REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO _14679_ DE 2022

(Marzo 24 de 2022)

Por la cual se resuelve un recurso de apelación

Radicación 20-355760

VERSIÓN ÚNICA

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por el numeral 8 del artículo 16 del Decreto 4886 de 2011 (modificado por el artículo 6 del Decreto 92 de 2022), y

CONSIDERANDO

PRIMERO. Que mediante **Resolución N°. 31996 del 26 de mayo de 2021**, la Dirección de Investigaciones impuso una sanción pecuniaria a la sociedad CONDIVAL S.A.S., identificada con NIT 800.187.774-7 de TRES MILLONES CIENTO NOVENTA Y CINCO MIL CIENTO CUATRO PESOS M/CTE ($3.195.104) equivalentes a equivalentes a OCHENTA Y OCHO (88) Unidades de Valor Tributario Vigentes, por la violación de las disposiciones contenidas en el literal o) del art 17 de la Ley 1581 de 2012 en concordancia con el literal f) del artículo 21 de la norma en mención.

SEGUNDO. Que mediante comunicación recibida el 22 de junio de 2021 con radicado N°. 20-355760- 18, la sociedad CONDIVAL S.A.S. a través de su representante legal, interpuso recurso de reposición y en subsidio de apelación contra la resolución aludida, manifestando lo siguiente:

> En primer lugar, la sociedad investigada alega que, "(...) es necesario advertir que esta Dirección no puede ordenar el cumplimiento de la orden impartida en la Resolución No. 61479 del 7 de noviembre de 2019 dentro de los tres (3) días siguientes a la notificación de la Resolución No. 31996 del 26 de mayo de 2021, toda vez que esta última no se encuentra ejecutoriada, momento a partir del cual las órdenes e instrucciones contenidas en dicho acto administrativo cobran firmeza y son ejecutados por esta autoridad. En efecto, como bien lo señala el artículo tercero de la Resolución No. 31996 del 26 de mayo de 2021, contra esa decisión proceden los recursos de reposición y apelación dentro de los diez (10) días siguientes a su notificación, de manera que la citada Resolución se encontrará en firme cuando se resuelvan los recursos en sede administrativa, o cuando se venza el plazo para interponerlos y el administrado guarde silencio. Solo a partir de ese momento, todas las órdenes impartidas en la Resolución No. 31996 del 26 de mayo de 2021 serán de obligatorio cumplimiento y serán ejecutables (...)"[1].
>
> Adicionalmente, la sociedad investigada asegura que, "(...) En ese sentido, es confusa y ambigua la orden impartida por este Despacho en el en el artículo segundo de la Resolución No. 31996 del 26 de mayo de 2021, por cuanto no es claro si CONDIVAL cuenta o no con un término de tres (3) días o seis (6) meses para cumplir con la orden emitida en la Resolución No. 61479 del 7 de noviembre de 2019. En suma, en aras de que se garanticen los derechos fundamentales de CONDIVAL, es necesario que esta Dirección al momento de resolver el recurso de reposición y/o la Superintendencia Delegada al momento de decidir la apelación, se sirva aclarar que las ordenes impartidas en la Resolución No. 31996 del 26 de mayo de 2021 únicamente son exigibles y ejecutables al momento en que se decidan y notifiquen los recursos en sede administrativa (...)"[2].

[1] Recuperado de: Radicado N°. 20355760—0001800003. Página 3.
[2] Recuperado de: Radicado N°. 20355760—0001800003. Páginas 3 y 4.

Además, la sociedad investigada reitera que, "(...) En caso de que la pretensión principal sea resuelta desfavorablemente, el recurrente solicita que, de manera subsidiaria, se sirva aclarar el alcance de la orden contenida en la Resolución 61479 del 7 de noviembre de 2019, en el sentido de indicar si, visto que la sociedad sancionada no trata datos sensibles, debe efectivamente certificar a su Despacho cómo ha documentado sus prácticas en una Política de Seguridad de la Información o si, por el contrario, dado que no hace tratamientos de datos sensibles, le bastaría con acreditar y probar que ha implementado medidas de seguridad pertinentes, en los términos ordenados por la Ley 1581 de 2012 (...)"[3].

Por otro lado, la sociedad investigada argumentó que, *"(...) Estas condiciones de seguridad, como se explicó a su Despacho en los Descargos, se encuentran materializadas en una serie de medidas que han sido implementadas por CONDIVAL, y que han logrado, en la práctica, impedir de manera absoluta que se hayan presentado incidentes de seguridad que hayan resultado en la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos personales sobre los cuales hace tratamiento. Como consecuencia del error involuntario de CONDIVAL, que se informó a su Despacho en los descargos dentro de la investigación, esta sociedad reportó que trataba datos sensibles cuando en efecto no lo hace. CONDIVAL, valga la aclaración, no trata datos personales por el solo hecho de que así lo haya afirmado por equivocación involuntaria en el RNBD (...)"*[4].

