Un análisis comparativo del Reglamento (UE) 2016/679 Del Parlamento Europeo y Del Consejo y la Ley 1581 de 2012 Frente a los incidentes de seguridad de la información en el tratamiento de datos personales.

AUTOR

Miguel Ángel Rojas Campo

Trabajo de grado para optar por el título de Maestría en Derecho Empresarial de la Pontificia Universidad Javeriana Cali.

TUTOR

Luis Félix Barriga

PONTIFICIA UNIVERSIDAD JAVERIANA CALI

FACULTAD DE HUMANIDADES Y CIENCIAS SOCIALES

PROGRAMA DE MAESTRÍA EN DERECHO EMPRESARIAL

CALI, VALLE DEL CAUCA

13.08.2025

Un análisis comparativo del Reglamento (UE) 2016/679 Del Parlamento Europeo y Del Consejo y la Ley 1581 de 2012 Frente a los incidentes de seguridad de la información en el tratamiento de datos personales.

Miguel Ángel Rojas Campo[1].

RESUMEN

Colombia enfrenta crecientes desafíos en la protección de los datos personales frente a incidentes de seguridad; especialmente en un entorno empresarial donde el uso intensivo de tecnologías ha incrementado la exposición a ataques cibernéticos o en palabras de los profesores Adolfo García Arreola (2019) y Machuca Vivar, Silvio Amable; Vinueza Ochoa, Nelly Valeria; Sampedro Guaman, Carlos Roberto y Santillan Molina, Alberto Leonel. (2022) se ha denotado un incremento en el riesgo del manejo de la información y el tratamiento de datos personales. La insuficiencia del marco legal colombiano actual para responder eficazmente a estos incidentes plantea la necesidad de revisar su régimen normativo. Esta investigación adopta una metodología cualitativa de tipo jurídico comparado, orientada a comprender críticamente el régimen sancionatorio aplicable en casos de incidentes de seguridad en el tratamiento de datos personales. El objetivo general es Identificar las semejanzas y diferencias normativas entre el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) y la Ley 1581 de 2012 en relación con los incidentes de seguridad de la información de datos

[1] Egresado de la carrera de derecho de la Pontifica Universidad javeriana Cali, Especialista en Derecho Comercial de la misma Universidad, estudiante de la Maestría en Derecho Empresarial de la misma Universidad. Con experiencia en Derecho Comercial, Societario, Financiero, Civil y Procesal.

personales. Entre los principales hallazgos, se identifican vacíos normativos en plazos de notificación, mecanismos de transferencia internacional de datos y criterios sancionatorios, lo cual contrasta con la estructura más robusta y coherente del Reglamento General De Protección De Datos.

Key Words: Tratamiento de datos personales; Cultura de datos; Incidente digital, Seguridad de la información.

Introducción

En la actual economía digital que algunos autores denominan la quinta revolución industrial[2], los datos personales se han consolidado como uno de los activos más valiosos para las organizaciones, siendo utilizados intensivamente en actividades comerciales, tecnológicas y de servicios. Este fenómeno ha traído consigo no solo oportunidades de desarrollo económico, sino también riesgos asociados a la seguridad de la información y al tratamiento indebido de dichos datos. En este contexto, los incidentes de seguridad —entendidos como eventos que comprometen la confidencialidad, integridad o disponibilidad de los datos personales, por un acceso, intento de

[2] Taj, I., & Zaman, N. (2022). Towards industrial revolution 5.0 and explainable artificial intelligence: Challenges and opportunities. International Journal of Computing and Digital Systems.

acceso, uso, divulgación, modificación o destrucción no autorizada de información[3]— se han convertido en una de las principales preocupaciones regulatorias tanto para las autoridades como para los responsables del tratamiento. La capacidad de los marcos jurídicos nacionales para prevenir, gestionar y sancionar dichos incidentes representa un indicador crítico de madurez normativa en materia de protección de datos personales.

En el ámbito internacional, el Reglamento (UE) 2016/679 Del Parlamento Europeo y Del Consejo (RGPD) se ha consolidado como el modelo normativo más robusto e influyente en materia de protección de datos personales. Su enfoque integral no solo establece estándares elevados de cumplimiento para responsables y encargados del tratamiento, sino que también introduce mecanismos detallados de notificación de incidentes, así como un régimen sancionatorio riguroso, proporcional y disuasivo. En contraste, el marco colombiano, centrado en la Ley 1581 de 2012[4], aún se encuentra en proceso de evolución y consolidación frente a los retos contemporáneos de la economía digital, particularmente en lo relacionado con la respuesta a incidentes de seguridad y la efectividad de las sanciones impuestas por la autoridad nacional de protección de datos: la Superintendencia de Industria y Comercio (SIC).

Por lo anterior, se identifica la necesidad de analizar las semejanzas y diferencias normativas que existe el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) y la Ley 1581 de 2012 frente a los incidentes de seguridad de la información. Este análisis no es menor, si se considera que los incidentes de seguridad generan afectaciones directas a los derechos

[3] Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Disponible en https://gobiernodigital.mintic.gov.co/692/articles-237908_maestro_mspi.pdf

[4] Congreso de la república. Ley 1581 de 2012.

fundamentales de los titulares, como el habeas data y la intimidad[5], así como impactos significativos en la reputación y viabilidad económica de las organizaciones involucradas.

Ahora bien, una vez mencionado lo anterior, se procederá a desarrollar el presente proyecto de investigación de la siguiente manera: **(i)** Estudia el marco jurídico colombiano en materia de incidentes de seguridad de la información de datos personales y algunas de sus sanciones más representativas; **(ii)** Examinar el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) en materia de incidentes de seguridad de la información de datos personales y algunas de sus sanciones más representativas; **(iii)** Analizar los resultados del estudio del marco jurídico colombiano y el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) en materia de incidentes de seguridad de la información de datos personales y algunas de sus sanciones más representativas.

(i) **Estudiar el marco jurídico colombiano en materia de incidentes de seguridad de la información de datos personales y algunas de sus sanciones más representativas.**

Los datos personales en el marco jurídico colombiano, como lo menciona el profesor Diego Andrés Miranda (2023)[6], involucran la interacción de tres componentes (A) El derecho a la Intimidad; (B) El habeas Data y (C) La protección de datos personales; pues en el marco de los compromisos adquiridos tras la adhesión de Colombia a la OCDE y como consecuencia de la apertura económica y globalización, se consagró por medio de la constitución política de Colombia de 1991 el principio de la dignidad humana y se reconoció el derecho fundamental al Hábeas Data, en concordancia

[5] Corte Constitucional de Colombia. sentencia SU139/21. MP. JORGE ENRIQUE IBÁÑEZ NAJAR; Corte Constitucional de Colombia. T-143/22. MP. ALEJANDRO LINARES CANTILLO.
[6]Miranda, Diego Andrés. (2023, 17 octubre). Los Datos Personales y su regulación en Colombia (datos sensibles, datos públicos, semiprivado y privado)

a esto se expidieron normas clave en materia de protección de datos personales, entre ellas la Ley 1266 de 2008, la Ley 1581 de 2012 y sus respectivos decretos reglamentarios.

Es importante mencionar que en materia de tratamiento de datos personales el desarrollo constitucional se puede evidenciar desde la implementación del artículo 15[7] de la Constitución Política de Colombia, por medio del cual se desarrolló el derecho al Habeas Data, la intimidad y el buen nombre reconocido por medio de la sentencia T-552 de 1997[8] , por medio del cual se denota claramente que el derecho a la intimidad consiste en no obligar a ser visto o escuchado a quien no quiera serlo, situación de la cual se deriva esencialmente el correcto tratamiento de datos personales. En igual sentido expresó la Corte Constitucional por medio de sentencia T-277 de 2015[9] y T-050 de 2016[10], lo relativo a los derechos de dignidad, buen nombre y a la intimidad, pues por medio de la jurisprudencia indicada, se analizan casos de solicitud de eliminación de información, de prevalencia del derecho a la intimidad y la dignidad sobre la libertad de publicación de información.

Aunado a lo anterior, por medio del artículo 20[11] constitucional, se contempla lo relacionado al derecho de libertad de información, ya sea de la recepción o divulgación de la misma siempre que sea veraz e imparcial, pues tal categoría e importancia ha sido reconocida jurisprudencialmente por las sentencias SU139/21[12]; T-143/22[13].

Por lo anterior, se puede observar que el desarrollo y regulación constitucional sobre el tratamiento de datos personales no ha sido reciente, sino que, el mismo tiene un origen inicial desde la

[7] Constitución política de Colombia. Artículo 15. Derecho al habeas data – Intimidad y buen nombre.
[8] Corte Constitucional de Colombia. MP. VLADIMIRO NARANJO MESA.
[9] Corte Constitucional de Colombia. MP. MARÍA VICTORIA CALLE CORREA.
[10] Corte Constitucional de Colombia. MP. GABRIEL EDUARDO MENDOZA MARTELO.
[11] Constitución política de Colombia. Artículo 20. Derecho libertad de información.
[12] Corte Constitucional de Colombia. MP. JORGE ENRIQUE IBÁÑEZ NAJAR.
[13] Corte Constitucional de Colombia. MP. ALEJANDRO LINARES CANTILLO.

constitución de 1991, reflejando un desarrollo progresivo en esta materia. Ahora bien, una vez analizada la categoría constitucional del tratamiento de datos personales, es importante mencionar que en Colombia, el desarrollo legal se puede evidenciar por medio de: la Ley 1266 de 2008, por medio de 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*"; La Ley 1581 de 2012 por medio de la cual "*se dictan disposiciones generales para la protección de datos personales*"; El Decreto 1377 de 2013, por medio del cual "*se reglamenta parcialmente la Ley 1581 de 2012*", compilado en el decreto 1074 de 2015 "*por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo*".

