



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

RESOLUCIÓN NÚMERO 34913 DE 2020

(03 de Julio)

VERSIÓN PÚBLICA

Radicación 18– 128271

El Superintendente Delegado para la Protección de Datos Personales

En ejercicio de sus facultades legales, en especial las conferidas por los artículos 19 y 21 de la Ley 1581 de 2012, numeral 7 del artículo 16 del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO. Que en virtud de la denuncia¹ presentada el 24 de abril de 2018 por la señora [REDACTED] ante esta Superintendencia, se tuvo conocimiento de la presunta violación de las normas de protección de datos personales contenidas en la Ley 1581 de 2012, por parte de la sociedad **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.** identificada con el Nit. 830.122.566-1, por lo que la Dirección de Investigación de Protección de Datos Personales mediante Resolución N° 87593 del 30 de noviembre de 2018² decidió iniciar una investigación administrativa por la presunta vulneración a las disposiciones contenidas en el literal a) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal e) del artículo 8 de la norma en mención y el artículo 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015.

SEGUNDO. Que una vez agotada la etapa probatoria, y efectuado el análisis de los elementos probatorios que reposan en el expediente, así como del escrito de descargos³ allegado por **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.** la Dirección de Investigación de Protección de Datos Personales mediante la Resolución No. 19012 de 31 de mayo de 2019⁴, resolvió:

“ARTÍCULO PRIMERO: *IMPONER una sanción pecuniaria a la sociedad COLOMBIA TELECOMUNICACIONES S.A. E.S.P. identificada con el Nit. 830.122.566-1, de VEINTICUATRO MILLONES OCHOCIENTOS CUARENTA Y TRES MIL CUATROCIENTOS OCHENTA PESOS M/CTE (\$24.843.480)”, equivalentes a TREINTA (30) salarios mínimos legales mensuales vigentes, por la violación a lo dispuesto en el literal a) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal e) del artículo 8 de la norma en mención y el artículo 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015.*”

De igual forma,

“ARTÍCULO SEGUNDO: *ORDENAR a la sociedad COLOMBIA TELECOMUNICACIONES S.A. E.S.P., identificada con Nit. 830.122.566-1,*

¹ Expediente. Folios 1 a 8.

² Expediente. Folios 19 a 22.

³ Expediente. Folios 7 a 8.

⁴ Expediente. 39 a 45.

Por la cual se resuelve un recurso de apelación

deberá adecuar la política interna señalada en el párrafo anterior (Ver numeral 10 considerativo de la Resolución 19012 del 31 de mayo de 2019) con el fin de que la misma establezca términos de supresión y/o actualización de los datos de acuerdo al artículo 15 de la Ley 1581 de 2012”.

TERCERO. Que en el término legal establecido, mediante escrito 18-128271- -00024-0001 de 4 de julio de 2019, la apoderada de **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.** (en adelante la recurrente), interpuso recurso de reposición y en subsidio de apelación, contra la Resolución N° 19012 de 31 de mayo de 2019, con fundamento en los siguientes argumentos:

1. INEXISTENCIA DE UNA TRASGRESIÓN DE LAS NORMAS SOBRE PROTECCIÓN DE DATOS PERSONALES CONSAGRADAS EN EL LITERAL A) DEL ARTÍCULO 17 Y LITERAL E) DEL ARTÍCULO 8 DE LA LEY 1581 DE 2012, EN CONCORDANCIA CON EL ARTÍCULO 2.2.2.25.2.6 DEL DECRETO ÚNICO REGLAMENTARIO 1074 DE 2015:

La recurrente niega haber cometido conductas contrarias a la ley o a la Constitución Política. Asimismo aduce no haber generado ninguna clase de lesión al pleno y efectivo derecho de *habeas data* del titular de la información. Además afirma que por la señora [REDACTED] fue excluida de las bases de datos comerciales de Colombia Telecomunicaciones S.A. E.S.P., el 17 de abril de 2018, como consecuencia de la solicitud expresa por parte de la Titular. Con esto se evidenciaría la garantía del usuario a exigir la supresión de sus datos.

Así las cosas la recurrente advierte que no hay claridad en la relación de causalidad entre los hechos y las normas en las que se fundamenta la sanción. Pues, en todo caso hubo un uso responsable de la información y datos del Titular. A su parecer, el libre y pleno ejercicio del derecho de *habeas data* se concreta de la siguiente manera:

- a. Es el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre el Titular de la información en bancos de datos y en archivos de entidades públicas y privadas.
- b. Resulta vulnerado cuando la información tratada es recogida de forma ilegal, es errónea, o versa sobre aspectos reservados o íntimos del Titular de la información.

Por tanto, según la recurrente, para que exista una vulneración del derecho al *habeas data*, la información debió haber sido recogida de manera ilegal, sin el consentimiento del Titular del dato, ser errónea o recaer sobre aspectos íntimos de la vida del Titular no susceptibles de ser conocidos públicamente.

2. LA ORDEN ADMINISTRATIVA RESULTA INNECESARIA. COLOMBIA TELECOMUNICACIONES S.A. ESP CUMPLE LOS PARÁMETROS NORMATIVOS DEL ARTÍCULO 15 DE LA LEY 1581 DE 2012.

Afirma la recurrente que la acreditación del cumplimiento de la orden bien puede ser proferida por el Representante Legal de Colombia Telecomunicaciones S.A. ESP o en su defecto por el Oficial de Protección de Datos Personales, en tanto que se trata de una política interna de la Compañía, la cual es autónoma, por lo que no se encuentra necesario que terceros entre a pronunciarse sobre aspectos que son de ámbito privado y que regulan aspectos intrínsecos de la Compañía, la cual está en la capacidad de expedir de manera legal e imparcial la certificación de cumplimiento y así acreditarlo ante la SIC de ser el caso.

Por la cual se resuelve un recurso de apelación

3. VALORACIÓN PROBATORIA. PRINCIPIO DE PROPORCIONALIDAD. PROPORCIONALIDAD DE LA SANCIÓN

Frente a este punto, la recurrente considera que los hechos que sirvieron como fundamento para sancionar no fueron valorados de manera razonable a la luz de los criterios establecidos en el artículo 24 de la Ley 1581 de 2012, el cual establece unos parámetros para que la administración los valore a la hora de graduar e imponer la sanción correspondiente.

