Superintendencia de
Industria y Comercio

CIRCULAR EXTERNA No. 003 DE 2024
22 de agosto de 2024

Para: Administradores de entidades vigiladas por la Superintendencia de Industria y Comercio en su rol de Autoridad de Protección de Datos personales.

Asunto: Instrucciones para los administradores societarios en relación con el Tratamiento de Datos personales.

Consideraciones

El artículo 2 de la Constitución Política de Colombia señala como uno de los fines esenciales del Estado: "*garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución*". Se desprende de ello, la exigencia tanto a particulares como a autoridades de garantizar resultados concretos para materializar el conjunto de las disposiciones constitucionales, legales y reglamentarias, entre las que se encuentran las relacionadas con la protección al *Habeas Data* y con el debido Tratamiento de Datos personales previstos en el artículo 15 de la Constitución.

El artículo 333 de la Constitución Política de Colombia establece que "*la actividad económica y la iniciativa privada son libres, dentro de los límites del bien común*". Dicho mandato constitucional resalta que la "*libre competencia económica es un derecho de todos que supone responsabilidades*" y que la "*empresa, como base del desarrollo, tiene una función social que implica obligaciones*". Dentro de tales obligaciones se encuentran aquellas que permiten materializar los derechos de los Titulares de los Datos personales.

Cuando la forma jurídica escogida para desarrollar una actividad empresarial es una sociedad, los administradores de esta cumplen un papel esencial para el cumplimiento de tales obligaciones. Parte de esas disposiciones legales incluyen las normas sobre Tratamiento de Datos personales, como lo son, entre otras, las leyes estatutarias 1266 de 2008, 1581 de 2012, 2157 de 2021 y sus decretos reglamentarios[1]. Así, siendo el Tratamiento de Datos personales parte de la actividad de las empresas, los administradores societarios están obligados a actuar con la diligencia de un buen hombre de negocios velando por el estricto cumplimiento de las disposiciones legales y reglamentarias.

La Corte Constitucional, en la sentencia C-123 de 2006, resaltó la importancia de los administradores debido al impacto que tienen en el orden social y económico de país. Indicó la Corte:

> *"Puede concluir la Corte, que en materia de sociedades, dada la importante labor que desempeñan sus administradores, en razón a la gran responsabilidad que*

[1] Téngase presente: Decreto 2952 de 2010 (incorporado en el Decreto único Reglamentario 1074 de 2015), Decreto 1377 de 2013 (incorporado en el Decreto único Reglamentario 1074 de 2015) y el Decreto 255 de 2022.

asumen y la repercusión que sus actuaciones pueden tener en el desarrollo social, ha sido la ley la que les ha impuesto de manera general a éstos, ejercer sus funciones con sujeción a los principios de lealtad y buena fe, así como actuar con la diligencia de un buen hombre de negocios, en interés de la sociedad y teniendo en cuenta los intereses de sus asociados. En tal medida, la actuación de los administradores debe ir más allá de la diligencia común y corriente, pues su gestión profesional de carácter comercial debe orientarse al cumplimiento de las metas propuestas por la sociedad".

En materia de Tratamiento de Datos personales impera como regla de responsabilidad el deber de responsabilidad demostrada o "*accountability*", el cual exige a los administradores societarios adoptar medidas útiles, oportunas, eficientes y demostrables para acreditar el total y correcto cumplimiento de la regulación. Lo anterior, se ve materializado en el artículo 19A de la Ley Estatutaria 1266 de 2008, que establece: "*Los operadores, fuentes y usuarios de información financiera, crediticia, comercial y de servicios* ***deben ser capaces de demostrar*** *que han implementado medidas apropiadas, efectivas y verificables para cumplir con las obligaciones establecidas en la Ley 1266 de 2008*" (subrayado fuera de texto). Y, a su vez, en el artículo 26 del Decreto 1377 de 2013 (incorporado en el Decreto Único Reglamentario 1074 de 2015) al establecer que: "*Los Responsables del Tratamiento de Datos personales* ***deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio****, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto*". (Subrayado fuera de texto).