Previo a la promulgación de la Ley 1581 de 2012, se agotó el respectivo control de constitucionalidad[14] cuando se encontraba en la fase de proyecto de Ley, control realizado por medio de la Sentencia C-748 de 2011[15], por medio de la cual se aprobó el contenido del proyecto de Ley, analizando los principios rectores en esta materia, verificando si los mismos cumplían con los tratados internacionales y principios generales reconocidos previamente por medio jurisprudencial, inclusive llegando a analizar los principios derivados, como lo fue el principio de prohibición de discriminación por las informaciones recaudadas en las bases de datos, el principio de interpretación integral de los derechos constitucionales y la obligación de indemnizar ante

[14] Constitución Política de Colombia. Artículo 241: "A la Corte Constitucional se le confía la guarda de la integridad y supremacía de la Constitución, en los estrictos y precisos términos de este artículo. Con tal fin, cumplirá las siguientes funciones:
(…)
8. Decidir definitivamente sobre la constitucionalidad de los proyectos de ley que hayan sido objetados por el Gobierno como inconstitucionales, y de los proyectos de leyes estatutarias, tanto por su contenido material como por vicios de procedimiento en su formación.
(…)"

[15] Corte Constitucional de Colombia. Sentencia C-748/2011. MP. JORGE IGNACIO PRETELT CHALJUB.

eventuales perjuicios causados. Esta sentencia es relevante en los incidentes de seguridad en el tratamiento de datos personales, pues por medio de al misma fue que se dio origen a la discusión de la Ley 1581 de 2012, ley precursora en materia de tratamiento de datos personales.

La Ley 1581 de 2012 aborda el tratamiento de datos personales, de una manera amplia, pues expone desde principios rectores en el tratamiento de datos personales, como lo son los contenidos en el titulo II, dentro de los cuales se considera importante resaltar el principio de transparencia, consistente en el derecho que tiene el titular a conocer en cualquier tiempo y momento del encargado o responsable del tratamiento la información que se tiene sobre sus datos personales; El Principio de seguridad, consistente en que al información sometida a tratamiento deberá de ser manejada con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad, evitando adulteración, perdida, entre otras; Principio de acceso y circulación restringida, consistente en que el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, por lo cual, el tratamiento únicamente se podrá realizar por personas autorizadas por el titular o por la Ley 1581 de 2012, conllevando igualmente que la información que no sea pública, deba restringirse su acceso, y por ende no se publicada en internet, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido a los titulares o autorizados por el titular.

Pese a evidenciarse varios principios rectores contenidos en la Ley 1581 de 2012, estos principios se consideran los más relevantes para el presente estudio, pues se encuentran estrechamente ligados con los incidentes de seguridad de la información en el tratamiento de datos personales, pues en caso de presentarse un incidente de seguridad en el tratamiento de datos personales se vulnera de manera directa los principios antes mencionados.

Continuando con el análisis del marco jurídico Colombiano en cuanto a los incidentes de seguridad en el tratamiento de datos personales es importante mencionar que por medio de la Ley 1581 de 2012, en especifico por medio de su artículo 27 se desarrollan las normas corporativas vinculantes, indicando que, el gobierno expedirá la reglamentación correspondiente sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales, y su transferencia a terceros países, situación última que será desarrollada más adelante del presente escrito.

Las normas corporativas vinculantes son importante en el tratamiento de datos personales, pues las mismas son las que regularán la protección de datos personales dentro de un grupo empresarial, por lo cual, en aras de regular estas normas vinculantes se promulgó el decreto 255 de 2022, por medio del cual se establecieron las condiciones mínimas de las normas corporativas vinculantes, entre ellas las garantías y mecanismos de protección de datos que deben ofrecerse, así como el procedimiento para autorizarlas, para la obtención de la certificación de buenas prácticas, normas que una vez reconocidas serán de obligatorio cumplimiento para el grupo empresarial.

Ahora bien, dentro del desarrollo normativo antes mencionado, no se establecen criterios de análisis o gestión del riesgo ante incidentes de seguridad en el tratamiento de datos personales, situación que si se puede identificar claramente por medio de la guía realizada por la Superintendencia de Industria y comercio en el año 2020, para tal fin, por medio de la cual se indica que además de la gestión de un incidente de seguridad en el tratamiento de datos personales se debe contar con el principio y el deber de seguridad, el cual tiene un criterio eminentemente preventivo, por lo cual, se evidencia la necesidad y relevancia de la adecuada preparación en la etapa previa al acaecimiento del incidente.

En la guía en mención la Superintendencia de Industria y Comercio menciona que la gestión de los incidentes de seguridad debe ser desde: (A) El diseño de las actividades del tratamiento; (B) El complemento de Las políticas de seguridad de la información y protección de datos y (C) La ética corporativa de la empresa.

En cuanto a la mitigación y prevención de incidentes de seguridad de la información en el tratamiento de datos personales se debe realizar la revisión de la Guía No. 02[16] consistente en la elaboración de la política general de seguridad y privacidad de la información, realizada por el Ministerio de Tecnologías de la Información y las Comunicaciones, por medio de la cual se brinda una de la política general de seguridad y privacidad de la información, indicando los elementos mínimos que se recomienda implementar, al igual que se estipulan las fases de implementación de políticas de seguridad de la información, consistente en el desarrollo de las políticas, el cumplimiento de las mismas, la comunicación de las políticas, el monitoreo del cumplimiento, el mantenimiento de las políticas, pues las mismas deben ser actualizadas y el retiro, este último en caso que la policita haya cumplido su cometido, o la misma sea preferible eliminarla e implementar otra a una mera modificación de la misma. Este procedimiento de implementación de política general de seguridad y privacidad de la información es importante en el presente estudio, pues la misma aporta un camino al cual se puede recurrir si se pretende minimizar riesgos de incidentes de seguridad en el tratamiento de datos personales.

Ahora bien, en la previsión, seguimiento y control de incidentes de seguridad en el tratamiento de datos personales, toma relevancia analizar la etapa previa a la ocurrencia del incidente, por lo cual,

[16] Ministerio de Tecnología de la Información y las Comunicaciones. Guía No. 02. Elaboración de la política general de seguridad y privacidad de la información.

es importante la revisión de la guía No. 03[17] consistente en el procedimiento de seguridad de la información, procedimiento realizado por el Ministerio de Tecnologías de la Información y las Comunicaciones, dentro del cual se establece la seguridad del recurso humano, estableciendo para esta área los procedimientos de capacitación y sensibilización del personal, procedimiento consistente en definir la metodología empleada por la entidad para realizar la capacitación y sensibilización del personal en temas de seguridad de la información, con ello intentando prevenir un incidente de seguridad de la información.

Igualmente, por medio de la guía No. 03 antes mencionada, en la misma área de seguridad del recurso humano, se establece el procedimiento de ingreso y desvinculación de personal, proceso consistente en definir la manera en que la entidad gestiona de manera segura el ingreso y desvinculación del personal, tales como verificación de antecedentes, firma de acuerdos de confidencialidad. Procedimiento importante en cuanto a la prevención de los incidentes de seguridad en el tratamiento de datos personales, pues la no implicación de este procedimiento podría derivar en la filtración de información confidencial o datos sensibles, generando una vulneración a los derechos del titular de la información.

Por medio de la guía en mención, igualmente se menciona el control de acceso, pues se pueden establecer el procedimiento para ingreso seguro a los sistemas de información, el cual consistiría en cifrar la información y establecer un acceso segmentado por tokens de verificación previo al acceso de la información; también en cuando al control del acceso se sugiere implementar el procedimiento de gestión de usuarios y contraseñas consistente en establecer un sistema seguro de asignación de contraseñas y creación de usuarios, evitando con ello las contraseñas débiles y

[17] Ministerio de Tecnologías de la Información y las Comunicaciones. Guía No. 03. Procedimientos de Seguridad de la Información.

mitigando un acceso fácil a la información. Los anteriores procedimientos implican un beneficio para la prevención de incidentes de seguridad, pues mitiga la brecha de información, generando un control de acceso robusto a la misma.

- **Sobre el deber de realizar reportes ante un eventual incidente de seguridad en el tratamiento de datos personales.**

La protección de datos personales es un pilar fundamental en la era digital. La gestión adecuada de incidentes de seguridad es esencial para salvaguardar la integridad y confidencialidad de la información. Este apartado analiza la normativa colombiana vigente respecto a los plazos de notificación de violaciones de seguridad.

En Colombia, la Superintendencia de Industria y Comercio (SIC) por medio de la guía para la gestión de incidentes de seguridad[18] ha establecido directrices claras para la notificación de incidentes de seguridad que comprometan datos personales. Tal directriz consiste en que todos los responsables y encargados del tratamiento de datos están obligados a reportar dichos incidentes dentro de los quince (15) días hábiles siguientes a su detección. Este reporte debe realizarse a través de los canales dispuestos por la SIC, como el Registro Nacional de Bases de Datos (RNBD) o por medio del módulo específico en su página web, de conformidad con lo contemplado por medio del título quinto de la Circular Única de la Superintendencia de Industria y Comercio[19].

El reporte antes mencionado se desprende del cumplimiento del artículo 18 de la Ley 1581 de 2012, pues por medio del mismo se contemplan los deberes de los encargados del tratamiento de datos personales, dentro de los cuales se establece el deber de reportar ante la Superintendencia de

[18] Superintendencia de Industria y Comercio. Guía para la gestión de incidentes de seguridad. Disponible en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf
[19] Superintendencia de Industria y Comercio. (2022). Circular Única. Título V. Numeral 2.1. literal F. (ii). Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/092022/Título%20V%20Versión%2029-09-2022.pdf

Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

Sobre este reporte es importante mencionar que, puede ser el caso en que el responsable del tratamiento de datos personales contrate con una tercera empresa para que sea esta la encargada del tratamiento del dato personal, con lo cual es importante la implementación por medio del clausulado del contrato de transmisión de datos personales la obligación de informar al responsable del tratamiento del dato personal de manera inmediata ante la presentación de un incidente de seguridad en el tratamiento de datos personales, pues así se podrá asegurar un mayor tiempo de respuesta ante el incidente de seguridad.

