir que del total de las Resoluciones estudiadas en la presente investigación, un porcentaje total del sesenta y nueve por ciento (69%) evidenciaron la existencia de requerimiento previo por parte de la Superintendencia de Industria y Comercio, lo que en términos porcentuales es mucho más de la mitad, numéricamente este valor representa cuarenta y cinco (45) Resoluciones de los sesenta y cinco (65) actos administrativos que se estudiaron; este resultado refleja que aún así se requiera previamente a los Responsables y/o Encargados del Tratamiento, estos estuvieron sujetos a sanciones administrativas. Por otro lado, en cuanto a los casos donde no hubo requerimiento previo a la entidad por parte de la Superintendencia de Industria y Comercio, se obtuvo un porcentaje del treinta y un por ciento (31%) de las resoluciones analizadas, lo que numéricamente representa una cifra mucho menor, en cuanto solamente fueron veinte (20) las Resoluciones en las cuales no hubo requerimiento previo por parte de la Superintendencia de Industria y Comercio.

En cuanto a la cuantía de las Resoluciones.

En el transcurso de la investigación realizada, se observa que las sanciones impuestas por la Superintendencia de Industria y Comercio, para el año 2022, por indebido manejo de datos personales, son multas de carácter pecuniario, lo que involucra una sanción económica a los Responsables y/o Encargados del Tratamiento. Sin embargo, otro parámetro que se identifica es la existencia de casos en donde no se adopta una sanción de carácter económico, sino meramente la imposición de órdenes administrativas que involucran el cumplimiento de los deberes. Es menester mencionar que en la presente investigación solamente se encontraron actos administrativos que imponen sanciones administrativas de carácter pecuniario, por lo tanto, un criterio diferenciador es la cuantía del monto de la sanción impuesta por la Superintendencia de Industria y Comercio en cada una de las resoluciones emitidas

Se ha definido el concepto de cuantía a instancias de la Corte Constitucional de Colombia, donde se estipula que el término de cuantía se refiere al*"Costo del proceso en cuanto a lo reclamado en la petición y el valor de la diferencia entre lo reclamado y lo concedido."*(Corte Constitucional, Sala Séptima de Revisión de Tutelas, T-308, 2014).

El Artículo 25 del Código General del Proceso determina la cuantía en los procesos; de manera literal la disposición normativa consagra lo siguiente,

Cuando la competencia se determine por la cuantía, los procesos son de mayor, de menor y de mínima cuantía.

Son de mínima cuantía cuando versen sobre pretensiones patrimoniales que no excedan el equivalente a cuarenta salarios mínimos legales mensuales vigentes (40 smlmv).

Son de menor cuantía cuando versen sobre pretensiones patrimoniales que excedan el equivalente a cuarenta salarios mínimos legales mensuales vigentes (40 smlmv) sin exceder el equivalente a ciento cincuenta salarios mínimos legales mensuales vigentes (150 smlmv).

Son de mayor cuantía cuando versen sobre pretensiones patrimoniales que excedan el equivalente a ciento cincuenta salarios mínimos legales mensuales vigentes (150 smlmv).

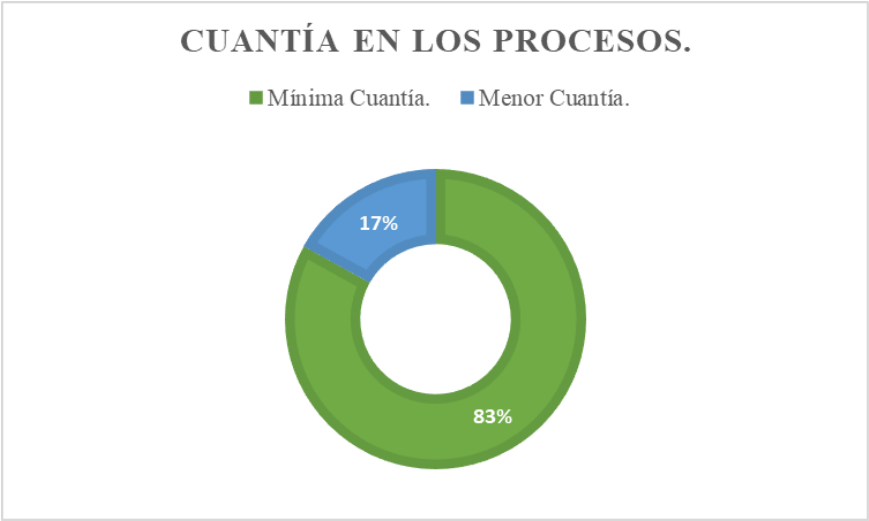
El salario mínimo legal mensual a que se refiere este artículo, será el vigente al momento de la presentación de la demanda.

En síntesis, de ideas, el Artículo 25 del Código General del Proceso clasifica los montos pecuniarios por cuantías, considerando tres tipos de ella, en cuanto, puede ser de, mínima cuantía, menor cuantía y mayor cuantía. Por otro lado, es relevante mencionar que para el año 2022, el salario mínimo legal mensual vigente era de un millón de pesos ($1.000. 000).

Dicho lo anterior, y siguiendo los parámetros del estudio de investigación, se mostrará gráficamente la cantidad de resoluciones emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de datos personales, durante el periodo comprendido entre el 01 de enero de 2022 y el 31 de diciembre de ese mismo año, atendiendo al criterio de la cuantía procesal bajo los tres tipos de diferenciación, mínima cuantía, menor cuantía y, mayor cuantía.

Cuantía.	
Descripción	**Cantidad**
Mínima Cuantía.	54
Menor Cuantía.	11
Mayor Cuantía.	0
Total	65

Tabla No. 12 para la cuantía de las Resoluciones.



Gráfica No. 12 para la cuantía de las Resoluciones.

De las anteriores gráficas estadísticas, se puede afirmar que de las sesenta y cinco (65) resoluciones emitidas por la Superintendencia de Industria y Comercio, por indebido manejo de datos personales, durante el periodo comprendido entre el 01 de enero de 2022 y 31 de diciembre de 2022, para el primer criterio, cincuenta y cuatro (54) resoluciones fueron de mínima cuantía, que en términos porcentuales refleja la mayor cantidad de actos administrativos expedidos en ese año, con un total de ochenta y tres por ciento (83%); por otro lado, para el segundo criterio diferenciador de la cuantía, únicamente once (11) resoluciones se emitieron por montos de menor cuantía; y por último, no hubo ninguna resolución sancionada bajo el parámetro de mayor cuantía.

En cuanto a los parámetros para establecer la cuantía.

Los parámetros para establecer la cuantía son criterios que utiliza la Superintendencia de Industria y Comercio para imponer y graduar la sanción atendiendo a los hechos constitutivos de la sanción, la adecuación típica en el análisis del caso, el principio de proporcionalidad que orienta el derecho administrativo sancionador y su facultad sancionatoria. Este enfoque permite emplear parámetros objetivos al momento de imponer cualquiera de las sanciones contenidas en el Artículo 23 de la Ley 1581 de 2012, para asegurar la coherencia y equidad en la imposición de sanciones, garantizando que estas sean proporcionales a la gravedad de las conductas cometidas y proporcionando así un marco normativo que promueva prácticas comerciales íntegras, la efectividad del sistema regulatorio al ofrecer un mecanismo equitativo y transparente para abordar las violaciones normativas, y el cumplimiento normativo de los principios, derechos y garantías constitucionales y legales relacionados con el Régimen de Protección de Datos Personales.

Acerca de la adecuación típica al caso en concreto.

En relación al principio de tipicidad en el derecho administrativo sancionador, la Corte Constitucional de Colombia en sentencia C-748 de 2011, ha establecido que la infracción

administrativa podrá ser aplicable a cualquiera de los casos de estudio en concreto, bajo el entendido que los hechos constituyan una vulneración al Régimen General de Protección de Datos Personales, pese a la generalidad de la ley, puesto que, si se comprueba que la conducta viola alguno de los deberes consagrados en el Artículo 17 y el Artículo 18 de la Ley 1581 de 2012, que le corresponden a los Responsables y/o Encargados del Tratamiento, habrá una adecuación típica entre los hechos generadores y la imposición de una sanción, que se enmarca en el principio de tipicidad, es decir, que la conducta que conlleva una acción u omisión se ajusta a los presupuestos detalladamente establecidos dentro de un cuerpo legal.

De manera literal, la jurisprudencia ha establecido lo siguiente en cuanto al principio de tipicidad y la adecuación típica de la conducta a la sanción que se pretende imponer,

"En relación con el principio de tipicidad, encuentra la Sala que pese a la generalidad de la ley, es determinable la infracción administrativa en la medida en que se señala que la constituye el incumplimiento de las disposiciones de la ley, esto es, en términos específicos, la regulación que hacen los artículos 17 y 18 del proyecto de ley, en los que se señalan los deberes de los responsables y encargados del tratamiento del dato". (Corte Constitucional, Sala Plena, C-748, 2011).

A saber, el Artículo 17 de la Ley 1581 de 2012 establece los deberes que le asisten a los Responsables del Tratamiento respecto del manejo de los datos personales de los titulares de la información, mientras que, el Artículo 18 de la Ley 1581 de 2012 consagra los deberes que le asisten a los Encargados del Tratamiento. De ahí que, el incumplimiento de los deberes que le asisten a cada uno según su calidad da lugar a la adopción de las sanciones descritas en el Artículo 23 de la Ley 1581 de 2012 por parte de la Superintendencia de Industria y Comercio.

Así las cosas, con la apertura de las respectivas investigaciones, ya sea de oficio por la Superintendencia de Industria y Comercio o, a petición de parte quien presenta la queja y, el acervo probatorio que reposa en el expediente de cada una de las diligencias procesales y en los actos administrativos, se puede establecer por medio de los parámetros que la conducta desplegada por el sujeto investigado se concreta en la posible vulneración de la norma, particularmente a los dispuesto en el Artículo 17 de la Ley 1581 de 2012.

En este orden de ideas, le corresponde al Despacho establecer si la conducta desplegada por cada uno de los sujetos investigados da lugar o no a la imposición de una sanción administrativa, de carácter pecuniario o en la adopción de órdenes administrativas, para lo cual se debe tener en cuenta los hechos constitutivos de la infracción que motivaron la apertura de la investigación, así como las razones de hecho y de derecho que se aducen en el transcurso del proceso, junto con las demás pruebas allegadas.

Acerca del cálculo para establecer el valor de la sanción.

Para establecer el valor de una sanción administrativa de carácter pecuniario, es decir, del Literal A del Artículo 23 de la Ley 1581 de 2023, en cuanto, la Superintendencia de Industria y Comercio dentro del ejercicio de sus funciones podrá imponer, multas de carácter personal

e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición dela sanción, se debe tener en cuenta, la disposición normativa consagrada en el Artículo 49 de la Ley 1955 de 2019, mediante la cual se expide el Plan Nacional de Desarrollo 2018-2022, que de forma literal expresa el cálculo de valores tomando como referencia la Unidad de Valor Tributario (UVT), de la siguiente manera,

A partir del 1º de enero de 2020, todos los cobros, sanciones, multas, tasas, tarifas y estampillas, actualmente denominados y establecidos con base en el salario mínimo mensual legal vigente, SMMLV, deberán ser calculados con base en su equivalencia en términos de la unidad de valor tributario, UVT. En adelante, las actualizaciones de estos valores también se harán con base en el valor de la UVT vigente.

PAR. —Los cobros, sanciones, multas, tasas, tarifas y estampillas, que se encuentren ejecutoriados con anterioridad al 1º de enero de 2020 se mantendrán determinados en SMMLV.

De conformidad con la prerrogativa consagrada en el Artículo 49 de la Ley 1955 de 2019, la manera establecida y adecuada para realizar el cálculo del valor la sanción de carácter pecuniario, atiende a la condición de que si el valor de los cobros, sanciones o multas se encuentran establecidos en salarios mínimos, como ocurre en las resoluciones objeto del presente estudio de investigación, estos deberán ser calculados con base en su equivalencia en términos de la unidad de valor tributario UVT. Por lo cual, las multas de carácter personal e institucional dispuestas en la Ley 1581 de 2012, serán determinadas por la siguiente fórmula:

$$\frac{\boldsymbol{SMMLV}}{\boldsymbol{UVT\ vigente\ 2022}} = \boldsymbol{SMMLV\ expresado\ en\ UVT'S}$$

$$\boldsymbol{SMMLV\ expresado\ en\ UVT'S} * \boldsymbol{Número\ de\ SMMLV\ a\ convertir} = \boldsymbol{Sanción\ expresada\ en\ UVT'S}$$

Acerca del principio de proporcionalidad durante el proceso administrativo sancionatorio.

Conforme al principio de proporcionalidad que orienta las actuaciones administrativas en el derecho administrativo sancionador, la Superintendencia de Industria y Comercio, en el ejercicio de sus funciones, debe ejercer la potestad sancionatoria de manera razonable y proporcionada, de manera tal que se obtenga un equilibrio entre la sanción y la finalidad que la norma vulnerada establezca, así como la proporcionalidad entre la gravedad de la infracción y la sanción aplicada.

La Corte Constitucional en Sentencia C-125 de 2003, sobre la aplicación del principio de proporcionalidad en las actuaciones administrativas del derecho administrativo sancionador, ha establecido lo siguiente,

"En cuanto al principio de proporcionalidad en materia sancionatoria administrativa, éste exige que tanto la falta descrita como la sanción correspondiente a las mismas que resulten adecuadas a los fines de la norma, esto es, a la realización de los principios que gobiernan

la función pública. Respecto de la sanción administrativa, la proporcionalidad implica también que ella no resulte excesiva en rigidez frente a la gravedad de la conducta, ni tampoco carente de importancia frente a esa misma gravedad" (Corte Constitucional, Sala Plena, C-125, 2003).

Por ello, para la correcta adecuación de los hechos constitutivos de la vulneración y la sanción aplicable, la Superintendencia de Industria y Comercio, en su calidad de encargada de la protección de datos personales en Colombia, al momento de imponer una sanción por infracción a los deberes contenidos en el Régimen de Protección de Datos Personales, debe tomar en cuenta la adecuación típica al caso en concreto, el principio de proporcionalidad, los criterios de graduación contenidos en el Artículo 24 de la Ley 1581 de 2012, y otro demás parámetros mencionados a continuación para establecer la forma en cómo se aplican al caso y, en este sentido, seleccionar y graduar la sanción que se impondrá al sujeto investigado.

Acerca de la dosificación de la sanción.

Antes de adoptar sanciones administrativas de carácter pecuniario o la imposición de órdenes administrativas, la Superintendencia de Industria y Comercio, autoridad encargada del control y vigilancia de los sujetos Responsables y/o Encargados del Tratamiento involucrados en el Régimen de Protección de Datos Personales, toma en cuenta ciertos parámetros que pueden afectar la dosificación de la sanción a imponer, lo cuales pueden ser, el tamaño de la empresa, los ingresos operacionales, el patrimonio, la información financiera y también el rol del sujeto investigado dentro del cumplimiento de la Ley de Hábeas Data.

La Superintendencia de Industria y Comercio adopta dentro de la motivación de los actos administrativos sancionatorios, los parámetros mencionados anteriormente para aplicar sanciones que resulten ser disuasorias más no confiscatorias.

La expresión correspondiente a que la *"sanción resulte disuasoria más no confiscatoria"* hace referencia a que el objetivo es imponer sanciones que tengan un carácter disuasorio, es decir, que desincentivan la comisión de acciones indebidas o infracciones, pero sin llegar a ser confiscatorias. El término disuasorio implica que la sanción busca prevenir futuras violaciones a las normativas mediante el temor a las consecuencias legales, mientras que el término no confiscatorio indica que la sanción no debe ser tan excesiva como para privar completamente al infractor de sus bienes o recursos. El objetivo es encontrar un equilibrio donde la penalización sea proporcional a la gravedad de la infracción, sin llegar a un extremo que implique una confiscación desproporcionada.

La finalidad que busca este tipo de procesos sancionatorios es promover y garantizar el cumplimiento de la Ley de Hábeas Data y, de esta forma, proteger el derecho fundamental a la protección de datos personales, pues se entiende que la vulneración del derecho fundamental a la protección de datos personales no solo afecta los derechos de una persona en particular, sino que pone en riesgo los derechos fundamentales de toda la sociedad. Por eso, las sanciones de dichas conductas no pueden ser tratadas como un asunto insignificante o de poco valor.

Acerca de los criterios para graduar las sanciones.

De conformidad con la imposición de la sanción por indebido manejo de datos personales, en el marco de la Ley 1581 de 2012, el Artículo 24 establece los criterios para graduar sanciones, lo que permite garantizar el respeto de la garantía constitucional del debido proceso consagrada en el Artículo 29 de la Constitución Política de 1991 de Colombia, que, por lo tanto, la Superintendencia de Industria y Comercio deberá analizar para cada caso en concreto y así determinar cuáles debe de tener en cuenta para ser aplicados.

Según la Corte Constitucional de Colombia en Sentencia C-748 de 2012, se refiere a cinco (05) circunstancias de agravación, entre los literales A y E del Artículo 24 de la Ley 1581 de 2012, y a una circunstancia de atenuación o disminución de la sanción, correspondiente al literal F del mismo artículo.

El Artículo 24 de la Ley 1581 de 2012, de manera literal consagra los siguientes criterios para graduar las sanciones, a saber,

Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

c) La reincidencia en la comisión de la infracción;

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

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

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

De conformidad con el objeto del presente estudio de investigación, se presenta una breve descripción conceptual para cada uno de los literales contenidos en el Artículo 24 de la Ley 1581 de 2012 en cuanto a identificar los criterios para graduar las sanciones se requiere.

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;

Este criterio implica considerar la magnitud del perjuicio o la amenaza a los derechos tutelados por las normas de privacidad y seguridad de la información, por lo tanto, es un criterio agravante de la sanción.

La relevancia de este criterio radica en la necesidad de adecuar las sanciones a la gravedad del impacto generado por las acciones de las entidades Responsables y/o Encargadas del Tratamiento de Datos Personales. La dimensión del daño o peligro a los intereses jurídicos tutelados por la ley debe ser evaluada de manera proporcionalmente a la veracidad de la

infracción, para así poder graduar en debida forma la sanción en un sentido directamente proporcional, buscando así garantizar la protección efectiva de los derechos fundamentales de los titulares de la información personal y mantener la integridad del marco legal de protección de datos personales.

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

Este criterio reconoce la importancia de evaluar si el sujeto investigado o terceros involucrados se han lucrado económicamente a raíz de la comisión de la infracción, proporcionando un criterio agravante de la sanción para aquellas conductas que obtienen un beneficio económico derivado de las prácticas irregulares.

El agravante de la sanción por obtener un beneficio económico de la comisión de la infracción para sí mismo o para terceros, busca desincentivar las prácticas irregulares e injustificadas a través de la adopción de sanciones que no solo compensen el daño causado, sino que también busca condenar las prácticas lucrativas contrarias a las normas de privacidad y seguridad de la información. Así, se promueve la idea de que las sanciones deben ser disuasivas y capaces de contrarrestar las motivaciones económicas detrás de las conductas vulneratorias al Régimen de Protección de Datos.

c) La reincidencia en la comisión de la infracción;

Este criterio evalúa si el sujeto investigado Responsable y/o Encargado del Tratamiento ha incurrido previamente en más de una ocasión en prácticas contrarias a las normas de privacidad y seguridad de la información.

La reincidencia se suele considerar como un indicador de que las medidas previas no han sido efectivas para disuadir al infractor de repetir la conducta infractora, lo que demuestra una falta de corrección, modificación y adaptación a las disposiciones legales en materia de datos personales, sugiriendo una resistencia o negligencia persistente ante el cumplimiento de las regulaciones acerca de la protección de datos personales.

En este contexto, la reincidencia es un criterio que ocasiona la imposición de sanciones más severas, reflejando la necesidad de medidas más contundentes para corregir patrones vulneratorios que con continuidad se repiten, así como sancionar cuando no se respetan o cumplen a cabalidad los requerimientos previos, la imposición de sanciones administrativas anteriores y las disposiciones legales, lo que refleja que el parámetro de la reincidencia en la comisión de la reincidencia en la comisión de la infracción es visto un criterio agravante de la sanción.

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

Este criterio resalta la importancia de la promover la colaboración y la transparencia por parte de los sujetos investigados Responsables y/o Encargados del Tratamiento y sanciona severamente las situaciones en las que una persona, entidad o empresa muestra resistencia,

negativa u obstrucción frente a las acciones de investigación o vigilancia llevadas a cabo por la Superintendencia de Industria y Comercio, lo que refleja que es un criterio agravante de la sanción.

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

La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio sugiere una resistencia directa a corregir las conductas infractoras del Régimen de Protección de Datos y el incumplimiento a las órdenes impartidas, lo que obstaculiza los refuerzos de la autoridad para garantizar el cumplimiento de las regulaciones en cuanto a la privacidad y seguridad de la información, por ello, es un criterio que agrava la sanción.

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

La declaración del sujeto investigado Responsable y/o Encargado del Tratamiento respecto al reconocimiento o aceptación expresa de la comisión de la infracción, resalta la importancia en el reconocimiento de la responsabilidad de las entidades y la cooperación proactiva con las autoridades por parte del infractor. Cuando el investigado admite abiertamente la infracción, muestra una disposición a asumir las consecuencias de sus acciones y a corregir las deficiencias identificadas en relación con la protección de datos, lo que favorece la graduación de la sanción mediante un criterio atenuante de ella.

De conformidad con el presente estudio de investigación, se presentan los siguientes gráficos estadísticos que reflejan los resultados obtenidos en cuanto a la cantidad de veces que la Superintendencia de Industria y Comercio motivó la graduación de la sanción utilizando cualquiera de los criterios para la graduación de las sanciones contenidos en el Artículo 24 de la Ley 1581 de 2012.

Criterios para graduar las sanciones.	
Descripción	**Cantidad**
Literal A del Artículo 24 de la Ley 1581 de 2012.	65
Literal B del Artículo 24 de la Ley 1581 de 2012.	0
Literal C del Artículo 24 de la Ley 1581 de 2012.	1
Literal D del Artículo 24 de la Ley 1581 de 2012.	0
Literal E del Artículo 24 de la Ley 1581 de 2012.	3
Literal F del Artículo 24 de la Ley 1581 de 2012.	12

Tabla No. 13 Para los criterios para la graduación de las sanciones.

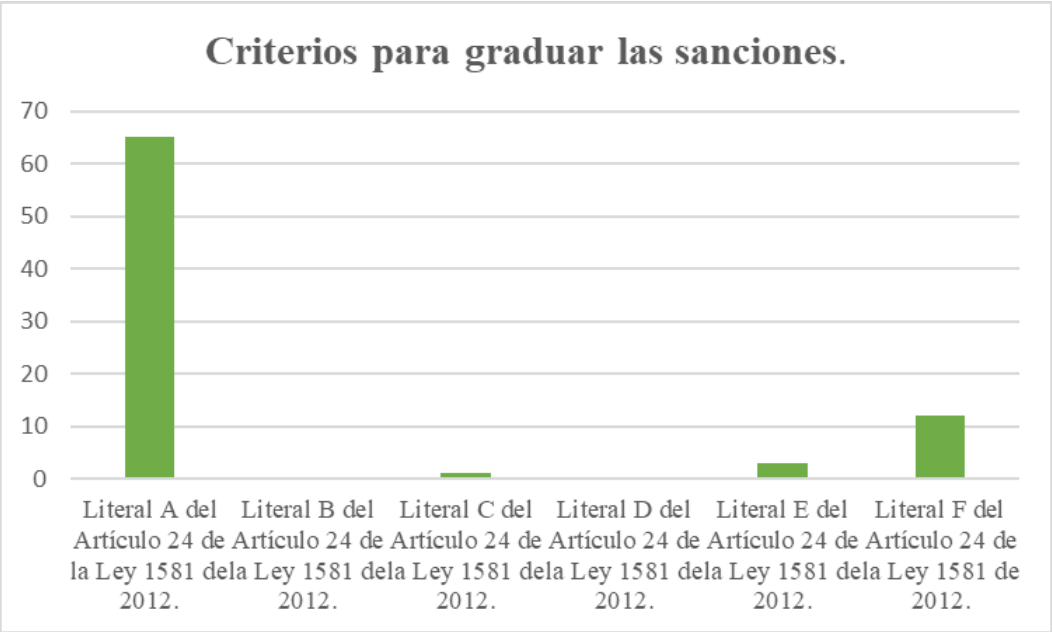


Gráfico No. 13 Para los criterios para la graduación de las sanciones.

De las anteriores gráficas que reflejan los datos obtenidos acerca de la cantidad de veces que se aplicaron los criterios para graduación de las sanciones contenidos el Artículo 24 de la Ley 1581 de 2012 se puede afirmar que del número total de la muestra analizada, es decir, sesenta y cinco (65) resoluciones emitidas por las Superintendencia de Industria y Comercio, por indebido manejo de datos personales, durante el periodo comprendido entre el 01 de enero de 2022 y 31 de diciembre de 2022, se puede afirmar que para el Literal A que corresponde al primer criterio de graduación, en sesenta y cinco (65) resoluciones se aplicó éste, que en términos porcentuales refleja el cien por ciento (100%); por otro lado, el Literal B y el Literal D no sé aplicó en ninguna de las resoluciones emitidas, el Literal C se fijó en una (01) sola resolución, el Literal E solo en tres (3) resoluciones, y el literal F en doce (12) resoluciones.

Por otro lado, se observa que, sin distinción alguna, en un solo acto administrativo se pueden aplicar varios de los literales consagrados en el Artículo 24 de la Ley 1581 de 2012, en cuanto los hechos constitutivos de la infracción pueden involucrar un número plural de criterios para graduar la sanción, y considerar si se adoptan medidas agravantes o atenuantes al momento de ajustar el monto de la sanción.

Conclusión

A continuación, el Capítulo Número tres (03) que presenta las conclusiones obtenidas en la investigación, a saber,

Que, el presente capítulo refleja las conclusiones de investigación obtenidas por los estudiantes en el transcurso de la investigación del trabajo de grado.

Que, en el transcurso de la presente investigación se recopiló la información relevante contenida en las resoluciones emitidas por la Superintendencia de Industria y Comercio en el periodo comprendido entre e1 01 de enero de 2022 y 31 de diciembre de ese mismo año, por indebido manejo de datos personales; dicha información se recolectó bajo parámetros de análisis previamente establecidos, lo que permitió la elaboración de las respectivas fichas de investigación para cada una de las resoluciones. Estas fichas constituyen la muestra objeto de estudio del proyecto de grado, que representa el primer capítulo de la investigación

Que, después de obtener los datos plenamente compilados, se elaboró el segundo capítulo a través de un análisis cuantitativo y cualitativo de los resultados obtenidos, con la intención de determinar los parámetros objetivos que utiliza la Superintendencia de Industria y Comercio para sancionar a los Responsables y/o Encargados del Tratamiento, particularmente, por indebido tratamiento de datos personales durante el proceso administrativo sancionatorio. Dentro de este capítulo, se incluyen conclusiones de investigación derivadas de los datos estadísticos obtenidos para cada uno de los parámetros objetivos analizados a través de ellos, lo que proporciona al lector una visión integral de las condiciones de la investigación.

Que, la Superintendencia de Industria y Comercio es la autoridad nacional encargada de velar por el cumplimiento de la legislación en materia de protección de datos personales, por ello, bajo el ejercicio de su facultad sancionatoria, se encuentran las resoluciones objeto de la presente investigación, en consideración a que reflejan los aspectos fundamentales al tema central del proyecto de grado, es decir, las conductas vulneratorias del Régimen de Protección de Datos Personales.

Que, la Superintendencia de Industria y Comercio debe de asegurarse a través de procesos de inspección, control, supervisión y vigilancia de que las organizaciones limiten su actuar de conformidad con las normativas establecidas en la legislación vigente; así las cosas, tiene la facultad de investigar y sancionar a los Responsables y/o Encargados del Tratamiento, cuando en el ejercicio de sus funciones transgreden las disposiciones legales relacionadas con la protección de datos, asegurando de esta forma que adecuen su actuar a las prerrogativas establecidas en la ley para que cumplan con los deberes que les conciernen en relación a su calidad y se respeten los derechos fundamentales de los ciudadanos en el manejo de su información personal.

Que, una vez mencionada la función de la Superintendencia de Industria y Comercio, en el transcurso de la investigación, se observan ciertas conductas vulneratorias del Régimen de Protección de Datos Personales por las cuales la Superintendencia de Industria y Comercio

en el ejercicio de sus funciones, sanciona en mayor medida a las entidades Responsables y/o Encargados del Tratamiento.

Que, las sanciones impuestas a los Responsables y/o Encargados del Tratamiento están destinadas específicamente a conductas que transgreden los principios, derechos y garantías constitucionales y legales enfocados a salvaguardar la privacidad y la seguridad de la información personal de los individuos. Algunas de las conductas vulneratorias que representan un mayor índice de infracción son, la recolección no autorizada de los datos personales, la divulgación indebida y no autorizada de la información personal del titular, el tratamiento de datos sin contar con la autorización previa, expresa e informada del titular, la falta de implementación de medidas adecuadas de seguridad, no atender las consultas y reclamaciones de los ciudadanos, no atender las instrucciones y requerimientos de la Superintendencia de Industria y Comercio.

Que, después de analizar a detalle el contenido de cada una de las resoluciones objeto del estudio de investigación, se concluye que los procesos administrativos pueden iniciarse de dos formas, de oficio o a petición de parte; generalmente en el primer escenario, la Superintendencia de Industria y Comercio antes de imponer las respectivas sanciones realiza previamente requerimientos al sujeto investigado, a fin de que implemente las órdenes e instrucciones que se requieren para el cumplimiento de las disposiciones en materia de protección de datos, sin embargo, la cantidad de veces que la entidad inició la investigación fue menor en comparación con el segundo escenario, donde se observa que supera numéricamente a la otra condición, y es mayor la cantidad de ocasiones donde un ciudadano eleva una queja ante esta Superintendencia siempre y, cuando haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

Que, en relación a que el objetivo central de la investigación es establecer si la Superintendencia de Industria y Comercio utiliza parámetros objetivos para motivar la imposición de las sanciones administrativas por indebido manejo de datos personales, se puede afirmar que en el transcurso de la investigación se observa minuciosamente cómo esta Superintendencia motiva a detalle cada uno de los actos administrativos de manera razonable e imparcial atendiendo a parámetros objetivos, indicadores precisos y directrices puntuales en cada una de ellas para la adecuación típica de la norma a los hechos constitutivos de la infracción , como lo son,

Que, la Superintendencia de Industria y Comercio considera la calidad del sujeto investigado, en relación a si es Responsable y/o Encargado del Tratamiento. Por ello, distinguir la calidad de cada uno de los sujetos investigados, entre Responsables y/o Encargados del Tratamiento de Datos Personales, es un criterio que contribuye al momento de aplicar las sanciones administrativas a que haya lugar, lo cual, le permite a esta superintendencia imponer las sanciones consagradas en el Artículo 23 de la Ley 1581 de 2012, de forma adecuada, justa y proporcional, atendiendo criterios objetivos, como la adecuación típica, el principio de tipicidad, el principio de proporcionalidad, la valoración cuantitativa de la sanción, de acuerdo con las disposiciones legales de protección de datos personales, pues esto refleja que esta superintendencia comprende los diferentes roles dentro de la protección de datos, y que cada una de los hechos constitutivos de la infracción, según corresponda, deben adecuarse a la infracción a los deberes del Artículo 17 y Artículo 18 de la Ley 1581 de 2012.

Que, en el transcurso de la investigación, se observa que la Superintendencia de Industria y Comercio considera las distintas clasificaciones que pueden tener los datos personales, toda vez que no es posible valorar en la misma forma, las infracciones cometidas a un dato de carácter público, que a un dato que tenga las características de dato semiprivado, dato, privado y/o dato sensible, puesto que al momento de imponer las sanciones respectivas es crucial y fundamental reconocer que la sensibilidad, la privacidad, la seguridad, y la protección de la información son aspectos variables, según corresponda. Esta superintendencia comprende que no todas las infracciones tienen el mismo impacto, diferenciando así entre las diversas acepciones que pueden tener los datos personales, pues en términos generales, aquellas infracciones que involucran datos sensibles y/o privados, están en una escala de mayor grado de confidencialidad y las posibles vulneraciones pueden ser objeto de sanciones más drásticas debido al mayor riesgo de afectación a la privacidad y derechos fundamentales del titular de la información, lo que evidencia una relación directamente proporcional entre el hecho constitutivos de la sanción y la sanción impuesta.