Igualmente afirma que el Estado en ejercicio de su potestad sancionatoria, debe incluir en la valoración de cada caso algunos elementos necesarios para consolidar el principio de razonabilidad:

- La determinación de la sanción debe considerar criterios como la existencia o no de la intencionalidad.
- El perjuicio causado.
- Las circunstancias de la comisión de la infracción.

De igual manera, debe darse aplicación a los criterios taxativos que determina el artículo 24 de la Ley 1581 de 2012. Por consiguiente, se trata de un deber en cabeza de la Superintendencia de Industria y Comercio analizar y sustentar a la luz de la norma citada, cada uno de los criterios, para que con base en ellos profiera una decisión lógica, de acuerdo con los hechos concretos del caso.

La recurrente manifiesta que el acto administrativo recurrido carece de motivación suficiente, en razón a que solo se limitó a señalar que los literales b); d); e) y f) del artículo 24 en mención no serían tenidos en cuenta debido a que dentro del trámite adelantado no se evidenció la obtención de un beneficio económico por parte de la investigada; no hubo reincidencia en la comisión de la infracción; no se presentó resistencia u obstrucción a la acción investigativa por parte de esta autoridad; y tampoco hubo resistencia o desacato a las instrucciones impartidas.

En este punto, el principal motivo de inconformidad de la recurrente es que, en su parecer, la sanción no se graduó conforme con las circunstancias de modo que demostrarían que Colombia Telecomunicaciones no incurrió en ninguna de las conductas infractoras que refirió la Dirección de Investigación de Protección de Datos Personales. Adicionalmente, alega que no se explica cuáles fueron los criterios que se utilizaron para imponer una multa de treinta (30) salarios mínimos legales mensuales vigentes, máxime cuando en su concepto, no se realizaron valoraciones que sustentaran y motivaran la decisión.

“En cuanto al perjuicio, dentro del presente caso, no se evidencia de manera clara el el daño causado al usuario puesto que tales afirmaciones no han pasado de ser aseveraciones no demostradas ni por el usuario ni por la SIC, puesto que no se logró establecer materialmente el daño y su valor.

A efectos de valorar el caso, la SIC tenía el deber de examinar los elementos del daño y verificar su ocurrencia en el presente asunto.

(...)

Para que el perjuicio pueda ser predicado dentro del presente asunto, y la sanción tenga pleno sustento en los hechos acaecidos, es necesario que dentro de la actuación administrativa se hubiera probado plenamente el menoscabo sufrido por el usuario y en esa medida graduar la sanción, sin embargo dicha sanción impuesta no

Por la cual se resuelve un recurso de apelación

se encuentra enmarcada dentro del elemento fáctico y menos aún dentro del elemento jurídico puesto que la [sic] SIC [sic] la decisión de la SIC es claramente desproporcionada y no guarda equilibrio alguno con las circunstancias de modo que se presentaron dentro de este caso.

Si en gracia de discusión se admitiera que dentro de este asunto, se causó perjuicio alguno, era deber del usuario demostrar el perjuicio generado y en segundo lugar, era deber de la SIC analizar el caso conforme a [sic] las circunstancias acaecidas y de esta manera calificar el perjuicio conforme a [sic] las reglas establecidas en las normas ya señaladas líneas atrás para así tasar la sanción de manera equilibrada con los elementos del caso. No obstante, se evidencia que la SIC desconoció por completo los parámetros normativos establecidos para la graduación de la sanción, y adoptó una decisión claramente desproporcionada y alejada de derecho”.

La recurrente continúa el recurso aduciendo que la multa impuesta por esta autoridad es claramente desproporcionada y arbitraria. Asimismo afirma que resulta lesiva y excesiva, si se compara con la conducta desplegada.

Por último, solicita la revocatoria de la Resolución No. 19012 de 31 de mayo de 2019 y subsidiariamente reconsiderar el valor de la sanción.

CUARTO. Que mediante la Resolución No. 59232 de 31 de octubre de 2019, la Dirección de Investigación de Protección de Datos Personales resolvió el recurso de reposición interpuesto por la recurrente, confirmando en todas sus partes la Resolución No. 19012 de 31 de mayo de 2019.

QUINTO. Que mediante el artículo primero de la Resolución No. 12169 del 31 de marzo de 2020 de esta entidad se ordenó lo siguiente: *“SUSPENDER los términos de las actuaciones administrativas sancionatorias y disciplinarias en curso, que se surten ante las dependencias de esta Superintendencia, desde el 1º de abril del 2020 y hasta la vigencia del Estado de Emergencia Económica, Social y Ecológica decretada por el Presidente de la República, fechas en que no correrán los términos legales, incluidos los de caducidad de la facultad sancionatoria de la administración prevista de manera general en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y en las normas especiales aplicables a las actuaciones de la Superintendencia de Industria y Comercio.”*

Que mediante el artículo 1 de la Resolución 28182 del 12 de junio de 2020 de la Superintendencia de Industria y Comercio se ordenó *“REANUDAR a partir del 16 de junio de 2020, los términos de las actuaciones administrativas sancionatorias y disciplinarias que se surten ante las dependencias de esta Superintendencia (...)”*

SEXTO. Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, y con base en lo expuesto por la recurrente en el escrito de reposición y en subsidio apelación contra la Resolución No. 19012 de 31 de mayo de 2019, se procede 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.

Por la cual se resuelve un recurso de apelación

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011⁵ establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destacan las siguientes:

(...)

7. 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. DERECHO DE LOS TITULARES A SOLICITAR LA SUPRESIÓN DE SUS DATOS. DEBER DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES DE TRAMITAR LOS RECLAMOS Y CONSULTAS ELEVADAS POR LOS TITULARES DE LA INFORMACIÓN EN EL TÉRMINO LEGAL.

La Corte Constitucional ha establecido que “*el derecho al habeas data otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos “el acceso, inclusión, **exclusión**, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales. (...)*”⁶. (Énfasis añadido).

En el escrito del recurso, la recurrente manifiesta que la multa impuesta por esta autoridad es claramente desproporcionada y arbitraria. Asimismo afirma que resulta lesiva y excesiva, si se compara con la conducta que realizó.

Es imperativo *-no facultativo-* que los Responsables o Encargados del Tratamiento de datos personales garanticen oportuna y debidamente los derechos constitucionales y legales de las personas. Se trata de un asunto muy importante sobre el cual las organizaciones deben obrar de manera profesional, diligente y efectiva porque ello es parte central del mandato constitucional previsto en el artículo 15 cuyo texto señala lo siguiente:

“En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución”.

Dado lo anterior, este Despacho ha sido enfático en señalar que:

*“No puede convertirse en práctica empresarial que el titular del dato tenga que insistir varias veces para que se garantice el respecto de sus derechos. Con una sola solicitud es suficiente y le corresponde al Responsable hacer efectivo el derecho de las personas dentro de los plazos máximos legales establecidos en la ley. Los derechos de los titulares son para respetarlos en el tratamiento de datos personales y no para dilatar su cumplimiento o negar su efectividad en la práctica.”*⁷

⁵ 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.

⁶ Sentencia C-748 de 2011. Control constitucional al Proyecto de Ley Estatutaria No. 184 de 2010 en Senado; 046 de 2010 en Cámara de Representante, “por la cual se dictan disposiciones generales para la protección de datos personales” (Ley 1581 de 2012).

⁷ Cfr. Resolución 83882 del 15 de noviembre de 2018 de la Superintendencia de Industria y Comercio.

Por la cual se resuelve un recurso de apelación

Frente al argumento de la recurrente es necesario precisar que la autorización es un mecanismo de legitimación del Tratamiento de datos personales, pero no es un título traslativo de la propiedad del dato. El Responsable y/o el Encargado no son propietarios de los datos, sino meros tenedores o administradores de esa información. Ellos, no pueden efectuar el tratamiento de los datos personales de cualquier manera sino solo como lo indica la Constitución y la ley.

La autorización no le permite a Responsables o Encargados obrar de cualquier manera cuando tratan datos personales porque ello atenta contra mandatos constitucionales y legales. Por eso, los Responsables y Encargados, deben, entre otras cosas, garantizar los derechos de los Titulares de los datos para que se pueda predicar que estamos frente a un tratamiento lícito de la información mencionada. En este sentido, la Corte Constitucional, ha señalado lo siguiente:

*“En efecto, el artículo 15 de la Constitución Política señala que “En la recolección, tratamiento y circulación de datos se respetaran la libertad y demás garantías consagradas en la Constitución.” El hábeas [sic] data confiere en palabras de la Corporación “según la norma constitucional citada, un grupo de facultades al individuo para que, en ejercicio de la cláusula general de libertad, pueda controlar la información que de sí mismo ha sido recopilada por una central de información”. **Este control, no sólo se predica de la autorización previa para el Tratamiento del dato, sino que el individuo también es libre de decidir cuales informaciones desea que continúen y cuáles deben sean excluidas de una fuente de información, siempre y cuando no exista un mandato legal que le imponga tal deber, o cuando exista alguna obligación contractual entre la persona y el controlador de datos, que haga necesaria la permanencia del dato.***

Considerar lo contrario significaría que los administradores de la información, pudieran disponer libremente y sin término definido, de los datos personales del sujeto concernido y, en consecuencia, aquel quedaría privado materialmente de la posibilidad de ejercer las garantías previstas a su favor por el Texto Constitucional.

(...)⁸. (Énfasis añadido)

Como es sabido, la supresión de la información es un derecho del titular del dato, previsto en la Ley 1581 de 2012 en los siguientes términos:

*“**Artículo 8°. Derechos de los Titulares.** El Titular de los datos personales tendrá los siguientes derechos:*

(...)

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

(...)⁹.

La Corte Constitucional mediante Sentencia C-748 de 2011 se refirió al precitado artículo de la siguiente manera:

⁸ Sentencia C-748 de 2011. Control constitucional al Proyecto de Ley Estatutaria No. 184 de 2010 en Senado; 046 de 2010 en Cámara de Representante, “por la cual se dictan disposiciones generales para la protección de datos personales” (Ley 1581 de 2012).

⁹ Cfr. Literal e) del artículo 8 de la Ley 1581 de 2012.

Por la cual se resuelve un recurso de apelación

“

(...) el literal e) debe ser entendido en el sentido que el Titular podrá revocar la autorización y solicitar la supresión del dato cuando: (i) no se respeten los principios, derechos y garantías constitucionales y legales. En este caso, y en aras de garantizar el debido proceso, siempre y cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias al ordenamiento y (ii) en virtud de la solicitud libre y voluntaria del Titular del dato, cuando no exista una obligación legal o contractual que imponga al Titular el deber de permanecer en la referida base de datos”

En línea con lo anterior, ordena lo siguiente el artículo 9 del Decreto 1377 de 2013 (incorporado en el decreto 1074 de 2015) y titulado “**REVOCATORIA DE LA AUTORIZACIÓN Y/O SUPRESIÓN DEL DATO**”.

“Los Titulares podrán en todo momento solicitar al responsable o encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo, de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

El responsable y el encargado deben poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada.

Si vencido el término legal respectivo, el responsable y/o el encargado, según fuera el caso, no hubieran eliminado los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012”.

Así las cosas, es evidente que en virtud del ejercicio del derecho fundamental de *habeas data* a que se refiere el literal a) del artículo 17 de la Ley 1581 de 2012¹⁰ los Titulares pueden solicitar la exclusión o supresión de la información que repose en las bases de datos de los Responsables o Encargados del Tratamiento, siempre que no exista un deber legal o contractual que lo impida.