Sobre el contrato de transmisión de datos personales, por medio de la guía emitida por la Superintendencia de Industria y Comercio Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales se establecen igualmente la sugerencia de la implementación de los siguientes aspectos dentro del contrato en mención: " *(A) El protocolo de respuesta en el manejo de incidentes de seguridad; (B) Roles y responsabilidades del encargado del tratamiento y del responsable del tratamiento del dato; (C) Puntos o personas de contacto ante un incidente de seguridad; (D) El procedimiento para el trámite de las consultas e inquietudes que puedan presentar los Titulares de la información; (E) Reporte de los incidentes de seguridad por parte de otros Encargados del Tratamiento, en caso de que se hayan hecho subencargos sobre cualquier operación del Tratamiento; (F) Cumplir las políticas de Tratamiento de información (PTI) de su entidad.".*

En igual sentido tiene relevancia lo mencionado por medio de la Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)[20] emitida por la Superintendencia de Industria y Comercio, la cual ha mencionado que las medidas adoptadas por el responsable del tratamiento de datos personales deben ser apropiadas; efectivas; útiles; oportunas; eficientes; demostrables, además de ello, reitera lo mencionado por medio del Decreto 1377 de 2013, en especifico de su artículo 26 y 27, pues por medio de los mismos se implementa la obligación de ante un eventual requerimiento por parte de la Superintendencia de Industria y Comercio, se debe demostrar por parte del responsable del tratamiento de datos personales las medidas propias y efectivas para cumplir con las obligaciones contempladas en la Ley 1581 de 2012, en la medida en que sea proporcional a la naturaleza de los datos personales objeto del tratamiento, la naturaleza juridica del responsable, teniendo en cuenta el tamaño empresarial, los riesgos potenciales que el tratamiento podría causar sobre los derechos de los titulares.

En cuanto al reporte ante un eventual incidente de seguridad en el tratamiento de datos personales, toma relevancia mencionar que, por medio de la circular externa 002 de la Superintendencia de Industria y Comercio[21] se estableció a las personas jurídicas de naturaleza privada inscritas en las Cámaras de Comercio y sociedades de economía mixta para efectos de los registros de sus bases de datos en el Registro nacional de bases de Datos, la obligación de reportar como novedades los incidentes de seguridad, situación que es muy importante en los incidentes de seguridad de la información, pues se proporciona el plazo de quince días anteriormente indicado, y el tiempo de reacción ante el incidente debe ser el más rápido posible, evitando así la maximización del daño o

[20] Superintendencia de Industria y Comercio. (2021). Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability).

[21] Superintendencia de industria y Comercio. (2015) Circular Externa No. 02. Por medio de la cual se imparten instrucciones a los Responsables del Tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las Cámaras de Comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el Registro Nacional de Bases de Datos (RNBD).

la filtración de mayor información a la inicial. Misma situación es incluida por medio de la circular externa 03 de la Superintendencia de Industria y Comercio[22] sin embargo, en este caso para las sociedades y entidades sin ánimo de lucro con activos totales superiores a 100.00 UVT y personas jurídicas de naturaleza pública.

Es cuanto a los incidentes se seguridad en el tratamiento de datos personales, toma relevancia el análisis de la circular externa 003 del 22 de agosto de 2024 promulgada por la Superintendencia de Industria y Comercio[23], pues por medio de esta se incluye la obligación de los admisnitradores de soceidades vigiladas por la Superintendencia de Industria y Comercio de establecer e implementar lineamientos corporativos adecuados para adoptar medidas precautorias o preventivas para proteger los derechos de los titulares de Datos Personales, además de obligarlos a implementar políticas interna efectivas para garantizar el debido tratamiento de Datos personales. situación que demuestra que los incidentes de seguridad en el tratamiento de datos no únicamente tienen relevancia cuando ya se han consolidado, sino que, también deben ser atendidos desde una etapa preventiva.

- **Sobre las sanciones más representativas impuestas por los entes sancionadores respectivos**

Por medio de la presentación de un derecho de petición ante la Superintendencia de Industria y Comercio, entidad encargada de la vigilancia y sanción de infracciones ante incidentes de seguridad en el tratamiento de datos, la entidad proporcionó las sanciones que se presentaron entre el año 2022 y el año 2024, relacionando en esta respuesta el monto de la sanción, la cantidad de

[22] Superintendencia de Industria y Comercio. (2018) Circular externa No. 003. Por medio de la cual se modifican los numerales 2.1 al 2.4 y eliminar los numerales 2.5 al 2.7 del capítulo segundo del título V de la Circular Única de la Superintendencia de Industria y Comercio.

[23] Superintendencia de Industria y Comercio (2024). Circular externa No. 03. Por medio de la cual se dictan instrucciones para los administradores societarios en relación con el tratamiento de Datos personales.

sanciones impuestas por cada periodo anualizado, los motivos sancionados más comunes, el porcentaje que representan las sanciones impuestas a cada sector económico, al igual que las mayores sanciones económicas entre el año 2022 y 2024, la anterior información se procederá a analizar a continuación.

Sin perjuicio de lo anterior, y de la información completa proporcionada por la SIC, es importante mencionar que, a diferencia de en la Unión Europea, no existe una información pública que determine o permita prever la cuantía de la sanción con base en el tipo de infracción, lo que ha generado críticas sobre la falta de previsibilidad.

De conformidad con lo anterior, ahora es importante presentar las cifras de las sanciones impuestas por año y la cantidad de sanciones igualmente por periodo anualizado, teniendo entonces que, en el año 2022 se impusieron sanciones por valor de SEIS MIL CUATROCIENTOS TREINTA Y SEIS MILLONES QUINIENTOS NUVE MIL CUATROCIENTOS CINCUENTA Y SEIS PESOS COLOMBIANOS ($6.436.509.456), por medio de ciento veinticuatro (124) sanciones impuestas; para el periodo del año 2023, se realizaron noventa y dos (92) sanciones, por medio de las cuales se obtuvo un monto total de CUATRO MIL NOVECIENTOS TREINTA Y DOS MILLONES NOVECIENTOS OCHENTA Y DOS MIL CIENTO TREINTA Y DOS PESOS COLOMBIANOS ($4.932.982.132), y en el año 2024 se evidencia una minoría en la sanciones impuestas, siendo estas cuarenta y ocho (48), pero sumando un monto mayor al del año anterior, ya que fue de CINCO MIL QUINIENTOS TREINTA Y SEIS MILLONES CIENTO SETENTA Y NUEVE MIL CUATROCIENTOS NOVENTA Y UN PESOS COLOMBIANOS ($5.536.179.491) como se observa en la siguiente grafica.

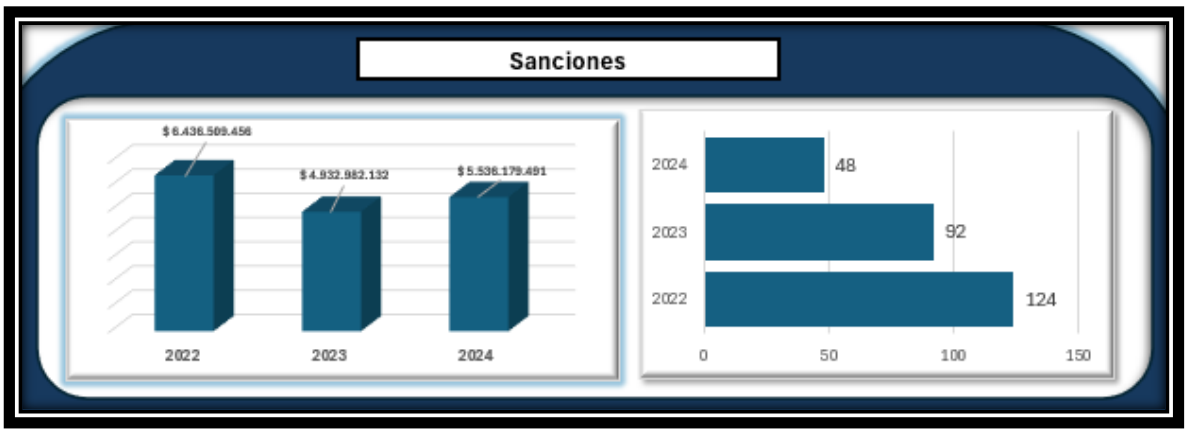

Ilustración 1. Sanciones año 2022 - 2024. Monto y cantidad de sanciones.

Ahora bien, es importante igualmente analizar que, dentro de los motivos más sancionados por la ley 1581 de 2012 se encuentra con un cincuenta y cinco por ciento (55%) sanciones asociadas a la autorización del tratamiento de datos, esto puede ser por una autorización no solicitada, o no realizarla en debida forma, posterior se evidencia que el segundo motivo más común dde las sanciones impuestas con un diecinueve por ciento (19%) es el Manual de Políticas como se observa a continuación.

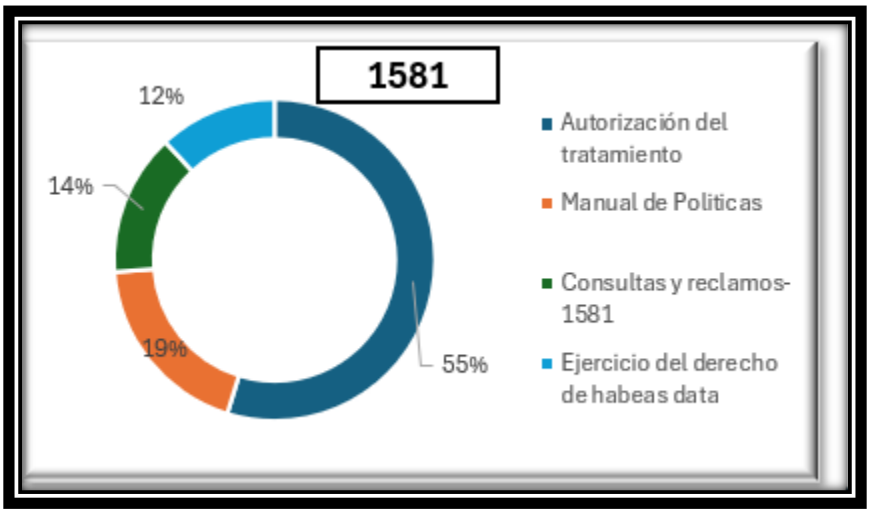

Ilustración 2. Motivos más sancionados. Ley 1581 de 2012.

Observando la anterior información proporcionada por la Superintendencia de Industria y Comercio, la cual puede ser cotejada por los informes públicos realizados anualizados y publicados

por esta entidad, se observa que una implementación de la cultura del dato personal o capacitación en cuanto al buen uso de autorización del tratamiento de datos y la debida implementación del manual de políticas, podría generar en primer lugar una minoría en las sanciones, al igual que una minimización de riesgos para los titulares de los datos.

Ahora bien, para sectorizar y poder iniciar esta cultura de datos o capacitaciones se debe analizar los sectores económicos más sancionados, dentro de los cuales, se evidencia que en primer lugar se encuentran las Actividades de Servicios Administrativos y de Apoyo, pues este sector representa el veinte por ciento (20%) de las sanciones impuestas por el incumplimiento de la Ley 1581 de 2012, siguiéndole el sector económico de las Actividades Inmobiliarias con un diecisiete por ciento (17%) como se evidencia a continuación.