Sumado a esto, la sociedad investigada aduce que: *"(...) La orden proferida por su Despacho en 2019, mediante la cual se exigió a CONDIVAL adoptar una política de seguridad de la información, se basó en una valoración hecha sobre información errada. Esa valoración hecha en 2019, por supuesto, no es imputable a su Despacho. Fue CONDIVAL, como se reconoció en los descargos, quien erradamente manifestó que trataba datos sensibles y fue dicha afirmación la que dio lugar a que su Despacho le ordenara documentar sus medidas de seguridad en una Política de Seguridad (...)"*[5].

Así mismo, la sociedad investigada indicó: *"(...) La Ley 1581 de 2012 no exige que los Responsables del tratamiento documenten sus prácticas de seguridad en una Política de Seguridad. Exige, eso sí, que se dispongan las condiciones de seguridad necesarias para impedir la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos. La decisión de ordenarle a Condival que fuera más allá de su deber legal, y que documentara una Política de Seguridad de la información, se desprendió de haber asumido que dicha entidad procesaba datos personales sensibles, hecho que se aclaró ya a su Despacho (...)"*[6].

Finalmente, la sociedad investigada solicitó: *"(...) (i) Revocar el artículo segundo de la Resolución recurrida, en el entendido que las medidas de seguridad informadas a su Despacho dan cuenta del efectivo despliegue de actividades encaminadas a prevenir la ocurrencia de incidentes de seguridad. (ii) En el evento de que dicha pretensión no sea acogida por su Despacho, solicitamos respetuosamente aclarar si, en criterio de la Superintendencia, las medidas informadas son insuficientes como medida de contención de potenciales incidentes de seguridad en los términos ordenados por el literal d) del artículo 17 de la Ley 1581 de 2012 y en consecuencia, se sirva también ampliar el término para presentar la Política de Seguridad a que hace referencia su Despacho, en un plazo que se debe contar desde la fecha de ejecutoria de la resolución sancionatoria, una vez resueltos los recursos que aquí se interponen (...)"*[7].

TERCERO. Que, efectuando el análisis del recurso de reposición, la Dirección de Investigación de Protección de Datos Personales de la Superintendencia de Industria y Comercio, mediante Resolución N°. 69805 del 28 de octubre de 2021 resolvió,

*"**ARTÍCULO PRIMERO: MODIFICAR** el artículo segundo del resuelve de la Resolución N°. 31996 del 26 de mayo de 2021 por las razones expuestas en la parte motiva de este acto administrativo, el cual quedará así:*

---

[3] Recuperado de: Radicado N°. 20355760—0001800003. Página 4.
[4] Ibídem.
[5] Recuperado de: Radicado N°. 20355760—0001800003. Página 5.
[6] Ibídem.
[7] Ibídem.

> ***"ARTÍCULO SEGUNDO: CONMINAR** a la sociedad **CONDIVAL S.A.S.** a que dentro del término de tres (3) días siguientes a la ejecutoria del presente acto administrativo, de estricto cumplimiento a la orden impartida por esta Superintendencia a través de la Resolución N°. 61479 del 07 de noviembre de 2019, so pena de que esta Superintendencia haga la respectiva aplicación del artículo 90 de la Ley 1437 de 2011".*
>
> ***ARTÍCULO SEGUNDO: CONFIRMAR** en sus demás partes la Resolución N°. 31996 del 26 de mayo de 2021".*

CUARTO. Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, se procederá a resolver el recurso interpuesto de acuerdo con las siguientes,

CONSIDERACIONES DEL DESPACHO

1. FUNCIONES DEL DESPACHO DEL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011[8] (modificado por el artículo 6 del Decreto 92 de 2022) establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destaca la siguiente:

> *"(…)*
>
> *8. Decidir los recursos de reposición y las solicitudes de revocatoria directa que se interpongan contra los actos que expida, así como los de apelación que se interpongan contra los actos expedidos por la Dirección a su cargo.*
>
> *(…)"*

2. DEL PRINCIPIO Y DEL DEBER DE SEGURIDAD EN EL DEBIDO TRATAMIENTO DE DATOS PERSONALES

Sin seguridad no existe debido tratamiento de datos personales. Es por eso que la Ley Estatutaria 1581 de 2012 señala, entre otras, lo siguiente:

> ***ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.** En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*
> *(...)*
> *g) **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
>
> ***ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO.** Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
> *(…)*
> *d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

[8] Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones.

Nótese que **la redacción del principio de seguridad tiene un criterio eminentemente preventivo**, lo cual obliga a los Responsables a adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información sobre las personas.