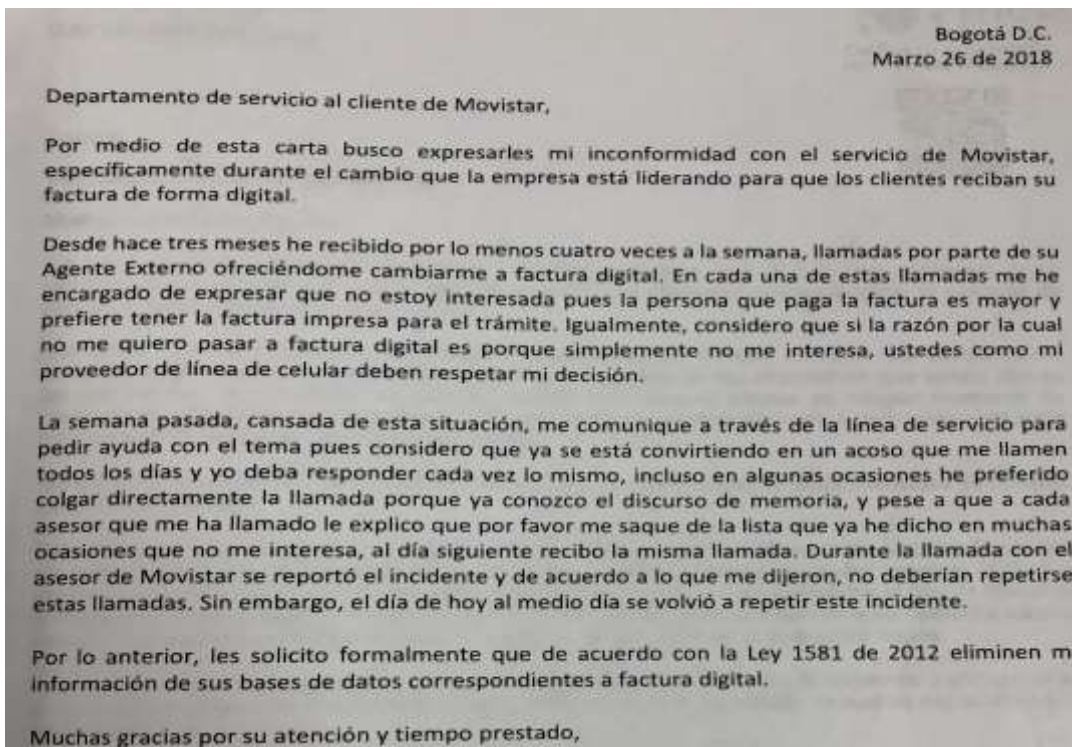
Del material probatorio del expediente se concluye lo siguiente:

- I. El **veintiséis (26) de marzo de 2018** la Titular de la información solicita a COLOMBIA TELECOMUNICACIONES S.A. E.S.P. la supresión de su información mediante comunicado remitido a la Responsable tal y como consta en el folio 4:

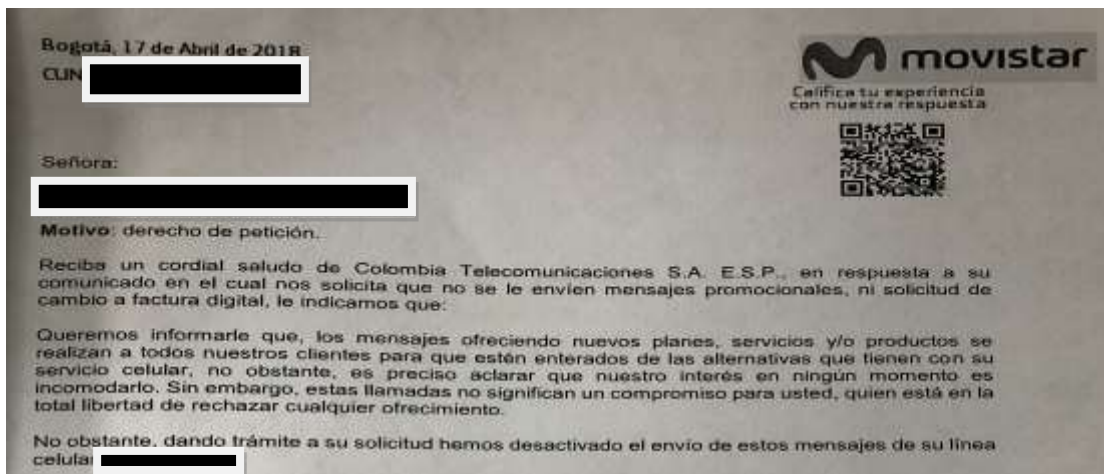
¹⁰ El texto del literal a) del artículo 17 de la ley 1581 de 2012 dice: “Artículo 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de *habeas* [sic] *data*;

Por la cual se resuelve un recurso de apelación



- II. Posteriormente, el **diez y siete (17) de abril** de 2018 COLOMBIA TELECOMUNICACIONES S.A. E.S.P. le respondió a la Titular que, "(...) dando trámite a su solicitud hemos desactivado el envío de estos mensajes de su línea celular [REDACTED]". Como consta en el folio 5:

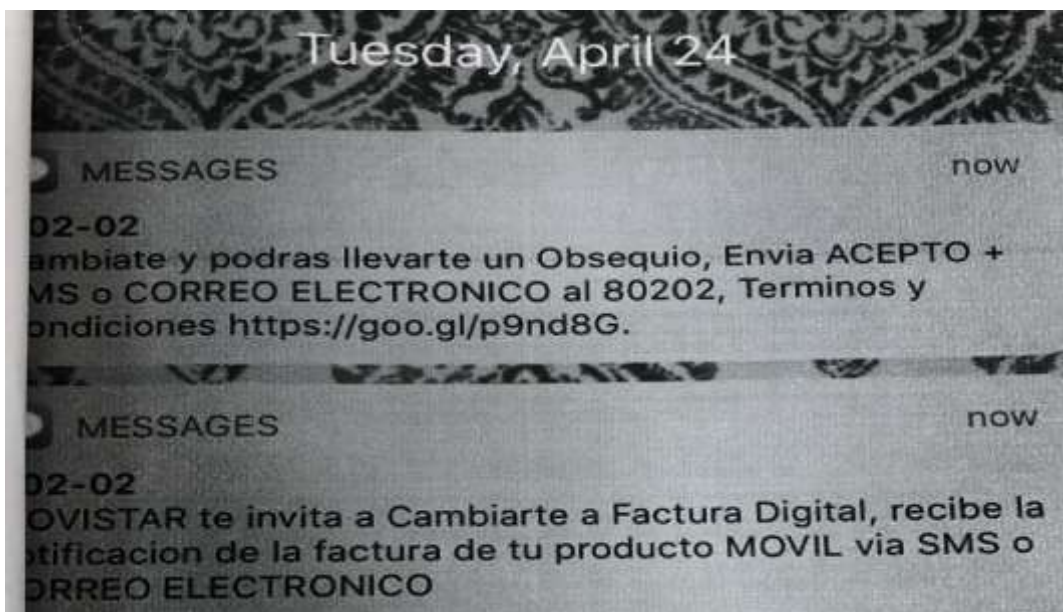


Nótese que la Titular del Dato solicita que se elimine sus datos de una base de datos y la recurrente responde que "*dando trámite a su solicitud hemos desactivado el envío de estos mensajes a su línea celular*". Como se observa, una cosa solicita el Titular y otra diferente responde la recurrente. Desactivar no es igual a eliminar.

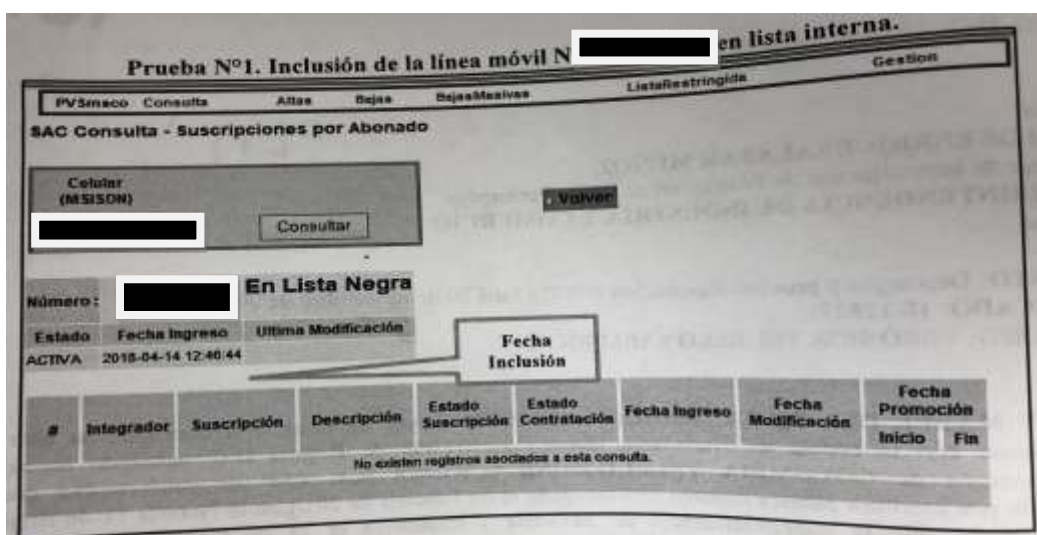
Ahora, con respecto a la supresión del dato se identifica el siguiente material probatorio.

- I. En primer lugar, la Titular [REDACTED] recibió el **veinticuatro (24) de abril de 2018** un mensaje por parte de COLOMBIA TELECOMUNICACIONES S.A. E.S.P. invitándola a cambiarse a la factura digital. Como se observa en el folio 6:

Por la cual se resuelve un recurso de apelación



- II. COLOMBIA TELECOMUNICACIONES S.A. E.S.P. allega prueba de que se incluyó el número [REDACTED] en lista negra el **14 de abril de 2018**, como puede observarse (folio 7 reverso):



- III. COLOMBIA TELECOMUNICACIONES S.A. E.S.P. reconoce que por política interna la actualización solicitada por la Titular quedó consolidada en el sistema a partir del **treinta (30) de abril de 2018** (folio 7 reverso):

Como se desprende de la imagen anterior, el registro se hizo el 14 de abril de 2018. Sin embargo, debido a que los cambios o actualizaciones en los bases de datos se realizan a corte de cada mes, por política interna, la actualización solicitada por la usuaria quedó consolidada en el sistema a partir del 30 de abril de 2018.

En suma, la señora [REDACTED] solicitó el **veintiséis (26) de marzo de 2018** la supresión de su información, pero solo fue suprimida el **treinta (30) de abril de 2018**, cuando el plazo máximo para ello era el 18 de abril de ese año porque según el artículo 15 de la Ley 1581 de 2012, la recurrente tenía un plazo "*quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo*". Por lo tanto, es claro que incumplió la ley porque no atendió oportunamente la solicitud de supresión de la información.

Por la cual se resuelve un recurso de apelación

Solicitud de supresión	Fecha máxima para atender la solicitud	Supresión de la información por parte de la recurrente
26 de marzo de 2018	18 de abril de 2018	30 de abril de 2018

Así las cosas, es claro que la recurrente no atendió de manera oportuna la solicitud de eliminación de los datos personales de la Titular del Dato. Pues, contrario a las afirmaciones realizadas por COLOMBIA TELECOMUNICACIONES S.A. E.S.P. cuando indica que "(...) Si bien es cierto, la supresión de los datos se hizo el día 30 de abril de 2018, es más cierto aún que ello no implica una lesión o estorbo al ejercicio del derecho en mención, pues no se evidencia de que manera ello generó una lesión para la usuaria (...)" el no atender a tiempo una solicitud no solo viola el derecho de habeas data sino también el derecho de petición de la Titular. Los derechos de las personas deben garantizarse de manera oportuna y correcta. La ley exige a los Responsables del Tratamiento responder dentro de un plazo concreto y no los faculta para hacerlo cuando quieran.

En consecuencia, no serán acogidos los argumentos de la recurrente, por cuanto no se demostró que la investigada hubiese atendido la solicitud de supresión de los datos del Titular de manera oportuna y en cumplimiento de los tiempos legales establecidos para ser atendidos.

3. DE LA BASE DE DATOS "LISTA NEGRA" DE COLOMBIA TELECOMUNICACIONES S.A. E.S.P.

Nótese que el escrito de descargos (folio 7) allegado por la recurrente, se menciona la inclusión del número móvil en "lista interna" que también se rotula como "**lista negra**". Por tanto, esta Delegatura se permite realizar las siguientes observaciones.