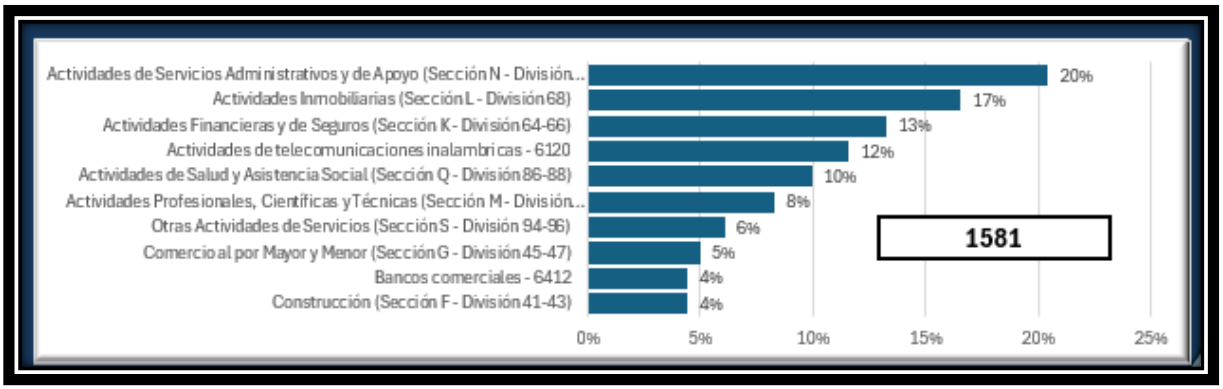

Ilustración 3. Representación porcentual de las sanciones impuestas por incumplimiento de la Ley 1581 de 2012 por sector empresarial.

Es importante en igual sentido presentar algunos de los casos encontrados frente a las sanciones presentadas en Colombia, casos que se estiman más representativos por ser los casos con las sanciones más altas hasta el momento, o algunos de los casos más recientes, entre las cuales se encuentra el caso de COMUNICACION CELULAR S A COMCEL S A, empresa que fue sancionada en el año 2023 por medio de la resolución 35435 por la reincidencia en el indebido tratamiento para obtener números telefónicos de referidos para ofrecer servicios de

telecomunicaciones, a través de la campaña comercial "*Amigos que te premian*" sin solicitar la autorización previa, expresa e informada de los titulares, sanción que entre el periodo de 2022 a 2024 fue la mayor, con un monto de MIL TRESCIENTOS SEIS MILLONES DOSCIENTOS OCHENTA Y NUEVE MIL SEISCIENTOS PESOS COLOMBIANOS ($1.306.289.600), es importante mencionar que, esta empresa además llama la atención porque ha sido sancionada por la SIC entre el periodo 2022 a 2024 en varias ocasiones por el incumplimiento de la Ley 1581 de 2012 sumando en sanciones la totalidad de SEIS MIL TRESCIENTOS CINCUENTA MILLONES OCHOCIENTOS OCHENTA Y CINCO MIL QUINIENTOS SETENTA Y SEIS PESOS COLOMBIANOS ($6.350.885.576).

Otra de las sanciones más altas impuestas por la SIC fue a COLOMBIA TELECOMUNICACIONES S.A. E.S.P. BIC, la cual fue de NOVECIENTOS CINCUENTA Y UN MILLONES TRESCIENTOS NOVENTA Y DOS MIL CIENTO TREINTA Y SEIS PESOS COLOMBIANOS ($951.392.136), entidad que en total entre el periodo de 2022 a 2024 fue multada por un valor total de CUATRO MIL CUATROCIENTOS OCHENTA Y CINCO MILLONES TRESCIENTOS NOVENTA Y SEIS MIL QUINIENTOS OCHENTA Y CINCO PESOS COLOMBIANOS ($4.485.396.585).

Pese a en Colombia no existir un sistema público de sanciones, y únicamente contar con los criterios establecidos en el artículo 24 de la Ley 1581 de 2012, los cuales son: "*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."; no es clara la relación entre el tamaño de la empresa, esto es, si se trata de una micro, pequeña o mediana empresa clasificación realizada mediante el decreto 957 de 2019, situación que podría conllevar una prevención de la posible sanción de conformidad con el tamaño empresarial.

Es importante precisar que, pese a que la respuesta de los datos remitida por la Superintendencia de Industria y Comercio únicamente suministró los datos entre 2022 y 2024, recientemente se ha publicado la resolución 16581 de 2025[24], por medio de la cual sancionaron a sociedad MERCADO LIBRE COLOMBIA LTDA por el monto de DOSCIENTOS CATORCE MILLONES CUATROCIENTOS CINCO MIL CIENTO VEINTE PESOS M/CTE (214.405.120), sanción impuesta por la vulneración de la Ley 1581 y su respectivo decreto reglamento, esta resolución y sanción toma relevancia, pues se menciona de manera general que la sanción interpuesta obedece al principio de proporcionalidad constitucional, sin detallar como se da aplicación al principio o qué criterios se aplican en la cuantificación de la sanción.

- **Sobre la protección de datos personales a terceros países**

En Colombia, la Ley 1581 de 2012, en concordancia con el decreto reglamentario 1377 de 2013 establece que las transferencias internacionales de datos personales solo pueden realizarse hacia países que proporcionen niveles adecuados de protección, reconocidos como tales por la Superintendencia de Industria y Comercio. Además de mencionar por medio del artículo 26 de la Ley 1581 de 2012 las excepciones en las cuales no se encuentra prohibida la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de

[24] Superintendencia de Industria y Comercio. Resolución 16582 del 31 de marzo de 2025. Radicación 22-301462.

datos. El análisis de la protección de datos personales a terceros países es relevante para el presente estudio, pues se evidencia una preocupación por parte de la Superintendencia de industria y comercio y una intervención marcada para prevenir los incidentes de seguridad en el tratamiento de datos personales a terceros países.

Dentro de las excepciones a la prohibición general se encuentra las situaciones en las cuales medie la autorización del titular; el intercambio de datos de carácter médico cuando así lo exija el tratamiento del titular por cuestiones de salud; transferencias bancarias o bursátiles; trasferencias acordadas en el marco de tratados internacionales en cumplimiento del principio de reciprocidad; trasferencias necesarias en etapa precontractual o contractual siempre que se cuente con autorización del titular; trasferencias requeridas para la salvaguarda del interes público o en reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En similar sentido fue desarrollado por medio del artículo 24 del decreto 1377 de 2013, por medio del cual se establecen las obligaciones en cabeza del respetivo encargado del tratamiento de datos personales, las cuales deben ser contenidas por medio de un contrato de transmisión de datos personales. Además de incluir como obligación la observancia de las particularidades antes mencionadas que conlleva el cumplimiento en esta materia contenida en el artículo 26 de la Ley 1581 de 2012.

No obstante, en la normativa colombiana no se ha previsto, hasta la fecha, un conjunto de cláusulas contractuales tipo, ni modelos aprobados o recomendados oficialmente, que sirvan como instrumentos preestablecidos para garantizar las condiciones de legalidad y seguridad en dichas transferencias. En consecuencia, la inclusión de cláusulas específicas queda a discreción de las partes contratantes, bajo el cumplimiento general de los principios de legalidad, finalidad, libertad,

veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, los cuales se desarrollan por medio de la Ley 1581 de 2012.

Por lo anterior, se evidencia un marco jurídico frente a incidentes de seguridad en el tratamiento de datos personales en Colombia consistente en la Ley 1581 de 2012 por medio de la cual "*se dictan disposiciones generales para la protección de datos personales*"; El Decreto 1377 de 2013, por medio del cual "*se reglamenta parcialmente la Ley 1581 de 2012*", compilado en el decreto 1074 de 2015 "*por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo*", además de ello, pese a no ser normas de obligatorio cumplimiento per sé, la Superintendencia de Industria y Comercio ha establecido guías sobre la gestión de incidentes de seguridad en el tratamiento de datos personales y la implementación del principio de responsabilidad demostrada, las cuales no son de obligatorio cumplimiento, sin embargo, son guías que brindan apoyo para el cumplimiento de normas de carácter imperativo, por ende, en caso de no cumplir estas guías, igualmente se debe demostrar el cumplimiento de las obligaciones contenidas por medio de la Ley 1581 de 2012 y el decreto 1377 de 2013, además de que las normas corporativas vinculantes se vuelven obligatorias unas vez son aprobadas por la Superintendencia de Industria y Comercio para aquel grupo empresarial que solicitó el reconocimiento de las mismas.

(ii) El Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) en materia de incidentes de seguridad de la información de datos personales y algunas de sus sanciones más representativas

Por medio del presente apartado se examinará el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) en materia de incidentes de seguridad de la información en el tratamiento de datos personales y sus sanciones más representativas, pues inicialmente se podría

pensar que se trataría de una normativa más avanzada en esta materia, sin perjuicio de ello, por medio del presente análisis podrán comprobar o improbar esta afirmación, al evidenciar las similitudes y diferencias que existen entre el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) y la normativa colombiana, pues se examinará los mismos aspectos que se estudiaron en el acápite primero del presente documento.

Sobre este análisis, es importante mencionar que en la Unión Europea por medio de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), en específico del artículo octavo, se desarrolló el derecho fundamental a la protección de datos de carácter personal en el siguiente sentido: "1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. ; 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."*

Situación que refleja una protección constitucional del derecho a la protección de datos de carácter personal, ahora bien, en igual sentido es desarrollado por medio del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD), pues se establece en varios acápites este derecho y su regulación, como lo es por medio del artículo 16, el cual contempla el derecho a la rectificación de los datos personales, o el artículo 17 el cual contempla el derecho a la supresión, o lo regulado en el artículo 18 concerniente a la limitación del tratamiento, ahora bien, pese a contar con este robusto desarrollo en materia de tratamiento de datos personales, es importante continuar con el análisis de los mismos frente al reporte de un eventual incidente de seguridad de la información, frente a la transferencia internacional de datos personales y en cuanto a las sanciones más relevantes impartidas por el ente encargado.

Igual de relevante es el análisis de los incidentes de seguridad de la información en la Unión Europea, los cuales de conformidad con el del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) se denominan "violación de la seguridad de los datos personales", la cual es definida en este reglamento en su artículo cuarto numeral 12, de la siguiente manera *"toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*".