El literal e) del del artículo 3 de la Ley Estatutaria 1581 de 2012 define al Responsable del Tratamiento como "*Persona natural o jurídica, pública o privada,* ***que por sí misma o en asocio con otros****, decida sobre la base de datos y/o el Tratamiento de los datos*". (Destacado fuera de texto).

Por su parte, la Corte Constitucional, en Sentencia C–748 de 2011, al revisar la constitucionalidad de la definición de Responsable del Tratamiento, estableció que:

> "(...) *no basta con que una ley o un contrato señalen expresamente que una determinada persona o* ***grupo de personas son Responsables del Tratamiento****, por cuanto en cada caso corresponderá analizar el contexto de las actuaciones de los agentes concernidos en el Tratamiento del dato para establecer su verdadera posición y, en este orden, sus obligaciones y régimen de responsabilidad. En ese orden de ideas,* ***corresponderá a la autoridad competente de asegurar la vigilancia****, control y garantía del dato personal****, examinar la posición que ocupa cada agente en el Tratamiento del dato****, en especial****, porque como lo señala la misma definición de Responsable*** *y de encargado del Tratamiento,* ***éstos pueden estar constituidos por una pluralidad de sujetos que pueden tener distintos grados de responsabilidad****.*

Finalmente, como ejemplifica la Directiva referida –ejemplos que la Sala considera también son aplicables a nuestro caso, ***el Responsable del Tratamiento puede surgir****: (i) cuando en el cumplimiento de una determinada función, se impone la recolección de datos, por ejemplo, en el caso de la seguridad social; la directiva en comento denomina esta situación competencia legal explícita; (ii) cuando en el ámbito propio de la actividad se produce el Tratamiento, se trata del caso de los empleadores frente a sus trabajadores, lo que se denomina competencia jurídica implícita; y (iii)* ***cuando sin existir las competencias anteriores, se tiene la capacidad de determinación, hecho que se denomina capacidad de influencia de hecho****."*[2]. (Destacado fuera de texto).

Así, siguiendo el alcance de la definición de "Responsable del Tratamiento", los administradores societarios serán corresponsables del Tratamiento cuando en conjunto con la persona jurídica determinen, respecto de unas operaciones de Tratamiento específicas, o bien los **fines** o bien aquellos elementos esenciales de los **medios** que caracterizan al Responsable del Tratamiento.

En materia de datos personales, la Superintendencia de Industria y Comercio tiene entre las funciones asignadas por la Ley Estatutaria 1581 de 2012, las de "*velar por el cumplimiento de la legislación en materia de protección de datos personales*" e "*impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley*"[3].

Las circulares no tienen como propósito repetir exactamente lo que la ley dice. Las circulares son instrumentos normativos para ampliar y actualizar nociones jurídicas. Las circulares tienen la vocación de dar alcance a lo establecido en la norma y ampliar, actualizar y adaptar el marco de aplicación como poder instructivo de la administración a luz de las facultades otorgadas por la Ley Estatutaria 1581 de 2012 a la Autoridad de datos personales. Justamente, afirma la Función Pública que "*Las circulares deben expresar el criterio jurídico o interpretación que un órgano administrativo formula en textos un tanto complejos sobre la legislación que aplica*"[4].La naturaleza jurídica de los datos personales están determinada por cambios tecnológicos constantes, cambios sociales y practicas nuevas de las empresas. El rol de la Autoridad es responder a los nuevos desafíos jurídicos con un alto grado de especificidad y tecnicismo, buscando desarrollar un marco de protección integral y reforzado al derecho fundamental al *Habeas Data.*

---

[2] Sobre el particular la Corte Constitucional trae a colación el Dictamen 1/2010 sobre los conceptos de «Responsable del tratamiento» y «encargado del tratamiento» del Grupo del Artículo 29 sobre Protección de Datos. Documento disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf#:~:text=Dictamen%201%2F2010%20sobre%20los%20conceptos%20de%20%C2%ABResponsable%20del,protecci%C3%B3n%20de%20datos%20y%20derecho%20a%20la%20intimidad.

[3] Literales a) y e) del artículo 21 de la Ley Estatutaria 1581 de 2012.

[4] Concepto 100921 de 2021 Departamento Administrativo de la Función Pública del 23 de marzo del 2021.