La expresión "lista negra"¹¹ utilizada por la recurrente en su base de datos, se ha vinculado a la recopilación de datos exclusivamente desfavorable sobre las personas. De entrada, se asocian esas listas para usos meramente negativos, discriminatorios o ilegales. En este sentido, la Corte Constitucional señaló, entre otras, lo siguiente en la Sentencia T-987 de 2012:

"Como se explicó en precedencia, la jurisprudencia constitucional ha fijado una prohibición general para la conformación de listas de información personal con consecuencias exclusivamente desfavorables para el titular del dato, en tanto esa práctica configura un ejercicio abusivo y desproporcionado de la facultad legal de administración de datos personales". Y, en ese caso, la Corte concluyó que ese tipo de listas: "(ii) es abiertamente contraria al derecho al hábeas data, en la medida en que fueron omitidos los deberes que se derivan de los principios de libertad, incorporación y finalidad, así como se desconoció la prohibición de confección de registros de datos personales destinados exclusivamente a imponer consecuencias desfavorables al titular del dato".

¹¹ Esta Delegatura se suma a lo expresado en la nota de pie de página número 35 de la Sentencia T-978 de 2012 respecto de la expresión "listas negras": Podría considerarse válidamente que esta expresión pudiese ser vinculada con algún factor de índole racial, lo que de suyo generaría una evidente discriminación, en tanto referiría el concepto "negro" con información desfavorable. No obstante, lo anterior, también debe resaltarse que la doctrina comparada ha utilizado uniformemente el concepto de "listas negras" o su par en idioma inglés blacklisting, para denominar la recopilación de información sobre datos exclusivamente desfavorables para el titular. Ante esta denominación y los problemas constitucionales que podría plantear desde determinada perspectiva, la Sala prescindirá de hacer uso de la expresión listas negras, salvo que se trate de citaciones de documentos que hagan uso de esa expresión. Por supuesto, esas citaciones no podrán en modo alguno comprenderse como el desconocimiento, por parte de la Corte, de las válidas preocupaciones que genera esa denominación".

Por la cual se resuelve un recurso de apelación

En virtud de lo anterior, en esa sentencia la Corte puso de presente que la creación de ese tipo de listas es una práctica abusiva en materia de Tratamiento de datos. En esa sentencia, se analizaron, entre otros, los siguientes temas: 1) registros de información exclusivamente desfavorables; 2) los principios de habeas data como límite al Tratamiento de datos personales, y 3) prácticas abusivas en la administración de datos personales. Los registros de información exclusivamente desfavorables¹² no fueron aceptados por la Corte por ser utilizados para fines ilegales, discriminatorios y oscuros.

Obsérvese que desde la década de los noventa la Corte Constitucional ha rechazado este tipo de listas o registros por, entre otras, las siguientes razones:

En primer lugar, violan “las garantías constitucionales establecidas por el Estado Social de Derecho”¹³ pues, en ciertas ocasiones, están destinadas a “intimidar a las personas, o a amenazarles, o a hacerlas víctimas de referencias, o de las llamadas “listas negras”¹⁴.

En segunda medida, son un instrumento de indebida represión, persecución o coerción contra las personas¹⁵. Finalmente, la creación de dichas listas o registros son una práctica abusiva en la administración de datos personales porque “desvirtúan la finalidad constitucionalmente legítima de los procesos de administración de datos personales”¹⁶.

Para la Corte, esta práctica vulnera los derechos del debido proceso y el habeas data, razón por la cual la eliminación de esta base de datos debe hacerse de tal forma que no sea posible su consulta “física o electrónica en el futuro”. Varias razones motivaron la decisión de la Corte:

- i. Está prohibido la conformación de listas “de información personal con consecuencias exclusivamente desfavorables para el Titular del dato, en tanto esa práctica configura un ejercicio abusivo y desproporcionado de la facultad legal de administración de datos personales”¹⁷.
- ii. La inclusión de los datos personales en ese tipo de listas es contraria al principio de libertad porque no se tenía autorización del Titular del dato para incluirlo en ese tipo de listas.
- iii. Desconoce el principio de finalidad y legalidad, ya que, se usaron datos de un ciudadano para propósitos no autorizados por el Titular del dato y proscritos por la regulación.

Nótese que la prueba N° 1 del escrito de descargos, la recurrente lo rotula en los siguientes términos:

4.1.1. Prueba N°1. Inclusión de la línea móvil N° [REDACTED] en lista interna.
4.1.2. Prueba N°2. Inclusión de la línea móvil N° [REDACTED] en lista interna actual.

¹² La Corte también ha proscrito por considerarlas prácticas abusivas “(i) la confección de “listas negras”, que se restringen a incluir datos comerciales y financieros negativos; (ii) el uso coercitivo de los reportes de riesgo para obtener el pago de las obligaciones dinerarias, pretermitiéndose los procedimientos de los instrumentos de ejecución previstos en la ley; y (iii) de manera general, el uso indiscriminado de los reportes de riesgo como instrumento para la exclusión *in limine* del acceso a los productos financieros y de crédito”. (Corte Constitucional, Sentencia C-1011 de 2008).

¹³ Corte Constitucional, Sentencia T-987 de 2012. M.P. Dr. Luis Ernesto Vargas Silva.

¹⁴ Corte Constitucional, Sentencia T-34 de 1995.

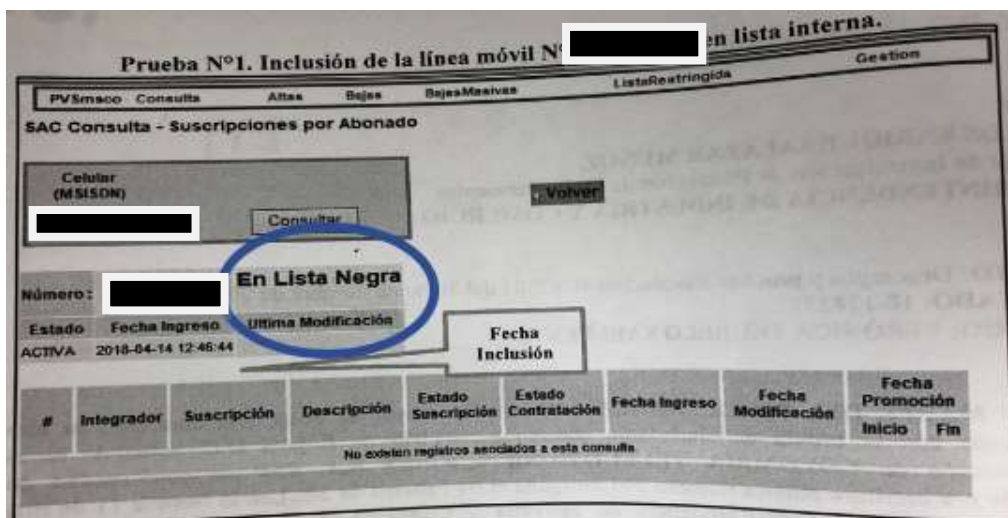
¹⁵ Corte Constitucional, Sentencia T- 761 de 2004.

¹⁶ Corte Constitucional, Sentencia C-1011 de 2008.

¹⁷ Corte Constitucional, Sentencia T-987 de 2012.

Por la cual se resuelve un recurso de apelación

No obstante, resulta que la prueba de la “inclusión de la línea móvil N° [REDACTED] en lista interna”, no es otra cosa que la evidencia de la inclusión del número de teléfono registrado por el usuario [REDACTED] a una base de datos que contraría los principios de libertad, legalidad y finalidad.



Como se mencionó previamente, este tipo de listas está proscrito (principio de legalidad) por el ordenamiento jurídico colombiano, ya que, configura un ejercicio abusivo y desproporcionado de la facultad legal de administración de datos personales. De igual forma, la recurrente está vulnerando el principio de libertad porque no se tenía la autorización de la Titular del dato para incluirla en esa clase de listados. Y, por consiguiente, se usaron datos de un ciudadano para finalidades no autorizadas por la Titular.

Incluso, es evidente para esta Delegatura que para la fecha la recurrente no ha atendido la solicitud de supresión de los datos del Titular porque COLOMBIA TELECOMUNICACIONES S.A. E.S.P. aún conserva en dicha lista el número del teléfono móvil de la Titular del dato.

En palabras de la Real Academia Española, suprimir es “Hacer cesar, hacer desaparecer”. Es decir, la recurrente no ha desaparecido la información de la Titular toda vez que todavía está inmersa en una base de datos ilícita.

Dado todo lo anterior y en virtud de las facultades legales de esta Delegatura, se solicitará a **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.**, que **elimine la base de datos “lista negra” y cese el uso de este tipo de listas o cree otras de esa naturaleza en un futuro.**

4. NO ES NECESARIO QUE SE CAUSE UN DAÑO PARA QUE SEA PROCEDENTE IMPONER UNA MULTA POR INFRACCIÓN A LA LEY 1581 DE 2012

En el caso concreto, la recurrente se pregunta ¿cuál fue la pérdida o perjuicio del usuario? en los siguientes términos (folio 62):

Por la cual se resuelve un recurso de apelación

Teniendo en cuenta que el daño se ha concebido mayoritariamente como la aminoración patrimonial sufrida por una persona con ocasión de la conducta desplegada por otra (natural o jurídica), lo cual genera per se un perjuicio como consecuencia, es claro que para que se predique daño y en consecuencia se genere su reparación, se tienen que verificar unos elementos necesarios que en el caso en particular no se encuentran demostrados tales como su veracidad, puesto que nunca fue claro ¿Cuál fue la pérdida o perjuicio del usuario?

Es suficiente desconocer cualquiera de las disposiciones de la Ley 1581 de 2012, para que la administración ejerza su poder sancionatorio dentro de los límites legales y observando el debido proceso.

En concordancia con lo dispuesto previamente en relación a la potestad sancionatoria del Estado, en el mismo sentido, y en relación con los principios¹⁸ señalados, dicha Corporación por medio de las Sentencias C-827 de 2001; C-401 de 2010 y C-948 de 2002 manifestó:

“En la doctrina¹⁹ se postula, así mismo, sin discusión que la administración o las autoridades titulares 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 explícita en los textos constitucionales. Así, a los principios de configuración del sistema sancionador como los de legalidad (toda sanción debe tener fundamento en la ley), tipicidad (exigencia de descripción específica 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 reprochabilidad dirigido al autor de un delito o falta²⁰), 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

¹⁸ “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.

¹⁹ Juan Alfonso Santamaría Pastor. Principios de Derecho Administrativo. Volumen II. Ed. Centro de Estudios Ramón Areces. Madrid. Tomo II. Segunda Edición. 2000.

²⁰ Ramón Parada Vásquez. Derecho Administrativo. Tomo I Marcial Pons. Madrid 1996. Luis Morell Ocaña. Curso de Derecho Administrativo. Tomo II “La actividad de las administraciones públicas. Su control administrativo y jurisdiccional”. Arandazi. Madrid. 1996.

Por la cual se resuelve un recurso de apelación

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 penas²¹. (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”*²².

Sobre dicho principio, la Corte Constitucional precisó lo siguiente en la Sentencia C-748 de 2011:

“En relación con el principio de tipicidad, encuentra la Sala que pese a la generalidad de la ley, es determinable la infracción administrativa en la medida en que se señala que la [sic] constituye el incumplimiento de las disposiciones de la ley, esto es, en términos específicos, la regulación que hacen los artículos 17 y 18 del proyecto de ley, en los que se señalan los deberes de los responsables y encargados del tratamiento del dato”.

Resulta útil reiterar la diferencia que existe entre los elementos que configuran la responsabilidad civil extracontractual y la facultad sancionatoria del Estado. Confunde el recurrente estas dos instituciones cuando afirma que “el denunciante no tuvo un daño en particular, para que existiese este se tenía que realizar una configuración entre un hecho generador, un nexo causal y finalmente un daño que fue el que en el expediente el denunciante nunca demuestra (...)”²³.