Como es sabido, la Corte Constitucional ha establecido que:

> *"Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
> *(...)*
>
> *En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. (...)*
>
> ***Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria.****"*[9] *(Destacamos).*

La sociedad CONDIVAL S.A.S., afirma que,

> "(*l)a Ley 1581 de 2012 no exige que los Responsables del tratamiento documenten sus prácticas de seguridad en una Política de Seguridad. Exige, eso sí, que se dispongan las condiciones de seguridad necesarias para impedir la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos. La decisión de ordenarle a Condival que fuera más allá de su deber legal, y que documentara una Política de Seguridad de la información, se desprendió de haber asumido que dicha entidad procesaba datos personales sensibles, hecho que se aclaró ya a su Despacho*".

No se ajusta a derecho esa aseveración toda vez que el Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015) ordena lo siguiente:

> *Artículo 26. Demostración. 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, en una manera que sea proporcional a lo siguiente:*
>
> *(…)*
>
> *En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales* ***deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas.***
>
> *(…)". (Destacamos).*

Como es sabido, el artículo 19 de la Ley Estatutaria 1581 de 2012, le otorgó competencia a esta entidad, a través de la Delegatura para la Protección de Datos Personales, para ejercer: "*(…) la vigilancia necesaria para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.*"

Asimismo, el artículo 21 determina las funciones que debe cumplir la Superintendencia de Industria y Comercio, en virtud de la competencia conferida por el artículo 19 mencionado:

> "*ARTÍCULO 21. FUNCIONES. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:*
>
> *a. "Velar por el cumplimiento de la legislación en materia de protección de datos* [sic] *personales;*

[9] Corte Constitucional. Sentencia C – 748 del 2011.

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

Visto lo anterior, existen expresas y suficientes facultades legales para que esta autoridad pueda impartir órdenes o instrucciones con miras a proteger el derecho al debido tratamiento de los datos personales.

No sobra traer a colación que, el artículo 21 fue declarado exequible por la Corte Constitucional mediante la Sentencia C-748 de 2011, la cual en su numeral 2.20.3, expresa:

> *"Esta disposición enlista las funciones que ejercerá la nueva Delegatura de protección de datos personales. Al estudiar las funciones a ella asignadas, encuentra esta Sala que todas corresponden y despliegan los estándares internacionales establecidos sobre la autoridad de vigilancia. En efecto, desarrollan las funciones de vigilancia del cumplimiento de la normativa, de investigación y sanción por su incumplimiento, de vigilancia de la transferencia internacional de datos y de promoción de la protección de datos."*

Así, la ley colombiana faculta a la Superintendencia de Industria y Comercio no solo para emitir órdenes o instrucciones sino para exigir el debido Tratamiento de los Datos personales. Por eso, emitir una orden es un acto respetuoso del marco legal.

En suma, las órdenes no son sanciones sino son medidas necesarias para, entre otras, hacer efectivo el derecho de hábeas data o para que los Responsables del Tratamiento y Encargados del Tratamiento cumplan correctamente los previsto en regulación con miras a garantizar el debido tratamiento de los datos personales y el respeto de los derechos de los Titulares de los datos.

Por lo expuesto, no se revocará el artículo segundo de la Resolución N°. 31996 del 26 de mayo de 2021. Así, la sociedad recurrente deberá acreditar el cumplimiento de las ordenes impartidas por esta autoridad.