Por su parte, el numeral 55 del artículo 1º del Decreto 092 de 2022 señala que la Superintendencia de Industria y Comercio tiene la función de impartir instrucciones en materia de administración de datos personales, fijar criterios que faciliten su cumplimiento y señalar los procedimientos para su cabal aplicación.

Conductas y deberes de los administradores

La Superintendencia de Industria y Comercio instruye a los administradores societarios de entidades bajo nuestra vigilancia, acerca del alcance de las obligaciones en el Tratamiento de Datos personales, como se indica a continuación:

I. Los administradores están obligados al cumplimiento de los establecido por la regulación relativa a la protección de datos personales.

II. Las *Políticas Internas Efectivas*[5] que establezcan los administradores para garantizar el debido Tratamiento de Datos personales en la actividad económica deben ser objeto de monitoreo y control para garantizar su cumplimiento.

III. La adopción de mecanismos internos para hacer cumplir las *Políticas Internas Efectivas*, incluyendo herramientas de implementación, entrenamiento y programas de sensibilización, deben ser conocidas y promovidas por los administradores. Para lograr estos objetivos, se puede: i) designar a la persona o al área que asumirá la función de protección de Datos personales dentro de la organización; ii) aprobar y verificar el real y efectivo cumplimiento de un manual interno de políticas y procedimientos[6] para garantizar el adecuado cumplimiento de las normas; iii) establecer canales de comunicación que le permitan a la persona o al área responsable informar de manera periódica a los administradores sobre la ejecución de las *Políticas Internas Efectivas* de la organización.

IV. Los administradores deben establecer los lineamientos corporativos adecuados para adoptar medidas precautorias o preventivas para proteger los derechos de los titulares de Datos personales, como lo son, por ejemplo, los estudios de impacto de privacidad[7].

Los estudios de impacto de privacidad podrían incluir, como mínimo, lo siguiente:

1. Una descripción detallada de las operaciones de Tratamiento de Datos personales.

---

[5] Artículo 27 del Decreto 1377 de 2013 (incorporado en el Decreto Único Reglamentario 1074 de 2015).
[6] El literal k) de la Ley Estatutaria 1581 de 2012 establece el deber de "Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos".
[7] Previo al diseño y desarrollo del proyecto de cualquier organización, y en la medida en que sea probable que el mismo entrañe un alto riesgo de afectación del derecho a la Protección de Datos personales de los Titulares, se sugiere efectuar una evaluación de impacto en la con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos para garantizar que los datos se tratarán debidamente y conforme con la regulación existente.

2. Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los Datos personales. En la evaluación de riesgos se espera, por lo menos, la identificación y clasificación estos.
3. Las medidas previstas para evitar la materialización de los riesgos, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de Datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas que puedan eventualmente resultar afectadas.

V. Los administradores deben establecer los lineamientos para fortalecer continuamente las medidas de seguridad de la información. En especial, el manual interno de políticas debería involucrar un componente de gestión de riesgos que le permita a la empresa identificar sus vulnerabilidades a tiempo y enfocar sus recursos en la adopción de las medidas de mitigación de riesgos, tanto para ellas como para los Titulares de la Información[8].

En armonía con las normas citadas y la jurisprudencia constitucional, los administradores societarios serán corresponsables del Tratamiento cuando en conjunto con la persona jurídica determinen, respecto de unas operaciones de Tratamiento específicas, los fines o los medios sobre la base de datos y/o el Tratamiento de los datos.

De esa manera, estas instrucciones armonizan las anteriores normas para garantizar el fin constitucional de una efectiva protección del derecho al *Habeas Data* y al debido Tratamiento de datos personales.

Cordialmente,

CIELO ELAINNE RUSINQUE URREGO
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Elaboró: Grenfieth Sierra/ Alejandro Londoño
Revisó: Héctor Barragán / Grenfieth Sierra
Aprobó: Grenfieth Sierra /Gabriel Turbay

[8] Esta Superintendencia de Industria y Comercio ha puesto a disposición de los sujetos obligados la "GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALESDATOS PERSONALES". Para mayor detalle en la materia: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf