SUPERINTENDENCIA DE SOCIEDADES

OFICIO 220-090221 DEL 02 DE MAYO DE 2023

REFERENCIA: **RADICACIÓN 2023-01-156740**
ASUNTO: **EL DESARROLLO E IMPLEMENTACIÓN DEL SAGRILAFT POR PARTE DE LA EMPRESA OBLIGADA DEBERÁ RESPETAR LAS DISPOSICIONES LEGALES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES CONTENIDAS EN LAS LEYES 1266 DE 2008, 1581 DE 2012 Y DEMÁS NORMAS APLICABLES**

Acuso recibo del escrito citado en la referencia, con el cual presenta una consulta relacionada con el SAGRILAFT.

Antes de resolver lo propio, debe reiterarse que la competencia de esta Entidad es eminentemente reglada y sus atribuciones se hayan enmarcadas en los términos del numeral 24 del artículo 189 de la Constitución Política, en concordancia con los artículos 82, 83, 84, 85 y 86 de la Ley 222 de 1995 y el Decreto 1736 de 2020, modificado por el Decreto 1380 de 2021.

Así, al tenor de lo dispuesto en el numeral 2 del artículo 11 del Decreto 1736 de 2020, es función de la Oficina Asesora Jurídica de esta Entidad absolver las consultas jurídicas externas en los temas de competencia de la Superintendencia de Sociedades, salvo las que correspondan a actuaciones específicas adelantadas por las dependencias de la Entidad y, en esa medida, emite un concepto u opinión de carácter general y abstracto que como tal no es vinculante ni compromete su responsabilidad.

Con el alcance indicado, este Despacho procede a responder sus inquietudes en el mismo orden en que fueron plantadas:

> ***"Amablemente solicito a ustedes me expidan un concepto jurídico respecto al deber de la oficial de cumplimiento del Sagrilaft frente a la protección de los datos personales de las contrapartes. Es importante conocer cómo se articula la ley de sagrilaft con la ley de protección de datos para la garantía de los derechos de los titulares"***

Sobre el particular, es precioso señalar que el numeral 5.5 de la Circular Externa 100-000016 de 24 de diciembre de 2020 de la Superintendencia de Sociedades, establece que las actividades adoptadas por la Empresa Obligada, en desarrollo de la implementación y ejecución del SAGRILAFT, deben reposar en documentos y registros que garanticen la integridad, oportunidad, confiabilidad, reserva y disponibilidad de la información.

La información suministrada por la Contraparte, como parte del proceso de Debida Diligencia y Debida Diligencia Intensificada, así como el nombre de la persona que la verificó, deben quedar debidamente documentadas con fecha y hora, a fin de que se pueda acreditar la debida y oportuna diligencia por parte de la Empresa Obligada. De cualquier forma, el desarrollo e implementación del SAGRILAFT por parte de la Empresa Obligada deberá respetar las disposiciones legales en materia de protección de datos personales contenidas en las Leyes 1266 de 2008, 1581 de 2012 y demás normas aplicables. Asimismo, los soportes deberán conservarse de acuerdo con lo previsto en el artículo 28 de la Ley 962 de 2005, o la norma que la modifique o sustituya.

Del mismo modo, el numeral 5.6 de la referida Circular establece que la Empresa Obligada y el Oficial de Cumplimiento deberán garantizar la reserva del reporte de una Operación Sospechosa remitido a la UIAF, según lo previsto en la Ley 526 de 1999 y demás normas que la adicionen, modifiquen o sustituyan.

> ***"Solicito adicionalmente me compartan un modelo de privacidad desde el diseño y por defecto para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento de los datos, teniendo en cuenta la privacidad en todo el ciclo de un proceso desde su inicio hasta el final."***

La Oficina Asesora Jurídica en las respuestas a las consultas no puede definir cuál es el *"diseño o modelo de privacidad"* que deberían implementar las Empresas Obligadas a implementar el SAGRILAFT, por cuanto este aspecto queda bajo la exclusiva responsabilidad de la Empresa Obligada.

"Requiero además que en el concepto jurídico se indique cuáles serían los posibles riesgos a los cuáles se encuentran expuestos los titulares de la información con ocasión a las operaciones de consultas de bases de datos del sagrilaft y si es considerada una buena práctica que la organización entregue la responsabilidad de consultar las bases de datos sagrilaft en varios colaboradores. En caso de ser considerada una buena práctica, ¿Á Cuáles son las medidas organizativas que se deben tener en cuenta para no vulnerar los derechos fundamentales a la intimidad y a la protección de los datos de los titulares? (sic)".

Sobre el particular, se pone de presente que la Superintendencia de Sociedades no es autoridad en materia de datos personales y que no puede valorar, calificar o aprobar si una medida como las que sugiere en el escrito de consulta, puede ser considerada como buena práctica para resguardar información personal. Sin perjuicio de lo anterior, se recuerda que en el desarrollo e implementación del SAGRILAFT por parte de la Empresa Obligada deberá respetar las disposiciones legales en materia de protección de datos personales contenidas en las Leyes 1266 de 2008, 1581 de 2012 y demás normas aplicables y, por lo tanto, le corresponde a la Empresa Obligada adoptar todas las medidas organizativas que consideren necesarias para dar cumplimiento a las normas legales, de acuerdo con la estructura de su negocio.

A su vez, es preciso recordar que la Corte Constitucional mediante Sentencia C-748-11 de 6 de octubre de 2011, señaló lo siguiente frente al uso de datos personales:

"2.4.5.4. Constitucionalidad del literal b): la excepción "las bases de datos o archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo"

2.4.5.4.1. Como se indicó en la sentencia C-251 de 2002, "una de las finalidades básicas de las autoridades colombianas es la defensa de la integridad nacional y la preservación del orden público y de la convivencia pacífica, no sólo porque así lo establece expresamente el artículo 2º de la Carta, sino además porque esos elementos son condiciones materiales para que las personas puedan gozar de sus derechos y libertades".

Las labores de defensa y seguridad, a diferencia de las de inteligencia y contrainteligencia –como se verá más adelante- tienen lugar con ocasión de la existencia de amenazas actuales y graves contra el orden público y la soberanía, y solamente pueden ser ejecutadas por la Fuerza Pública. Amenazas de tal magnitud justifican el tratamiento de datos personales para los propósitos de defensa y seguridad nacional; es más, esta Corporación ha indicado que el tratamiento de datos personales para esos propósitos "(…) es un elemento importante para el logro de sus fines constitucionales de mantenimiento del orden constitucional y de las condiciones necesarias para el ejercicio adecuado de los derechos y libertades previstos en la Carta", es decir, se trata de una herramienta importante de la que disponen las autoridades para cumplir sus funciones de defensa.

Sin embargo, como lo ha indicado esta Corporación, la defensa del orden público y de la integridad de la soberanía no pueden servir de excusa para desconocer las garantías básicas del estado social de derecho e implementar un estado totalitario en el que las personas se conviertan en objetos al servicio del Estado. Por ello, toda labor de seguridad y defensa nacional debe ser compatible con la dignidad y los derechos fundamentales de las personas que puedan resultar afectadas. En este orden de ideas, la Sala reitera que el tratamiento de datos personales con estas finalidades debe sujetarse de manera estricta a las exigencias del principio de proporcionalidad.

2.4.5.4.2. Consideraciones similares deben realizarse para las excepciones de "prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo", pues tanto el lavado de activos como el terrorismo son amenazas importantes contra la seguridad y el orden público.

Por ejemplo, en la sentencia C-537 de 2008, la Corte reconoció que el delito de terrorismo conlleva una grave afectación "(…) de derechos y libertades de primer orden, lo que impone la obligatoriedad para el Estado de establecer medidas suficientes y eficaces, tanto en el ámbito internacional como del derecho interno, para prevenir, combatir y sancionar esas conductas." Dada la gravedad del delito, la Corte agregó que "(…) las decisiones que adopte el legislador dirigidas a implementar medidas para la prevención, represión y sanción del terrorismo son prima facie armónicas con el Estatuto Superior."[1]

[1] De forma similar, en la sentencia C-127 de 1993, M.P. Alejandro Martínez Caballero, la Corte concluyó *"que la comunidad internacional ha reconocido en forma unánime y reiterada que el terrorismo es un delito que por ser atroz tiene un trato distinto."* Luego, en la sentencia C-762 de 2002, M.P. Rodrigo Escobar Gil, la Corte reconoció que el terrorismo afecta

La Sala también observa que la adopción de medidas para combatir efectivamente el terrorismo es una obligación internacional del Estado colombiano derivada de instrumentos tales como el Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas, el Convenio Internacional para la Represión de la Financiación del Terrorismo y la Convención Interamericana contra el Terrorismo, todos ratificados por Colombia y sus leyes aprobatorias declaradas exequibles por esta Corporación.

En materia de lavado de activos, la Corte ha señalado que el establecimiento de medidas para prevenir y sancionar esta conducta es un aspecto inseparable del éxito de las medidas para la represión del crimen organizado. Además, ha reconocido que, dada la sofisticación de las redes dedicadas a este delito y su naturaleza transfronteriza, se requieren medidas especiales y el uso de la tecnología.

En este orden de ideas, dada la entidad de la amenaza que para el orden constitucional representan las conductas delictivas de terrorismo y lavado de activos, la Corte considera razonable que el tratamiento de datos para su prevención, detección, monitoreo y control sea exceptuado de la aplicación del proyecto bajo revisión, salvo en materia de principios[2].” (Subrayado nuestro).

En resumen, se debe tener en cuenta que cuando se está frente a delitos tales como financiamiento del terrorismo y el lavado de activos, estos son de tal envergadura que las políticas y programas destinados a su prevención y detección, deben ser desarrollados siguiendo los lineamientos establecidos por la Honorable Corte Constitucional, aplicando el principio de proporcionalidad.

En los anteriores términos su solicitud ha sido atendida en el plazo y con los efectos descritos en el artículo 28 del Código de Procedimiento Administrativo y de lo

---

gravemente distintos derechos fundamentales y, por tanto, se trata de una conducta cuya necesidad de investigación y sanción ha sido previsto por las normas del derecho internacional, entre ellas aquellas que tienen carácter de *ius cogens*.

[2] La necesidad de dar aplicación a los principios del habeas data en las labores de detección de la financiación de terrorismo ya había sido anunciada por la Corte en la sentencia C-537 de 2008, M.P. Jaime Córdoba Triviño, en la que la Corporación explicó: “(…) el intercambio de información financiera que prevén las disposiciones analizadas deberá, en todo caso, estar precedido de la garantía del derecho a la autodeterminación informativa de los afectados con las medidas, en los términos del artículo 15 C.P. Por lo tanto, las acciones que ejecute el Estado con el fin de cumplir con sus compromisos en la interdicción de recursos destinados a la financiación del terrorismo, deberán garantizar que los titulares de la información conserven la facultad de conocer, actualizar y rectificar los datos concernidos. De la misma manera, el tratamiento de esa información estará supeditado a la eficacia de los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad, conforme lo ha precisado la jurisprudencia constitucional.”

Contencioso Administrativo. Se invita al usuario a consultar en nuestra página WEB www.supersociedades.gov.co los conceptos y normativa emitidos por la entidad, así como la herramienta tecnológica Tesauro.