Sobre el particular, por medio del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) en su artículo 68 se crea el Comité Europeo de Protección de Datos, el cual emitirá directrices, recomendaciones y buenas prácticas respecto a las particulares en las que el responsable o encargado del tratamiento debe notificar la violación de la seguridad de los datos personales; o de las circunstancias en que sea posible la ocurrencia de la violación de la seguridad de los datos personales.

Aunado a lo anterior, el mismo reglamento contempla los principios relativos al tratamiento de datos personales, por medio de su artículo quinto, dentro de los cuales se evidencia el principios de Principio de licitud, lealtad y transparencia; Principio de limitación de la finalidad; Principio de minimización de datos; Principio de exactitud. Los anterior principios a consideración del presente estudio se consideran que no responden a las necesidades de los incidentes de seguridad en el tratamiento de datos, pues no se evidencia en principio de seguridad, el cual es primordial, o algún principio que se vulnere por la presencia de un incidente de seguridad en el tratamiento de datos personales.

Continuando con la revisión de lo relativo a los incidentes de seguridad de la información en la Unión Europea, toma relevancia la revisión del Dictamen 03/2014 realizado por el grupo de trabajo

de protección de datos[25], pues por medio del mismo se estableció que las violaciones de información pueden clasificarse de conformidad con tres principios de información, los cuales son: (A) Violación de la confidencialidad, cuando se presenta una revelación no autorizada por el titular; (B) Violación de la integridad, cuando se produce una alteración no autorizada de los datos; (C) Violación de la disponibilidad, cuando se produce una pérdida de acceso accidental de los datos. Principios que de presentarse un incidente de seguridad en el tratamiento de datos personales se verían vulnerados de manera directa, a diferencia de los contemplado por medio del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD).

- **Sobre el deber de realizar reportes ante un eventual incidente de seguridad en el tratamiento de datos personales.**

Esta situación en la Unión Europea se evidencia por medio del artículo 33 del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) el cual establece que, en caso de una violación de seguridad de los datos personales, el responsable del tratamiento debe notificar a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de haber tenido constancia de ella[26]. Si la notificación no se realiza dentro de este plazo, debe ir acompañada de una justificación de la demora. Además, si la violación supone un alto riesgo para los derechos y libertades de las personas físicas, también se debe informar a los afectados sin dilación indebida.

Aunado a lo anterior, por medio del mismo reglamento se establece en su artículo 34 la obligación de remitir una comunicación ante la presencia de una violación de la seguridad de los datos

[25] Grupo de trabajo de protección de datos. Dictamen 03/2014 sobre la notificación de violación de datos personales.
[26] Diario Oficial de la Unión Europea. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Artículo 33.

personales del interesado, esta comunicación debe realizarse en caso de ser probable la materialización de una violación o en caso de ocurrencia de la violación, es importante denotar que esta comunicación debe realizarse con el uso de un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de la información y deberá contener como minimo las posibles consecuencias de la violación de la seguridad de los datos personales, describir las medidas adoptadas para poner remedio a la violación de la seguridad de los datos personales, informar el nombre y datos del delegado de protección de datos o en su defecto otro contacto con quien pueda obtenerse mayor información.

En igual sentido, se contempla en el artículo 34 del reglamento en mención las excepciones al deber de comunicación, cuando el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y han sido aplicadas a la violación de la información; cuando el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no hay probabilidad de que se concretice el alto riesgo a los derechos del titular.

Sobre el particular se expidió la Directrices 9/2022[27], relativo a la obligación de notificación de las violaciones de la seguridad de los datos personales en el marco del RGPD, adoptada el 28 de marzo de 2023, por medio de la cual se define el concepto de violación de la seguridad de los datos personales, definición contenida en el artículo cuarto del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo, antes desarrollado, aunado a ello se menciona que esta violación de la seguridad implica además un incumplimiento en los principios relativos al tratamiento de datos personales. Denotando lo anterior la reiteración de la obligación de

[27] Comité Europeo de Protección de Datos. (2022). Directrices 9/2022, sobre la notificación de las violaciones de la seguridad de los datos personales en el marco del RGPD.

información al titular en caso de materializarse un incidente de seguridad en el tratamiento de datos personales.

- **Sobre las sanciones más representativas impuestas por los entes sancionadores respectivos**

La respuesta sancionatoria en la Unión Europea a los incidentes de seguridad constituye un instrumento clave dentro de los regímenes de protección de datos personales, en tanto contribuye a disuadir comportamientos negligentes, promover la adopción de medidas preventivas y garantizar los derechos de los titulares.

El Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) por medio de su artículo 83 establece un sistema de sanciones administrativas que, se caracteriza por ser escalonado, proporcional y disuasorio. Las autoridades nacionales de protección de datos, como la Agencia Española de Protección de Datos (AEPD) o la Commission Nationale de l'Informatique et des Libertés (CNIL) en Francia, cuentan con facultades para imponer multas de considerable envergadura.

Los criterios que deben considerar las autoridades competentes al momento de imponer sanciones incluyen: (i) La naturaleza, gravedad y duración de la infracción; (ii) El número de titulares afectados y el nivel de daño sufrido; (iii) Si la infracción fue intencional o negligente; (iv) Las medidas adoptadas para mitigar el daño; (v) El grado de responsabilidad del infractor; (vi) Cualquier infracción anterior relacionada.

Ahora bien, una vez mencionados los criterios que se tienen en la Unión Europea en materia sancionatoria por le incumplimiento del correspondiente tratamiento de datos personales, resultante en incidentes de seguridad, toma importancia analizar los casos más representativos de

las sanciones impartidas, se consideran los más representativos por su cuantiosa sanción, los cuales son: El caso de Amazon en Luxemburgo, empresa que fue multada en el año 2021 por 746 millones de euros por prácticas relacionadas con publicidad dirigida sin consentimiento válido[28]; similar situación se presentó con British Airways en el Reino Unido, a quien en el 2020 se le impuso una multa de 22 millones de euros por un incidente de ciberseguridad que expuso datos personales de más de 400.000 usuarios[29]; o el caso de Meta en Irlanda, a quien en el 2023 se le impuso una multa por 1.200 millones de euros, una de las más altas hasta la fecha, por transferencias internacionales de datos sin garantías adecuadas[30].

Estas decisiones no solo imponen sanciones económicas, sino que también van acompañadas de órdenes correctivas que obligan a modificar las prácticas de tratamiento de datos. Las sanciones económicas obedecen el principio de proporcionalidad, proporción caracterizada por medio del artículo 83 del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD), esto implica, analizar la naturaleza de la infracción, la gravedad, la duración de la infracción, el número de afectados, los daños sufridos, las medidas mitigadoras, las infracciones previas.

Denotando lo anterior que el ejercicio sancionatorio en la unión Europea se puede interpretar como una repuesta ajustada a las necesidades correccionales de las infracciones pues responde a un criterio de proporcionalidad ante las características de la conducta de incumplimiento cometida y a las características propias del infractor.

- **Sobre la protección de datos personales a terceros países**

[28] Comisión Nacional de Protección de Datos de Luxemburgo. Sentencia del 15 de Julio de 2021.
[29] Oficina del Comisionado de Información. Case ref: COMo783542.
[30] Comisión de Protección de Datos de Irlanda. Decisión del 26 de septiembre de 2024. Referencia: IN-19-4-1-.

En la Unión Europea el tratamiento de datos personales a terceros países ha sido desarrollado por medio del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) establece en sus artículos 44 a 50 un régimen riguroso para la transferencia internacional de datos, como lo es el reconocimiento del principio general de la transferencia de datos contenido en el artículo 44 del reglamento en mención; las trasferencias basadas en una decisión de adecuación, consistente en la adecuación del país receptor, evaluando con ello los niveles de seguridad, el estado de derecho, los compromisos internacionales asumidos, las autoridades de control en materia de tratamiento de datos personales, entre otros factores contenidos en el artículo 45 del reglamento indicado.

Además de lo anterior, realiza un especial énfasis en la transferencia de datos mediante garantías adecuadas, pues establece los requisitos para considerar que se cumplen las garantías necesarias para el titular del dato, entre las cuales se encuentra cumplir con un instrumento jurídicamente vinculante y exigible, contar con normas corporativas vinculantes, cláusulas contractuales tipo adoptadas por la Comisión Europea mediante la Decisión de Ejecución (UE) 2021/914[31]. Estas cláusulas tipo están estructuradas modularmente, según la naturaleza de la relación jurídica entre exportador e importador de datos (por ejemplo, responsable a responsable, o responsable a encargado), y constituyen mecanismos estandarizados, exigibles y presumidos como adecuados para cumplir con los requisitos del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD). En virtud de su carácter normativo y de su reconocimiento a nivel comunitario, dichas cláusulas constituyen una herramienta esencial para asegurar la protección de los derechos fundamentales de los interesados en contextos extraterritoriales.

[31] Diario oficial de la Unión Europea. (2021). DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN EUROPEA.

(iii) Análisis comparativo de los resultados del estudio del marco jurídico colombiano y el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) en materia de incidentes de seguridad en el tratamiento de datos personales y algunas de sus sanciones más representativas

En el presente acápite se realizará el análisis comparativo de los resultados del estudio del marco jurídico colombiano y el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD) en materia de incidentes de seguridad en el tratamiento de datos personales y algunas de sus sanciones más representativas, análisis realizado desde un enfoque cualitativo de tipo jurídico-comparado, orientado a la comprensión profunda y crítica del régimen sancionatorio aplicable a los incidentes de seguridad en el tratamiento de datos personales en el ámbito empresarial, contrastando las disposiciones del Reglamento General de Protección de Datos en la Unión Europea con las contenidas en la Ley 1581 de 2012 y decretos reglamentarios.

Cuando se realiza una comparación entre países como Colombia y los integrantes de la Unión Europea, se debe mencionar que la comparativa puede no solo reflejar factores objetivos como lo es meramente la codificación o legislación vigente, sino además, debe reflejar o responder a la cultura, política e ideología de cada país, como bien lo definen los autores Veronese, A., Silveira, A., Lemos Igreja, R., Lopes Espiñeira Lemos, AN y Guimarães Moraes, T., al definir el término "*culture of personal data protection*", el cual hace referencia no solo a la regulación en materia de datos personales promulgada en cada país integrante de la unión Europea, sino además, a la cultura que gira en torno a esta, como lo puede ser de manera superflua mencionar que, en la Unión Europea de conformidad con los autores se menciona que los titulares de los datos personales y los responsables del manejo de los mismos acatan las normas pertinentes, pero aunado a ello, responden a los principios internacionales, usos y costumbres sobre los mismos, desde una

perspectiva de seguridad de la información que a su vez se ve reflejada en la sociedad, siendo conscientes que, el origen del buen manejo de los datos personales no es un capricho sino que, responde a un derecho fundamental internacional.