3. LA SOCIEDAD RECURRENTE REALIZA UN TRATAMIENTO DE DATOS SENSIBLES

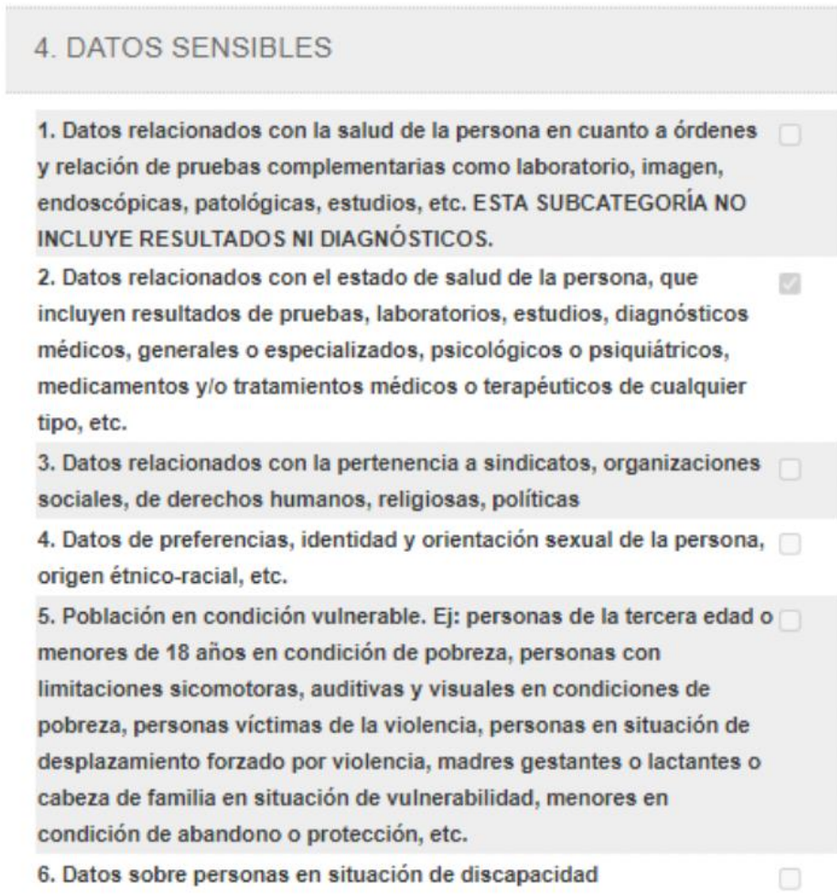
La recurrente afirma lo siguiente en su escrito de apelación:

> "*Como consecuencia del error involuntario de* ***CONDIVAL****, que se informó a su Despacho en los descargos dentro de la investigación, esta sociedad reportó que trataba datos sensibles cuando en efecto no lo hace.* ***CONDIVAL****, valga la aclaración, no trata datos personales por el solo hecho de que así lo haya afirmado por equivocación involuntaria en el RNBD*".

El artículo 5º de la Ley 1581 de 2012 establece lo siguiente:

> "*Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos* ***relativos a la salud****, a la vida sexual y los datos biométricos*". (Destacamos).

Por su parte, la sociedad CONDIVAL S.A.S. reportó la siguiente información en el Registro Nacional de Bases de Datos (RNBD) sobre la base de datos inscrita con el nombre de "empleados":



La recurrente reconoce en el Registro Nacional de Bases de Datos que trata datos sensibles como los relacionados con "el estado de salud de la persona". Por ende, no se ajusta a derecho que afirme que no realiza Tratamiento de datos de naturaleza sensible. Por lo tanto, está en la obligación de demostrar ante esta Superintendencia de Industria y Comercio cómo ha documentado sus prácticas en una Política de Seguridad de la Información en concordancia con lo establecido en la **Resolución N°. 61479 del 07 de noviembre de 2019**.

4. DEL TÉRMINO DE CUMPLIMIENTO DE LA ORDEN ADMINISTRATIVA

La sociedad recurrente afirma lo siguiente en su escrito de apelación,

> *"En suma, en aras de que se garanticen los derechos fundamentales de **CONDIVAL**, es necesario que esta Dirección al momento de resolver el recurso de reposición y/o la Superintendencia Delegada al momento de decidir la apelación, se sirva aclarar que las ordenes impartidas en la Resolución No. 31996 del 26 de mayo de 2021 únicamente son exigibles y ejecutables al momento en que se decidan y notifiquen los recursos en sede administrativa".*

Mediante Resolución Nº 69805 de 2021, "*Por la cual se resuelve un recurso de reposición y se concede el recurso de apelación*", la Dirección de Investigación de Protección de Datos Personales modificó en los siguientes términos el artículo segundo del resuelve de la Resolución N°. 31996 del 26 de mayo de 2021.

> ***"ARTÍCULO SEGUNDO: CONMINAR** a la sociedad CONDIVAL S.A.S. a que dentro del término de tres (3) días siguientes a la ejecutoria del presente acto administrativo, de estricto cumplimiento a la orden impartida por esta Superintendencia a través de la Resolución N°. 61479 del 07 de noviembre de 2019, so pena de que esta Superintendencia haga la respectiva aplicación del artículo 90 de la Ley 1437 de 2011".*

En conclusión, la sociedad recurrente deberá dar estricto cumplimiento a la orden impartida a través de la **Resolución N°. 61479 del 07 de noviembre de 2019** dentro del término de tres (3) días siguientes a la ejecutoria del acto administrativo recurrido.

5. POTESTAD SANCIONADORA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Según la Corte Constitucional, "*es innegable que a través del derecho administrativo sancionador se pretende garantizar la preservación y restauración del ordenamiento jurídico, mediante la imposición de una sanción que no sólo repruebe sino que también prevenga la realización de todas aquellas conductas contrarias al mismo. Se trata, en esencia, de un poder de sanción ejercido por las autoridades administrativas que opera ante el incumplimiento de los distintos mandatos que las normas jurídicas imponen a los administrados y aún a las mismas autoridades públicas*"[10].