Que la Superintendencia de Industria y Comercio, para determinar la conducta vulneratoria del Régimen de Protección de Datos Personales, encaja los hechos constitutivos de la infracción según corresponda la calidad del sujeto investigado a la infracción material de los deberes consagrados en la Ley 1581 de 2012, atendiendo a los criterios de adecuación típica, el principio de proporcionalidad y el principio de tipicidad.

La adecuación típica de la conducta a las disposiciones normativas consagradas en la Ley permite a esta Superintendencia evaluar de manera integral la conducta vulneratoria. Esto implica un análisis detallado de la gravedad y magnitud de la infracción, al mismo tiempo que verifica si los hechos constitutivos de la sanción determinan el incumplimiento de los deberes establecidos en las normas de protección de datos. El principio de adecuación típica asegura que la sanción se aplique conforme a los parámetros legales de la infracción, mientras que el principio de proporcionalidad garantiza que la sanción sea justa y equitativa en relación con la gravedad de la falta.

Queda demostrado que la Superintendencia de Industria y Comercio, en el transcurso del proceso de investigación a los sujetos investigados, examina el reconocimiento de la responsabilidad, respecto a la aceptación, no aceptación y/o guardar silencio frente a las conductas vulneratorias del Régimen de Protección de Datos Personales, lo que en parte influye en la adecuación de la sanción al momento de adecuar los hechos constitutivos de la sanción a la graduación de la sanción a través de los criterios para graduar las sanciones contenidos en el Artículo 24 de la Ley 1581 de 2012.

Que, en el transcurso de la investigación, se observa cómo la Superintendencia de Industria y Comercio, antes de imponer una sanción administrativa de carácter pecuniario en el marco del proceso administrativo sancionatorio, considera diversos parámetros objetivos para su graduación, entre ellos, el tamaño de la empresa, los ingresos operacionales, la dosificación de la sanción, así como criterios agravantes y atenuantes. Estos elementos son cruciales para asegurar que la cuantía de las sanciones sea proporcionada tanto a la gravedad del incumplimiento como a la capacidad económica de la entidad sancionada.

Que para establecer la cuantía de los valores monetarios de la sanciones administrativas de carácter pecuniario, esta superintendencia aplica la fórmula matemática contenida en el Artículo 49 de la Ley 1955 de 2019; esto proporciona un enfoque objetivo y consistente en la imposición de sanciones. Además, la imposición de medidas administrativas, como órdenes, instrucciones y requerimientos, se determina de acuerdo con la gravedad de los hechos constitutivos de la sanción, asegurando que estas medidas sean proporcionales y directamente relacionadas con la magnitud de la infracción que se adaptada a las circunstancias específicas de cada caso en particular.

Se logra evidenciar que esta superintendencia no adopta sanciona de manera subjetiva o arbitraria, por el contrario, se fundamenta en parámetros específicos, que han sido identificados a través del análisis cuantitativo y cualitativo detallado de sesenta y cinco (65) resoluciones emitidas por la SIC durante el periodo comprendido entre el periodo comprendido entre el 01 de enero de 2022 y 31 de diciembre de ese mismo año. Estos parámetros como el tamaño de la empresa, los ingresos operacionales y los criterios agravantes o atenuantes, proporcionan una base objetiva y consistente para calcular la magnitud de las sanciones. La revisión minuciosa de estas resoluciones permite establecer un marco claro y transparente que guía la imposición de sanciones, asegurando que estas sean proporcionales a la gravedad de las infracciones y evitando cualquier arbitrariedad en el proceso administrativo sancionatorio.

Por último, cabe resaltar que la Superintendencia de Industria y Comercio centra sus esfuerzos en la salvaguarda de los derechos de los titulares y en el cumplimiento integral del régimen general de protección de datos personales. Al desempeñar correctamente la función de control, inspección y vigilancia, la Superintendencia de Industria y Comercio se posiciona como un ente regulador comprometido con la protección de la integridad de la información personal. Su enfoque se dirige hacia la garantía de que las entidades sujetas a su supervisión respeten rigurosamente las normas establecidas, asegurando así el resguardo de los derechos fundamentales de los individuos en el tratamiento de sus datos. Este compromiso refleja la importancia que esta superintendencia asigna a la protección de la privacidad y seguridad de la información, en donde se pueda crear un entorno digital en el que los ciudadanos confíen en el manejo adecuado de su información personal.

Bibliografía

Argote, C. A. (2021, 12 diciembre). Conozca la protección del Habeas Data y las sanciones por el mal uso de datos personales. https://www.asuntoslegales.com.co/consumidor/conozca-la-proteccion-del-habeas-data-y-las-sanciones-por-el-mal-uso-de-datos-personales-3275456.

Angarita, N. R. (2010, 15 mayo). *¿TIENE COLOMBIA UN NIVEL ADECUADO DE PROTECCIÓN DE DATOS PERSONALES a LA LUZ DEL ESTÁNDAR EUROPEO?* https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/13847

Constitución Política de Colombia [Const]. Art. 15. 20 de julio de 1991 (Colombia).

Corte Constitucional, Sala Tercera de Revisión, sentencia 09 de septiembre de 1992, exp T-3999.

Corte Constitucional, Sala Primera de Revisión, sentencia de 1993, exp T - 4452.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia del 6 de febrero de 1997, exp D-1350

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia del 16 de mayo de 2000, exp D-2573

Corte Constitucional, Sala Quinta de Revisión, sentencia 30 de octubre de 2002, exp. T-591639.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia del 18 de febrero de 2003, exp D-4059.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia 18 de agosto de 2004, exp D-5025.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia 16 de octubre de 2008, exp PE-029.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia del 29 de octubre de 2009, exp. D- 7607.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia 28 de enero de 2009, exp. D-7290.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia del 2010, exp. D-7999.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia del 06 de octubre de 2011, exp. PE- 032.

Corte Constitucional, Sala Segunda de Revisión, sentencia 31 de mayo de 2012, exp T-3.348.314.

Corte Constitucional, Sala Plena, sentencia 09 de mayo de 2013, exp PE-036.

Corte Constitucional, Sala Séptima de Revisión de Tutelas, sentencia 28 de mayo de 2014, exp T- 4.203.808

Corte Constitucional, Sala Octava de Revisión, sentencia 20 de abril de 2015, exp T-4.609.989.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia 02 de noviembre de 2016, exp D-11332.

Corte Constitucional, Sala Tercera de Revisión, sentencia 14 de septiembre de 2017, exp T-6.142.741.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia 03 de marzo de 2020, exp. D-11902.

Corte Constitucional, Sala Plena de la Corte Constitucional, sentencia 14 de mayo de 2021, exp. T-8.004.793.

Corte Constitucional, Sala Octava de Revisión de tutelas, sentencia 8 de agosto de 2022, exp T-8.624.281.

Delimitación conceptual del principio de objetividad: objetividad, neutralidad e imparcialidad. (2011). *Documentación Administrativa*. https://dialnet.unirioja.es/servlet/articulo?codigo=4409606

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. 27 de junio de 2013.

Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. 13 de mayo de 2014

Decreto 1074 de 2015. Por medio del cuál se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. 26 de mayo de 2015.

Galvis Cano, L. y Salazar Bautista, R. (2018). Alcance del derecho al olvido en el tratamiento de datos personales en Colombia. Revista Verba Iuris, 14 (41). pp. 45-63

Gonzalez, P. (2023, 25 mayo). ¿Cuáles son las infracciones a la Ley de Datos Personales? Primicias.https://www.primicias.ec/noticias/economia/multas-datos-personales/

Gobernación del Valle del Cauca. (s. f.). Política de privacidad, tratamiento y protección de bases de datos. Ogpt.valledelcauca.gov.co. Recuperado 29 de noviembre de 2023, de https://ogpt.valledelcauca.gov.co/politica-proteccion.

Ley Estatutaria 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. 31 de diciembre de 2008. D.O. No. 47.219.

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 18 de octubre de 2012. D.O. No. 48.587.

Ley Estatutaria 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. 6 de marzo de 2014. D.O. No. 49.084.

Ley 1955 de 2019. Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. 25 de mayo de 2019. D.O No. 50.964.

Ordoñez, D. (2014). La protección judicial de los derechos en internet en la jurisprudencia europea. España.

OEA. (2022). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.file:///C:/Users/a/Downloads/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Perdigon Correa, L., & Cinfuentes Acosta, A. (2016). Protección de datos en Colombia y su posible afectación por terceros [Tesis para optar por Postgrado en derecho administrativo]. Universidad de la Gran Colombia.

Resolución 8862 de 2010. Por la cual se dictan las disposiciones para registrar bases de datos ante la SIC. 28 de octubre de 2010.

Real Academia Española. (2023). Parámetro. En Diccionario de la lengua española. https://dle.rae.es/par%C3%A1metro?m=form&m=form&wq=par%C3%A1metro

Real Academia Española. (2023). Sanción. En Diccionario de la lengua española. https://dle.rae.es/sanci%C3%B3n?m=form&m=form&wq=sanci%C3%B3n

Riande, Noé. (S.F). El derecho a la autodeterminación informativa. https://www.tfja.gob.mx/investigaciones/historico/pdf/elderechoalaautodeterminacion.pdf

Superintendencia de Industria y Comercio. (2021). Manejo de información personal «habeas data». Www.sic.gov.co. Recuperado 29 de noviembre de 2023, de https://www.sic.gov.co/manejo-de-informacion-personal.

Superintendencia de Industria y Comercio. (2023). Guía Oficial de Protección de Datos Personales: Manual de la Superintendencia de Industria y Comercio. Www.sic.gov.co. file:///C:/Users/a/Downloads/Guia%20de%20datos%202023%20(2)%20SIC.pdf

Superintendencia de Industria y Comercio. (S.F). Aspectos básicos sobre el Derecho de Hábeas Data. Cartilla protección de datos personales. https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf

Superintendencia de Industria y Comercio. (S.F). Manejo de la información personal, "Habeas data". https://www.sic.gov.co/manejo-de-informacion-personal#:~:text=En%20ese%20sentido%2C%20la%20SIC,que%20se%20hagan%20por%20escrito%2C

Universidad de los andes. Quejas protección datos personales Colombia | Uniandes. (s. f.). https://derecho.uniandes.edu.co/es/cada-d%C3%ADa-en-Colombia-se-presentan-cerca-de-79-casos-de-violacion-de-proteccion-de-datos-personales#:~:text=de%20datos%20personales-,Cada%20d%C3%ADa%2C%20en%20Colombia%20se%20presentan%20cerca%20de%2079%20casos,de%20protecci%C3%B3n%20de%20datos%20personales&text=En%202021%2C%20la%20SIC%20recibi%C3%B3,Ley%20Estatutaria%201266%20de%202008.