En la realización del análisis propuesto toma relevancia lo mencionado por Adolfo Arreola García en su libro "Ciberseguridad: ¿Por qué es importante para todos?" , por medio del cual nos pone de presente el incremento de los dispositivos móviles en el siglo XX, sin embargo, nos hace percatar de la importancia de proteger la seguridad de estos dispositivos, la cual en ciertas ocasiones se ha dejado en un segundo plano, enmarcando la importancia no solo a nivel individual de la seguridad de la información, sino a nivel empresarial y estatal, toda vez que, un ciber ataque puede provenir de una persona, un estado, o una organización independiente, logrando con ello inmiscuirse en la comunicación más pequeña como lo puede ser la inter personal como lo puede ser a nivel supranacional; en igual sentido destaca que los principales objetivos de la ciberseguridad son: (i) proteger la información, (ii) proteger la infraestructura

Sobre este punto, es importante mencionar que, desde esta perspectiva planteada por el profesor Adolfo Arreola García, se debe analizar la materia sujeto a estudio del presente trabajo, toda vez que, en el sector empresarial, la migración de datos, la filtración de la información, o inclusive, un secuestro de información, no solo tiene un impacto negativo de manera inmediata, sino que, conllevan un impacto social en el sector empresarial, toda vez que, si los empresarios no se sienten seguros de la información que tiene dentro de su empresa, o dentro de un territorio geográfico, no van a poder desarrollar nuevas invenciones, celebrar contratos comerciales, acuerdos empresariales o desarrollar proyectos a gran escala, por el temor de que sus proyectos sean secuestrados en un ciberataque. Lo cual se puede analizar en términos del premio nobel de

economía, el profesor Richard H. Thaler y Cass R[32]. Sunstein, como un "*Nudge*", pues en lugar de impulsar al desarrollo, generaría un efecto contrario, desincentivando a la innovación desde el sector empresarial.

Para realizar el ejercicio comparativo propuesto es importante establecer los criterios rectores, los cuales desde las sanciones serán el monto de la sanción, es decir, se comparará tomando las sanciones más cuantiosas en ambas regulaciones y determinando en cual regulación ha sido mayor la sanción aplicada, ahora bien, en cuanto al análisis comparado normativo, se realizará una revisión de los criterios de similitud, tales como lo pueden ser el nivel de comparación, el análisis del tipo de sistema jurídico a analizar, la jerarquía de la Ley, y sobre todo, los criterios que en palabras del profesor Cota, Adrián Mancera (2008), quien por medio de su texto "*Consideraciones durante el proceso comparativo*", menciona que se debe tener presente los criterios de sujeto común; nivel de comparación; sistemas jurídicos comparables e interés funcional, los cuales son analizados a continuación, y se escogen como criterios del presente análisis por su especificidad frente al relacionamiento entre los sistemas jurídicos a analizar .

El sujeto común de esta investigación se define en la regulación del tratamiento de datos personales y la gestión de incidentes de seguridad de la información en el contexto empresarial, tanto en el ordenamiento jurídico colombiano como en el europeo. Ambos sistemas jurídicos abordan esta materia desde una perspectiva normativa que establece deberes específicos para los responsables del tratamiento, en cuanto a la protección, gestión y respuesta frente a vulneraciones de seguridad.

Ahora bien, frente al nivel de comparación corresponde a una microcomparación temática, al centrarse en una materia jurídica específica: la gestión de incidentes de seguridad en el tratamiento

[32] Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving Decisions about Health, Wealth, and Happiness. Yale University Press. https://books.google.com.co/books?id=dSJQn8egXvUC

de datos personales. Este enfoque permite analizar en detalle aspectos concretos como los mecanismos de notificación, los plazos legales, las obligaciones de los responsables del tratamiento y los procedimientos sancionatorios previstos en el marco normativo colombiano y en el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD).

La elección de este nivel de análisis favorece una comparación precisa y estructurada, orientada a identificar similitudes, divergencias y oportunidades de mejora en la regulación colombiana a partir de la experiencia europea, o en su defecto, demostrar el avance legislativo en Colombia sobre los incidentes de seguridad en el tratamiento de datos personales.

El análisis comparativo desarrollado en el presente estudio se fundamenta en la compatibilidad estructural entre el ordenamiento jurídico colombiano y el sistema europeo de protección de datos, ambos enmarcados dentro de la tradición del "*Civil Law*"[33]. Esta pertenencia común facilita el ejercicio de comparación normativa, al compartir principios como la codificación, la sistematicidad de las fuentes y la función garantista del Derecho.

La comparación se centra específicamente en las normas que regulan los incidentes de seguridad en el tratamiento de datos personales, lo cual permite contrastar de manera precisa los elementos sustantivos, procedimentales y sancionatorios en ambos contextos jurídicos. Este marco común justifica tanto la viabilidad metodológica del análisis como la posibilidad de formular recomendaciones normativas adaptables a la realidad colombiana.

El presente análisis comparativo obedece a un claro interés funcional, al permitir evaluar la eficacia de los mecanismos jurídicos de reporte, prevención y sanción de incidentes de seguridad en el

[33] Merryman, J., & Pérez-Perdomo, R. (2018). The civil law tradition: an introduction to the legal systems of Europe and Latin America. Stanford University Press.

tratamiento de datos personales. Este interés es social, práctico y académico, ya que se relaciona con la protección efectiva de los derechos de los titulares y con la necesidad de promover el cumplimiento normativo en el ámbito empresarial. Tanto el sistema jurídico colombiano como el europeo buscan reducir los riesgos jurídicos derivados de los incidentes de seguridad y establecer obligaciones claras para los responsables del tratamiento. En este contexto, el análisis comparativo ofrece herramientas para identificar posibles mejoras normativas en Colombia o, en su defecto, reconocer los avances del marco nacional en materia de gestión, mitigación y sanción de este tipo de incidentes. La utilidad del enfoque funcional radica en su capacidad para generar propuestas aplicables y contextualizadas, con impacto tanto en la política legislativa como en la práctica empresarial.

Este análisis puede sorprender inicialmente, pues la diferencia estructural entre la unión europea y Colombia podría impedir la aplicación de una comparación juridica, razón por la cual, toma relevancia analizar a profundidad esta situación en el siguiente sentido. En el marco común europeo, el tratamiento de datos personales es un derecho fundamental, así se reconoce por medio de la carta de los derechos fundamentales de la Unión Europea, que por medio de su artículo octavo contempla el derecho a la protección de datos de carácter personal[34]. Situación que en Colombia no ocurre.

Sin perjuicio de lo anterior, de conformidad con lo mencionado por el profesor Mancera Cota, una diferencia estructural o de jerarquía normativa no impide per sé el análisis comparativo, siempre que se cumpla con el criterio de funcionalidad y con un eje temático común o mencionado en

[34] Parlamento Europeo, Consejo de la Unión Europea y Comisión Europea, Carta de los Derechos Fundamentales de la Unión Europea, Unión Europea, 26 Octubre 2012, https://www.refworld.org/es/leg/trat/ue/2012/es/129076 [accedida 11 March 2025]. "*Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan*."

palabras del profesor Mancera *"tertium comparationis"* que hace referencia a la prueba que pretende probar problemas comunes.

Por lo anterior, en el presente caso, pese a existir jerarquía normativa distinta, toda vez que, como se ha mencionado en la Unión Europea se le reconoce como un derecho fundamental al tratamiento de datos personales; mientras que en Colombia solo se da esa connotación por medio de un análisis jurisprudencia y esta connotación por conexidad[35], por lo que si existe funcionalidad normativa comparable en temas como: (i) Gestión de incidentes de seguridad; (ii) Obligaciones de las empresas frente al manejo de datos; (iii) Responsabilidad administrativa y sanciones; (iv) Deber de notificación ante incidentes.

Uno de los elementos diferenciadores de este estudio es el énfasis en el análisis sancionatorio. Pues resulta fundamental examinar cómo se materializa la aplicación práctica de las normas ante eventos adversos como las violaciones de seguridad. El régimen europeo ha desarrollado una política sancionatoria sistemática, con criterios públicos de graduación, cooperación transfronteriza entre autoridades, y la imposición de multas administrativas significativas, que en algunos casos han superado los cientos de millones de euros. En Colombia, por su parte, la Superintendencia de Industria y Comercio ha impuesto sanciones importantes, pero aún persisten desafíos relacionados con la publicidad, la proporcionalidad y la sistematicidad de los procesos sancionatorios.

Este enfoque resulta particularmente pertinente para el campo del Derecho Comercial, en tanto el cumplimiento normativo en materia de protección de datos se ha convertido en un componente

[35] Personería de Bogotá D.C. ABC de las acciones de tutela. Incidente de desacato e impugnaciones. *"Los derechos fundamentales por conexidad. Son aquellos derechos que, no siendo denominados como tales en la Constitución Política, les es reconocida esta condición en virtud de la íntima relación con otros derechos fundamentales".*

esencial del gobierno corporativo, el manejo del riesgo legal y la estrategia empresarial en mercados globalizados, tanto se ha visto la necesidad de mejorar la regulación que, el 06 de mayo de 2025 la SIC ha publicado el Proyecto Normativo *"Lineamientos sobre el tratamiento de datos personales en el ecosistema Fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros"*[36].

Además, la protección de datos ya no es solo una obligación sectorial, pues como se observó en los resultados expuestos en el presente estudio, se encontró que se ha sancionado por el incumplimiento de la Ley 1581 de 2012 en sectores como las actividades de servicios de apoyo; actividades Inmobiliarias; Actividades Financieras y de seguros; Actividades de telecomunicaciones inalámbricas; Actividades de salud y Asistencia social, razón anterior que demuestra que no hay relación en los sectores sancionados y existe una diversidad de sectores con necesidad de mejorar sus esquemas de protección de datos.

Así, la presente investigación se inscribe en una línea de análisis jurídico contemporáneo, que reconoce el papel estratégico de los datos en la actividad empresarial, y que busca contribuir al fortalecimiento de un régimen normativo colombiano más eficaz, preventivo y coherente con los estándares internacionales. En un escenario donde la circulación de datos es transfronteriza y los riesgos de seguridad son crecientes, contar con un sistema de gestión y sanción de incidentes robusto no solo garantiza los derechos de los ciudadanos, sino que también ofrece seguridad jurídica a las organizaciones que operan en el entorno digital.

---

[36] Superintendencia de Industria y Comercio. (2025). Proyecto Normativo: "Lineamientos sobre el tratamiento de datos personales en el ecosistema Fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros". Disponible en: https://sedeelectronica.sic.gov.co/transparencia/normativa/proyecto-normativo-lineamientos-sobre-el-tratamiento-de-datos-personales-en-el-ecosistema-fintech-y-los-modelos-de-negocio

Del desarrollo realizado en el presente trabajo de investigación, se puede evidenciar una clara diferencia normativa, en cuanto al tiempo de reporte del incidente digital entre Colombia y la Unión Europea, con ello, es importante mencionar que aunque en Colombia ya se cuenta con un plazo establecido para la notificación de incidentes de seguridad, se propone revisar la posibilidad de reducir este plazo, alineándolo más estrechamente con las prácticas europeas. Un plazo más corto, como el de 72 horas establecido por el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD), podría mejorando así la capacidad de respuesta ante incidentes y fortalecer la confianza de los ciudadanos en la protección de sus datos personales.

Las ventajas de la implementación que se presentan podrían representar: (i) Respuesta Rápida: Un plazo más corto permite una reacción más ágil ante incidentes, minimizando potenciales daños; (ii) Mayor Transparencia: Informar oportunamente a las autoridades y a los afectados refuerza la confianza en las entidades responsables del tratamiento de datos; (iii) Armonización Internacional: Alinear los plazos de notificación con estándares internacionales facilita la cooperación y el cumplimiento en contextos transfronterizos.

Si bien Colombia ha avanzado en la regulación de la notificación de incidentes de seguridad, la adopción de plazos más estrictos, inspirados en el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD), podría fortalecer aún más la protección de los datos personales y mejorar la confianza en el ecosistema digital del país.

- **Sobre las sanciones impuestas por los entes sancionadores respectivos**

Del análisis realizado, se evidencia que en Colombia, el principio de proporcionalidad frente a las sanciones se puede mencionar que es reflejado de manera parcial, pues no se establecen los criterios de estimación de la sanción, por lo cual, se recomienda implementar los estipulados por

medio del artículo 83 del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD), esto implica, analizar la naturaleza de la infracción, la gravedad, la duración de la infracción, el número de afectados, los daños sufridos, las medidas mitigadoras, las infracciones previas, y se propone además analizar de conformidad con los criterios antes expuestos de los riesgos, así mismo de conformidad con el riesgo en el cual se haya incurrido, en esa proporción fijar la sanción.

O en su defecto, de no estimarse suficientes los criterios antes mencionados para la imposición de sanciones y aplicación del principio de proporcionalidad, se sugiere dar aplicación a la inclusión de criterios claros por medio de la promulgación de una Ley, que incluya parámetros claros de dosificación de la sanción, propuesta presentada por la Profesora María-Lourdes Ramírez-Torrado, quien por medio de su texto[37] establece la necesidad de definir parámetros claros por medio de la legislación, para con ello al momento de imponer una sanción poder justificar la proporcionalidad de la misma. Pues en Colombia, pese a presentarse los criterios establecidos en el artículo 24 de la Ley 1581 de 2012, los mismos no cumplen con parámetros claros de dosificación o cuantificación de la sanción, los cuales son necesarios para prever una posible sanción.

A partir de lo expuesto, se advierte la existencia de un sistema sancionatorio divergente entre la Unión Europea y Colombia. Mientras que en el ámbito europeo se garantiza el acceso a información pública detallada sobre los criterios valorativos que orientan a las autoridades al momento de imponer sanciones —como la naturaleza y gravedad de la infracción, la intencionalidad, el daño causado, entre otros—, en el contexto colombiano dicha publicidad resulta limitada. Puesto que, en Colombia solo se publican las sanciones ya impuestas, sin que se haga

[37] Ramirez Torrado, María Lourdes. (2010. Estudios Socio Jurídicos. Reflexiones acerca del principio de proporcionalidad en al ámbito del derecho administrativo sancionador colombiano.

explícita la motivación técnica y jurídica que condujo a su determinación y cuantificación, particularmente se omite el análisis del principio de proporcionalidad en cuanto a la sanción impuesta. Esta ausencia de información impide a los sujetos que posiblemente puedan ser sancionados a anticipar con razonable certeza el impacto económico y jurídico de un eventual procedimiento sancionatorio, lo cual debilita los mecanismos de prevención, cumplimiento normativo y gestión del riesgo regulatorio en el ámbito empresarial.

Lo anterior puede generar incertidumbre en el sector empresarial y, además, podría derivar en la liquidación judicial de una empresa sancionada por el incumplimiento de la Ley 1581 de 2012. Esto se debe a que, al no conocer ni poder prever con certeza el alcance de la sanción, podría ocurrir que una empresa carezca de la liquidez necesaria para asumirla. En efecto, la sanción impuesta podría superar su flujo de caja o incluso comprometer su rentabilidad, lo que imposibilitaría su pago y, en consecuencia, llevaría a la disolución y liquidación de la compañía.

Sin perjuicio de lo anterior, de conformidad con los casos analizados anteriormente, se evidencia que, en la práctica las sanciones impuestas por la SIC tienden a ser menos severas que las contempladas en el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD), incluso frente a incidentes graves. Asimismo, la autoridad colombiana ha recibido críticas por la falta de publicación sistemática de sus decisiones, lo que limita la función ejemplarizante y pedagógica del régimen sancionatorio.

- **Sobre la protección de datos personales a terceros países**

Como resultado de este análisis comparativo, se evidencia similitud en cuanto a la transferencia internacional de datos personales a terceros países, similitud encontrada en cuanto a la aplicación de cooperación internacional, en cuanto a la necesidad de un documento jurídico como garantía de

la transferencia, sin embargo, se considera conveniente que Colombia adopte cláusulas tipo, como las desarrolladas en la normativa europea y las cuales fueron desarrolladas en la sección (ii) del presente escrito, tal inclusión se sugiere será por vía normativa, un modelo similar en lo concerniente a la transferencia internacional de datos en la Unión Europea. Tal adopción permitiría reducir los márgenes de discrecionalidad contractual, estandarizar los compromisos exigibles en materia de protección de datos en el contexto de flujos internacionales y facilitar la interoperabilidad regulatoria con socios comerciales en jurisdicciones más estrictas. En ese sentido, se recomienda la implementación progresiva de un mecanismo de cláusulas contractuales tipo en Colombia, con el fin de garantizar un nivel adecuado y homogéneo de protección en el tratamiento transfronterizo de datos personales.

Al inicio del presente estudio se tenía pensado realizar un análisis de contenido teniendo en cuenta la decisión de ejecución (UE) 2021/914 de la comisión de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el reglamento (UE) 2016/679 de Parlamento Europeo y del consejo, en comparación con las cláusulas tipo o modelo existentes en Colombia, sin embargo, el resultado de la investigación tuvo como hallazgo la inexistencia de este clausulado tipo en Colombia.

Por lo anterior, la sugerencia de la inclusión de cláusulas tipo de acuerdo con Michaels y Jansen (2006), se evidencia como una manera de respetar la autonomía privada de la voluntad, permitiendo articular la regulación de relaciones jurídicas en ámbitos transnacionales. Estas cláusulas desempeñan un papel central en la regulación contemporánea, al facilitar la conexión entre normas privadas transnacionales y las legislaciones nacionales, manteniendo cierta coherencia normativa y contribuyendo a la normalización de prácticas contractuales más allá de la estructura estatal tradicional (Michaels & Jansen, 2006, pp. 843–861). Lo anterior, respetando la

autonomía de la voluntad privada[38] en materia contractual, la cual en palabras del Dr. Hinestrosa (2014). La autonomía privada, es entendida como la concurrencia entre el poder de disposición particular y el poder normativo estatal del ordenamiento jurídico, autonomía que permite la colaboración entre ambos y reconoce a los particulares la facultad de disciplinar sus propias relaciones jurídicas, atribuyéndoles una esfera de interés y de iniciativa para su reglamentación, sin embargo, se sugieren las cláusulas tipo, para con ello delimitar ciertas disposiciones contractuales que podrían conllevar el abuso en contra del titular de los datos personales.

Del resultado del análisis comparativo antes realizado se presente el siguiente cuadro comparativo para mayor facilidad del lector.

Sujeto de análisis	**En cuanto al reporte de un eventual incidente de seguridad de la información frente al tratamiento de datos personales**	**En cuanto a la transferencia internacional de datos a terceros países**	**En cuanto a las sanciones**	**En cuanto a los principios rectores del marco jurídico en materia de tratamiento de datos personales**
Colombia	Se establece obligación de reporte dentro de los 15 días hábiles siguientes a su detección.	Se cumple con el principio de reciprocidad, cooperando internacionalmente para la transferencia de datos, sin embargo, la regla general es la prohibición y se establecieron ciertas excepciones. No existen cláusulas tipo como garantía.	Se evidencian sanciones económicamente inferiores, sin embargo, se observa que los criterios de graduación de una sanción son: a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la	Se evidencian los siguientes principios rectores: Principio de legalidad en materia de tratamiento de datos; Principio de finalidad; Principio de libertad; Principio de veracidad o calidad; Principio de transparencia; Principio de acceso y circulación restringida; El Principio de

[38] Hinestrosa, F. (2014). Función, límites y cargas de la autonomía privada. Revista de Derecho Privado, (26), 5-39.

			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.	seguridad; Principio de confidencialidad.
Unión Europea	Se establece un plazo de 72 horas desde el conocimiento del incidente, en caso	Se cumple con la cooperación internacional, se requiere autorización por medio de	Se establecen criterios claros frente a las sanciones a impartir, los	Se identificaron los siguientes principios: Principio de licitud, lealtad y transparencia;

	de no ser reportado en este periodo, debe ir acompañada de una justificación de la demora.	documento jurídico para la transferencia, se implementan cláusulas tipo como garantía del titular del dato personal.	cuales responden a (i) La naturaleza, gravedad y duración de la infracción; (ii) El número de titulares afectados y el nivel de daño sufrido; (iii) Si la infracción fue intencional o negligente; (iv) Las medidas adoptadas para mitigar el daño; (v) El grado de responsabilidad del infractor; (vi) Cualquier infracción anterior relacionada. Pese a esto, son más cuantiosas las sanciones comparadas con Colombia.	Principio de limitación de la finalidad; Principio de minimización de datos; Principio de exactitud.

Conclusiones

Por lo expuesto durante el presente trabajo de investigación, se puede decir que, Colombia cuenta con una regulación básica en materia de transferencia internacional de datos, pero carece de mecanismos estructurados de garantías equivalentes a los del Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo (RGPD), lo que genera inseguridad jurídica y dependencia excesiva del consentimiento individual. La Unión Europea, en cambio, ha desarrollado un sistema

completo que permite flexibilidad y seguridad para las empresas, protegiendo al mismo tiempo los derechos de los titulares, por medio de clausulas tipo por ejemplo.

La recomendación principal es avanzar hacia un modelo híbrido, que complemente el consentimiento con mecanismos objetivos de garantía, como cláusulas tipo, normas corporativas vinculantes obligatorias, fortaleciendo así la protección efectiva de los datos en el contexto internacional.

De conformidad con lo expuesto por medio del presente escrito, se observa como conclusión que posterior al incremento en tecnología se refleja un aumento en ciber ataques, conllevando ello que, se deba migrar a un sistema más robusto tecnológicamente desde la prevención de estos incidentes digitales, estructuras que se recomienda implementar de manera interna en cada una de las empresas, aunado a ello, se puede identificar que el tratamiento de datos personales es un aspecto que frente a la legislación colombiana está regulado, sin embargo, se encuentra de una manera superflua y que no corresponde a las necesidades actuales, razón por la cual, se presenta un análisis de derecho comparado con la legislación de España y Suecia, conllevando ello y evidenciando aspectos a mejorar e implementar en la regulación colombiana.

Además de ello, se denota la importancia de generar consciencia al interior de la compañía, sobre el tratamiento de datos personales responsable, es decir, contar con una policita de tratamiento de datos robusta, con un plan de respaldo frente a la presencia de un incidente digital y además de esto, contar con el esquema pertinente para realizar el reporte ante la entidad responsable de conocer de este asunto, que a la fecha del presente documento en Colombia es la Superintendencia de Industria y Comercio. Por todo lo anterior, se recomienda implementar en Colombia por medio del órgano legislativo, lo pertinente para prever, regular y mitigar el riesgo evidenciado por medio del presente escrito, determinando en mayor medida la responsabilidad del responsable del

tratamiento de datos y un paso a paso sobre la debida implementación de esquema de prevención de incidentes digitales.

Es importante mencionar entonces que, dentro de los hallazgos de la presente investigación se tiene que, en Colombia pese a existir normas de tratamiento de datos personales, las mismas no son suficientes para la prevención y gestión de incidentes de seguridad, pues se evidencia de las sanciones impuestas que se siguen presentando cada año las mismas circunstancias, por ello toma relevancia generar una cultura de datos personales, que incluya un conocimiento de las normas, un paso a paso para la prevención y gestión de los incidentes de seguridad de la información y aunado a ello, sanciones ejemplificadoras, sin perjuicio de ello, también toma relevancia la implementación de clausulados tipo, cerrando o minimizando así el riesgo del incumplimiento de autorizaciones por parte de los titulares de los datos personales.

Bibliografía:

- Cámara Colombiana de Informática y Telecomunicaciones. (2024). Estudio anual de ciberseguridad.https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology.
- Comisión de Protección de Datos de Irlanda. (2024, septiembre 26). Decisión IN-19-4-1.
- Comisión Nacional de Protección de Datos de Luxemburgo. (2021, julio 15). Sentencia.

- Comité Europeo de Protección de Datos. (2022). Directrices 9/2022, sobre la notificación de las violaciones de la seguridad de los datos personales en el marco del RGPD.
- Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. DO: 48489.
- Congreso de la República de Colombia. (2012). Ley 1581 de 2012, artículo 23. DO: 48489.
- Constitución Política de Colombia. (1991). Constitución Política de Colombia. Artículos 15, 20, 241.
- Corte Constitucional de Colombia. (1997). Sentencia 7-552/1997. (MP. Vladimiro Naranjo Mesa.)
- Corte Constitucional de Colombia. Sentencia C-748/2011. (MP. Jorge Ignacio Pretelt Chaljub.)
- Corte Constitucional de Colombia. (2015). Sentencia T277/2015. (MP. María Victoria Calle Correa.)
- Corte Constitucional de Colombia. (2016). Sentencia T 050/2016. (MP. Gabriel Eduardo Mendoza Martelo)
- Corte Constitucional de Colombia. (2021). Sentencia SU-139/21 (MP. Jorge Enrique Ibáñez Najar).
- Corte Constitucional de Colombia. (2022). Sentencia T-143/22 (MP. Alejandro Linares Cantillo).
- Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021. (2021). Relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países en conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

- Diario Oficial de la Unión Europea. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Artículo 33. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf
- Diario oficial de la Unión Europea. (2021). DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN EUROPEA.
- García, A. A. (2019). Ciberseguridad: ¿Por qué es importante para todos? Siglo XXI Editores México.
- Grupo de trabajo de protección de datos. Dictamen 03/2014 sobre la notificación de violación de datos personales.
- Hinestrosa, F. (2014). Función, límites y cargas de la autonomía privada. Revista de Derecho Privado, (26), 5–39.
- Machuca Vivar, Silvio Amable; Vinueza Ochoa, Nelly Valeria; Sampedro Guaman, Carlos Roberto y Santillan Molina, Alberto Leonel. Habeas data y protección de datos personales en la gestión de las bases de datos. Universidad y Sociedad [online]. 2022, vol.14, n.2 [citado 2025-06-12], pp.244-251. Disponible en: <http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000200244&lng=es&nrm=iso>. Epub 02-Abr-2022. ISSN 2218-3620.
- Merryman, J. H., & Pérez-Perdomo, R. (2018). The civil law tradition: An introduction to the legal systems of Europe and Latin America (4.ª ed.). Stanford University Press.
- Miranda, Diego Andrés. (2023, 17 octubre). Los Datos Personales y su regulación en Colombia (datos sensibles, datos públicos, semiprivado y privado): Blog Jurídico - TECH. https://telecomunicaciones.uexternado.edu.co/los-datos-personales-y-su-regulacion-en-

colombia-datos-sensibles-datos-publicos-semiprivado-y-privado-enfoque-ambito-de-aplicacion-y-contenido/

- Michaels, R., & Jansen, N. (2006). Private law beyond the state? Europeanization, globalization, privatization. The American Journal of Comparative Law, 54(4), 843–909. https://doi.org/10.1093/ajcl/54.4.843
- Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (s.f.). Boletines No. 2 al No. 9.
- Oficina del Comisionado de Información. (s.f.). Case ref: COM0783542.
- Ovejero y Maury, E. (1917). Sistema de lógica inductiva y deductiva. Madrid: Daniel Jorro.
- Parlamento Europeo, Consejo de la Unión Europea y Comisión Europea. (2012, octubre 26). Carta de los Derechos Fundamentales de la Unión Europea. https://www.refworld.org/es/leg/trat/ue/2012/es/129076
- Personería de Bogotá D.C. ABC de las acciones de tutela. Incidente de desacato e impugnaciones. Disponible en: https://www.personeriabogota.gov.co/images/libros/ABC_DE_LAS_ACCIONES_DE_TUTELA_DIGITAL-2.pdf
- Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Compilado por medio del decreto 1074 de 2015.
- Presidencia de la República de Colombia. (2015). Decreto 1081 de 2015. Decreto Único Reglamentario del Sector Presidencia de la República.
- Presidencia de la República de Colombia. (2022). Decreto 255 de 2022. Adición de normas corporativas vinculantes sobre protección de datos personales.

- Ramírez Torrado, M. L. (2010). Reflexiones acerca del principio de proporcionalidad en el ámbito del derecho administrativo sancionador colombiano. Estudios Socio-Jurídicos, 12(2), 209–242.
- Superintendencia de industria y Comercio. (2015) Circular Externa No. 02. Por medio de la cual se imparten instrucciones a los Responsables del Tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las Cámaras de Comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el Registro Nacional de Bases de Datos (RNBD).
- Superintendencia de industria y Comercio. (2018) Circular externa No. 003. Por medio de la cual se modifican los numerales 2.1 al 2.4 y eliminar los numerales 2.5 al 2.7 del capítulo segundo del título V de la Circular Única de la Superintendencia de Industria y Comercio.
- Superintendencia de Industria y Comercio. (2020). Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales. Disponible en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf
- Superintendencia de Industria y Comercio. (2021). Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability). Disponible en: https://www.sic.gov.co/sites/default/files/files/2021/2021%20Guías%20para%20implementación%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf
- Superintendencia de Industria y Comercio. (2022). Circular Única. Título V. Numeral 2.1. literal F. (ii). Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/092022/Título%20V%20Versión%2029-09-2022.pdf

- Superintendencia de Industria y Comercio (2024). Circular externa No. 03. Por medio de la cual se dictan instrucciones para los administradores societarios en relación con el tratamiento de Datos personales.
- Superintendencia de Industria y Comercio. Resolución 16582 del 31 de marzo de 2025. Radicación 22-301462.
- Superintendencia de Industria y Comercio. (2025). Proyecto Normativo: "Lineamientos sobre el tratamiento de datos personales en el ecosistema fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros". Disponible en: https://sedeelectronica.sic.gov.co/transparencia/normativa/proyecto-normativo-lineamientos-sobre-el-tratamiento-de-datos-personales-en-el-ecosistema-fintech-y-los-modelos-de-negocio
- Taj, I., & Zaman, N. (2022). Towards industrial revolution 5.0 and explainable artificial intelligence: Challenges and opportunities. International Journal of Computing and Digital Systems, 12(1), 295–320.
- Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving decisions about health, wealth, and happiness. Yale University Press. https://books.google.com.co/books?id=dSJQn8egXvUC
- Veronese, A., Silveira, A., Lemos Igreja, R., Lopes Espiñeira Lemos, A. N., & Guimarães Moraes, T. (2023). El concepto de cultura de protección de datos personales en los documentos de la Unión Europea: ¿un "efecto Bruselas" en América Latina? UNIO – Revista de Derecho de la Unión Europea, 9(1), 65–89.