Respecto de la "*potestad sancionatoria*", la Corte Constitucional ha señalado, entre otras, lo que sigue a continuación:

> *"El poder sancionador estatal ha sido definido como "un instrumento de autoprotección, en cuanto contribuye a preservar el orden jurídico institucional mediante la asignación de competencias a la administración que la habilitan para imponer a sus propios funcionarios y a los particulares el acatamiento, inclusive por medios punitivos, de una disciplina cuya observancia contribuye a la realización de sus cometidos.*
>
> *Esa potestad es una manifestación del ius punendi, razón por la que está sometida a los siguientes principios: (i) el principio de legalidad, que se traduce en la existencia de una ley que la regule; es decir, que corresponde sólo al legislador ordinario o extraordinario su definición. (ii) El principio de tipicidad que, si bien no es igual de riguroso al penal, sí obliga al legislador a hacer una descripción de la conducta o del comportamiento que da lugar a la aplicación de la sanción y a determinar expresamente la sanción. (iii) El debido proceso que exige entre otros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (iv) El principio de proporcionalidad que se traduce en que la sanción debe ser proporcional a la falta o infracción administrativa que se busca sancionar. (v) La independencia de la sanción penal; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal"[11]*.

En el mismo sentido, y en relación con los principios[12] señalados, dicha Corporación por medio de las Sentencias C-827 de 2001; C-401 de 2010 y C-948 de 2002 manifestó:

> *"En la doctrina[13] se postula, así mismo* [sic]*, sin discusión que la administración o las autoridades titulares* [sic] *de funciones administrativas lo sean de potestad sancionadora y que ésta en cuanto manifestación del ius puniendi del Estado está sometida a claros principios generalmente aceptados, y en la mayoría de los casos proclamados de manera explicita en los textos constitucionales. Así, a los principios de configuración del sistema sancionador*

---

[10] Cfr. Corte Constitucional, sentencia C-818 del 9 de agosto de 2005. MP. Dr. Rodrigo Escobar Gil. En: https://www.corteconstitucional.gov.co/relatoria/2005/C-818-05.htm

[11] Corte Constitucional. Sentencia C-748 de 2011.

[12] "Los principios señalados en el CPACA tienen un carácter normativo y vinculante, a diferencia de la naturaleza orientadora que se predicaba en el CCA. La aplicabilidad general de los principios previstos en el artículo 3o del CPACA, como desarrollo directo de la Constitución Política, conlleva a que dichos principios deban observarse para cualquier actuación administrativa, incluidas las reguladas en leyes especiales. Así las cosas, el intérprete deberá utilizarlos directamente o hacer un ejercicio de integración normativa entre los principios de la actuación administrativa previstos en la ley especial y los señalados en el CPACA". Juan Manuel Laverde Álvarez. Manual de Procedimiento Administrativo Sancionatorio. Ed. Legis S.A. Segunda Edición. Bogotá, Colombia. 2018.

[13] Juan Alfonso Santamaría Pastor. Principios de Derecho Administrativo. Volumen II. Ed. Centro de Estudios Ramón Areces. Madrid. Tomo II. Segunda Edición. 2000.

como los de legalidad (toda sanción debe tener fundamento en la ley), tipicidad (exigencia de descripción especifica y precisa por la norma creadora de las infracciones y de las sanciones, de las conductas que pueden ser sancionadas y del contenido material de las sanciones que puede imponerse por la comisión de cada conducta, así como la correlación entre unas y otras) y de prescripción (los particulares no pueden quedar sujetos de manera indefinida a la puesta en marcha de los instrumentos sancionatorios), se suman los propios de aplicación del sistema sancionador, como los de culpabilidad o responsabilidad según el caso – régimen disciplinario o régimen de sanciones administrativas no disciplinarias- (juicio personal de irreprochabilidad dirigido al autor de un delito o falta), de proporcionalidad o el denominado non bis in ídem".

Ahora, al hacer referencia al Principio de Legalidad en materia de protección del Derecho de Habeas Data, la Corte Constitucional mediante la Sentencia C-1011 de 2008, manifestó:

"(...) Para la Corte, en consecuencia, ***la flexibilidad que puede establecer el legislador en materia de derecho administrativo sancionador es compatible con la Constitución, siempre que esta característica no sea tan amplia que permita la arbitrariedad de la administración. Un cierto grado de movilidad a la administración para aplicar las hipótesis fácticas establecidas en la ley guarda coherencia con los fines constitucionales de esta actividad sancionatoria administrativa, en la medida que le permite cumplir eficaz y eficientemente con las obligaciones impuestas por la Carta. Sin embargo, ha advertido que la flexibilidad del principio de legalidad no puede tener un carácter extremo, al punto que se permita la arbitrariedad de la administración en la imposición de las sanciones o las penas****".* (Énfasis añadido).

Así las cosas, la administración no puede exceder los límites impuestos por el legislador al momento de aplicar una sanción. Por lo que, la conducta objeto de investigación debe tener el carácter de sancionable. Es aquí donde surge el principio de tipicidad, el cual no es otra cosa que el previo establecimiento por parte del legislador, de la forma más clara y precisa, "*de infracciones, penas, castigos o sanciones que pueden ser impuestas por las autoridades administrativas en ejercicio del poder punitivo estatal*"[14].

Como se observa, es suficiente desconocer cualquiera de las disposiciones de la Ley Estatutaria 1581 de 2012, para que la administración ejerza su poder sancionatorio. Claro está, en los casos en los que así lo determine la actuación administrativa correspondiente, como consecuencia directa de la trasgresión de las normas que amparan el Derecho Fundamental de *Habeas Data*.

En el presente caso, se dan los presupuestos requeridos para determinar que la conducta desplegada por la recurrente en reorganización vulneró las disposiciones legales mencionadas en la parte resolutiva de la resolución recurrida.

Respecto de la sanción se destaca lo siguiente:

I. La multa impuesta mediante la Resolución Nº 31996 de 2021 ($3.195.104) equivale al 0,18% del máximo legal permitido (2000 salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012.

II. El monto de dicha sanción es el resultado del análisis del daño y/o puesta en peligro de los intereses jurídicos tutelados en el trámite de la primera instancia de esta actuación administrativa. Así como del incumplimiento de los deberes impuestos por la citada Ley Estatutaria.

III. La Resolución recurrida fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Asimismo, también fue el resultado de la valoración fáctica y probatoria de la primera instancia que llevó a concluir y comprobar la vulneración al derecho de *habeas data* del Titular y en particular los mandatos legales señalados.

IV. Las sanciones que se imponen dentro de esta clase de procesos, no derivan de los daños o perjuicios causados a los Titulares por incumplir la regulación sobre tratamiento de datos personales. Es decir, las normas que protegen el derecho de *habeas data o protección de*

[14] Corte Constitucional. Sentencias C-1161 de 2000.

datos personales no se refieren a la responsabilidad civil de los Responsables del Tratamiento de Datos.

V. La vulneración del derecho de *habeas data o la protección de datos personales* no solo afecta al Titular, también pone en riesgo los derechos de toda la sociedad. Por esto, las sanciones no pueden ni deben tratarse como una cuestión insignificante o de poca cuantía, ni mucho menos como si las incidencias del proceso lo convirtieran en uno de indemnización de daños y perjuicios. Esto, en razón a que existe de por medio una trasgresión flagrante a los derechos humanos de un ciudadano, lo cual es suficiente para entender la gravedad de la conducta, sin necesidad de acudir a forzosos razonamientos o teorías complicadas, a fin de desentender o negar una verdad inconcusa, cual es la del quebrantamiento de derechos constitucionales.

Recuérdese que, según la Declaración Universal de los Derechos Humanos, *"el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad"*[15]. Por eso, según dicho documento, se considera *"esencial que los derechos humanos sean protegidos por un régimen de Derecho"*. No debe olvidarse que el respeto de los Derechos Humanos es un elemento esencial de la democracia[16]. Así las cosas, recalcamos, la violación de Derechos Humanos es una conducta gravísima que no solo atenta contra los intereses de un individuo en particular sino de la sociedad en general.

Con apoyo en estos argumentos, no se acogerán las consideraciones de la recurrente en la medida en que la sanción impuesta se ajusta a derecho y obedece a las particularidades propias de esta actuación administrativa.

6. RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY) Y "COMPLIANCE" EN EL TRATAMIENTO DE DATOS PERSONALES.

Nuestra la regulación no solo ordena a quien trate Datos personales a implementar las *"medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*" [17] y a "*conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*[18]. Sino que les exige "*(...) 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"*[19].

Nótese que la norma impone una carga probatoria en cabeza de los Responsables de probar que adoptado las medidas citadas para cumplir los ordenado por dicha ley. En este caso, como se mencionó, el principio y el deber de seguridad tiene un criterio eminentemente preventivo, lo cual obliga a las organizaciones a poner en marcha medidas técnicas, humanas, administrativas y de cualquier otra índole para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a los datos personales[20]. Pero, adicionalmente, es imprescindible que se esté efectuando un monitoreo o seguimiento permanente para asegurar que dichas medidas se aplican en la práctica y son útiles.

La Corte Constitucional mediante la sentencia C-32 de 2021 reconoció la existencia de la responsabilidad demostrada en los siguientes términos:

> "*219. El principio de responsabilidad demostrada, conocido en el derecho comparado como accountability en la protección de datos personales, es incorporado por la legislación interna por el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2013 (sic). El artículo 26 de esa normativa determina que los responsables del tratamiento de datos personales deberán demostrar, a petición de la Superintendencia de Industria y Comercio, entidad que obra como autoridad colombiana de protección de datos, que han*

[15] Organización de las Naciones Unidas (1948). Declaración Universal de los Derechos Humanos.
[16] Artículo 3 de la Carta Democrática Interamericana la cual se puede consultar en: http://www.oas.org/OASpage/esp/Documentos/Carta_Democratica.htm
[17] Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012
[18] Cfr. Literal d) del artículo 17 de la Ley Estatutaria 1581 de 2012
[19] Cfr. Artículo 26 del decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015)
[20] Cfr. Literal g) del artículo 4 de la Ley 1581 de 2012

implementado medidas apropiadas y efectivas para cumplir con las citadas normas jurídicas. Esto de manera proporcional a: (i) la naturaleza jurídica del responsable y, cuando sea el caso, su tamaño empresarial; (ii) la naturaleza de los datos personales objeto de tratamiento; (iii) el tipo de tratamiento; y (iv) los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares del dato personal. Con este fin, los responsables deben informar a la SIC acerca de los procedimientos usados para el tratamiento de datos. A esta medida se suma lo previsto en el artículo 27 ejusdem, que estipula la obligación del responsable de establecer políticas internas que garanticen: (i) la existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable; (ii) la adopción de mecanismos internos para poner en práctica dichas políticas; y (iii) la previsión de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, respecto de cualquier aspecto del tratamiento de datos personales.

El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de demostrar ante la autoridad de datos *que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal*."[21] (Destacamos).

La regulación colombiana le impone al Responsable del tratamiento la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante*"[22].

Adicionalmente, los Responsables o Encargados del tratamiento no son dueños de los datos personales que reposan en sus bases de datos o archivos. En efecto, ellos son meros tenedores que están en el deber de administrar de manera correcta, apropiada y acertada la información de las personas porque su negligencia o dolo en esta materia afecta los derechos humanos de los titulares de los datos.

En virtud de lo anterior, el capítulo III del Decreto 1377 del 27 de junio de 2013 -incorporado en el decreto 1074 de 2015- reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada.

El artículo 26[23] -*titulado DEMOSTRACIÓN*- establece 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". Así resulta imposible ignorar la forma en que el responsable o encargado del tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengas como propósito lograr que los postulados legales sean realidades verificables.

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la "*Guía para implementación del principio de responsabilidad demostrada (accountability)*"[24]. El término "accountability" a pesar de los diferentes significados ha sido entendido en el campo de la protección de datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

---

[21] Cfr. Corte Constitucional, sentencia C-032 del 18 de febrero de 2021. M.P. Dra Gloria Stella Ortiz. El texto de la sentencia puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/2021/C-032-21.htm

[22] Cfr. Corte Constitucional, sentencia T-227 de 2003

[23] El texto completo del artículo 26 del decreto 1377 de 2013 ordena lo siguiente: Artículo 26. Demostración. 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, en una manera que sea proporcional a lo siguiente:
1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.
En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas"

[24] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Conforme con ese análisis, las recomendaciones que trae la guía a los obligados a cumplir la ley 1581 de 2012:

1. Diseñar y activar un programa integral de gestión de datos (en adelante PIGDP). Esto, exige compromisos y acciones concretas de los directivos de la organización. Igualmente requiere la implementación de controles de diversa naturaleza.
2. Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP, y
3. Demostrar el debido cumplimiento de la regulación sobre tratamiento de datos personales.

El principio de responsabilidad demostrada –*accountability*- demanda implementar acciones de diversa naturaleza[25] para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los Responsables del tratamiento implementen medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

Dichas medidas deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

El principio de responsabilidad precisa menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido tratamiento de los datos personales. El éxito de este dependerá del compromiso real de todos los miembros de una organización. Especialmente, de los directivos de las organizaciones, pues, sin su apoyo sincero y decidido, cualquier esfuerzo será insuficiente para diseñar, llevar a cabo, revisar, actualizar y/o evaluar los programas de gestión de datos.

Adicionalmente, el reto de las organizaciones frente al principio de responsabilidad demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones.

El principio de responsabilidad demostrada busca que los mandatos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las organizaciones sean proactivos respecto del tratamiento de la información de manera que por iniciativa propia adopten medidas estratégicas capaces de garantizar los derechos de los titulares de los datos personales y su gestión siempre sea respetuosa de los derechos humanos.

Aunque no es espacio para explicar cada uno de los anteriores aspectos mencionados en la guía, ponemos de presente que el principio de responsabilidad demostrada se articula con el concepto de "compliance" en la medida que éste hace referencia al *"conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos"*[26].

También se ha afirmado que *"compliance es un término que hace referencia a la gestión de las organizaciones conforme a las obligaciones que le vienen impuestas (requisitos regulatorios) o que se ha autoimpuesto (éticas)"*[27]. Adicionalmente, se precisa que "ya no vale solo intentar cumplir" la ley sino que las organizaciones "deben asegurarse que se cumple y deben generar evidencias de sus esfuerzos por cumplir y hacer cumplir a sus miembros, bajo la amenaza de sanciones si no son capaces de ello. Esta exigencia de sistemas más eficaces impone la creación de funciones específicas y metodologías de compliance"[28].

Por tanto, las organizaciones deben "implementar el *compliance*" en su estructura empresarial con miras a acatar las normas que inciden en su actividad y demostrar su compromiso con la legalidad. Lo mismo sucede con "accountability" respecto del tratamiento de datos personales.

---

[25] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humanas y de gestión que involucran procesos y procedimientos.
[26] Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com/ (última consulta: 6 de noviembre de 2018)
[27] Cfr. Bonatti, Francisco. Va siendo hora que se hable correctamente de compliance (III). Entrevista del 5 de noviembre de 2018 publicada en Canal Compliance: http://www.canal-compliance.com/2018/11/05/va-siendo-hora-que-se-hable-correctamente-de-compliance-iii/
[28] Idem

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del compliance y buena parte de lo que implica el principio de responsabilidad demostrada (accountability). En la mencionada guía se considera fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un "*sistema de administración de riesgos asociados al tratamiento de datos personales"*[29] que les permita *"identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales"*[30].

CONCLUSIONES

Sin perjuicio de lo establecido, no se accederá las pretensiones de la recurrente por, entre otras, las siguientes razones:

- Sin seguridad no existe debido tratamiento de datos personales. El principio y el deber de seguridad tiene un criterio eminentemente preventivo, lo cual obliga a los Responsables a adoptar medidas apropiadas y efectivas para evitar afectaciones a la seguridad de la información sobre las personas.

- Las órdenes no son sanciones sino son medidas necesarias para, entre otras, hacer efectivo el derecho de hábeas data o para que los Responsables del Tratamiento y Encargados del Tratamiento cumplan correctamente los previsto en regulación con miras a garantizar el debido tratamiento de los datos personales y el respeto de los derechos de los Titulares de los datos.

- La multa impuesta mediante la Resolución Nº 31996 de 2021 ($3.195.104) equivale al 0,18% del máximo legal permitido (2.000 salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012.

- La recurrente realiza tratamiento de datos de naturaleza sensible (datos relativos a la salud), lo cual exige mayores medidas de seguridad, mucha diligencia y profesionalismo en el tratamiento de esta información.

De esta forma y de acuerdo con lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirma la Resolución N°. 31996 del 26 de mayo de 2021.

En mérito de lo expuesto, este Despacho

RESUELVE

ARTÍCULO PRIMERO. CONFIRMAR la Resolución N°. 31996 del 26 de mayo de 2021, de conformidad con lo expuesto en la parte motiva del presente acto administrativo y en especial lo decidido en la Resolución N°. 69805 del 28 de octubre de 2021.

ARTÍCULO SEGUNDO. NOTIFICAR personalmente el contenido de la presente resolución a la sociedad CONDIVAL S.A.S., identificada con NIT 800.187.774-7 a través de su representante legal o su apoderado o quien haga sus veces, entregándole copia de esta e informándole que contra el presente acto administrativo no procede recurso alguno.

[29] Cfr. Superintendencia de Industria y Comercio (2015) "*Guía para implementación del principio de responsabilidad demostrada (accountability)*". Págs 16-18
[30] Ibid. P 16

ARTÍCULO TERCERO. INFORMAR el contenido de este acto administrativo al Director de Investigación de Protección de Datos Personales y devolverle el expediente para su custodia final.

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá D.C., marzo 24 de 2022

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES

NELSON REMOLINA ANGARITA

Firmado digitalmente por NELSON REMOLINA ANGARITA
Fecha: 2022.03.24 12:39:46 -05'00'

NELSON REMOLINA ANGARITA

ALC

Notificación

Sociedad: CONDIVAL S.A.S.
Identificación: Nit. 800.187.774-7
Representante Legal: FELIPE ANDRÉS VALENCIA SAVEDRA
Identificación: C.C. No. 80.407.929
Correo electrónico: fvalencia@condivalsas.com
Dirección: Calle 98 N° 22-64 Of 201
Ciudad: Bogotá D.C.
País: República de Colombia