El ejercicio de *habeas data*, a saber, la solicitud de: corrección, actualización o supresión de los datos personales, no está sujeta a demostrar el acaecimiento de un daño y/o perjuicio. Incluso, los deberes que al Responsable le asigna el ordenamiento jurídico, no pueden ser evaluados a la luz del daño que ocasione su Tratamiento al Titular del dato. Los derechos que la Constitución Política de Colombia en su artículo 15 inciso segundo le confiere al Titular, le corresponden por su mera existencia y no al probar una situación fáctica. Recuérdese que la vulneración del debido Tratamiento de los datos personales no solo lesiona los derechos de una persona en particular, pero también, pone en riesgo los derechos humanos de toda la sociedad.

Bajo esta premisa, el ordenamiento jurídico colombiano le ha conferido a la Superintendencia de Industria y Comercio el deber de 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”²⁴. De este modo, no se enmarcan dentro de las competencias atribuidas a esta entidad aquellas que se desprenden de la configuración de la responsabilidad civil extracontractual.

Es decir, las normas que protegen el derecho a la protección de datos personales no se refieren a la responsabilidad civil de los Responsables o Encargados del Tratamiento de

²¹ Corte Constitucional. Sentencia C-406 de 2004.

²² Corte Constitucional. Sentencias C-1161 de 2000.

²³ Folio 89.

²⁴ Artículo 19 de la Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Por la cual se resuelve un recurso de apelación

datos. Resulta entonces que se trata es de una responsabilidad administrativa de la cual, pueden derivar multas y/o sanciones con el fin de promover y garantizar el cumplimiento del Régimen General de Protección de Datos Personales con el único propósito de amparar el derecho fundamental²⁵ a la protección de datos²⁶.

En suma, la Superintendencia de Industria y Comercio, está facultada para sancionar una vez se hubiese probado el desconocimiento de cualquiera de las disposiciones de la Ley 1581 de 2012. Por lo anterior tampoco se acogerá el argumento expuesto por el recurrente.

5. NECESIDAD DE LA ORDEN.

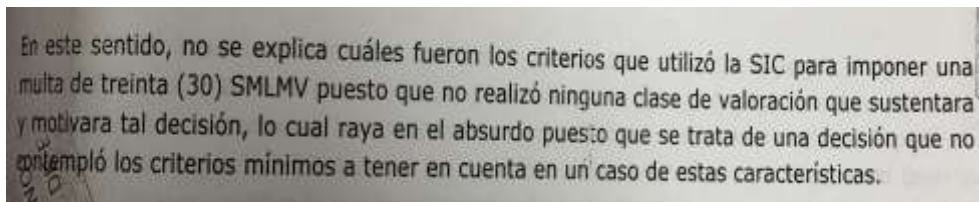
En su recurso de apelación, COLOMBIA TELECOMUNICACIONES S.A. E.S.P. arguye que la orden impartida por esta autoridad es exagerada. Entre otras, por cuanto no considera necesario que un tercero entre a pronunciarse sobre aspectos que son de ámbito privados de la compañía.

La orden no es exaerada porque la recurrente incumplió la ley y desconoció un derecho humano de una persona. La vulneración de derechos humanos no es un tema menor sino un asunto que demanda mucho cuidado, diligencia, profesionalismo y compromiso por parte de las organizaciones.

Otra cosa, es la manera de acreditar el cumplimiento de la orden. Sobre ese punto, la Delegatura considera apropiada la modificación que la Resolución N° 59232 del 31 de octubre de 2019 le realizó al segundo paragrafo de la resolución apelada. Aquella modificación, encaminada a permitirle a COLOMBIA TELECOMUNICACIONES S.A. E.S.P. acreditar el cumplimiento de la orden impartida por medio de un auditor interno o externo especializado en los temas que involucran la implementación de cada orden.

6. VALORACIÓN PROBATORIA Y DOSIMETRÍA PUNITIVA.

COLOMBIA TELECOMUNICACIONES S.A. E.S.P. considera que la sanción impuesta carece de motivación suficiente. Esto expresa en el folio 61:



En este sentido, no se explica cuáles fueron los criterios que utilizó la SIC para imponer una multa de treinta (30) SMLMV puesto que no realizó ninguna clase de valoración que sustentara y motivara tal decisión, lo cual raya en el absurdo puesto que se trata de una decisión que no contempló los criterios mínimos a tener en cuenta en un caso de estas características.

No comparte esta Delegatura el sentir de la recurrente, ya que, esta Entidad efectuó una correcta valoración probatoria en el caso bajo estudio. Lo anterior, por cuanto la Superintendencia de Industria y Comercio obró dentro del marco de sus facultades legales para, de una parte, garantizar a la Titular el derecho fundamental de la protección de datos personales y, de otra, respetar el debido proceso en cabeza de **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.**, En línea con lo anterior, tanto la investigación

²⁵ El derecho fundamental a la protección de datos personales, derecho humano (universal, inalienable, indivisible, irrenunciable e imprescriptible) que fue positivizado por el Constituyente Primario en el artículo 15 de la Constitución de 1991, y que en muchas ocasiones es conexo a otros derechos fundamentales de gran relevancia constitucional como la dignidad humana, el buen nombre, la intimidad, etc.

²⁶ Las sanciones impuestas en función del derecho administrativo sancionatorio pretenden asegurar el orden público y el correcto funcionamiento de la administración. Al respecto ver: Corte Constitucional, Sala Plena, C-703 de 2010, Magistrado Ponente Gabriel Eduardo Mendoza, Considerando 5; Corte Constitucional, Sala Plena, C-010-03, Magistrada Ponente Clara Inés Vargas.

Por la cual se resuelve un recurso de apelación

administrativa como la sanción impuesta se hicieron observando lo que ordena la regulación colombiana.

Sobre este particular, es necesario resaltar lo siguiente:

En primer lugar, el monto de la multa impuesta a la investigada, 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. El actuar de la recurrente fue negligente y violatorio de la ley por las razones mencionadas.

En segundo lugar, el monto de la multa impuesta no fue el máximo permitido (2000 salarios mínimos legales mensuales –SMLM-) sino de 30 SMLM que es equivalente al 1,5%.

En tercer lugar, debe recordarse que, las decisiones de la administración no necesariamente deben ser iguales en abstracto. Pues, todo dependerá de las similitudes o diferencias que se presenten con asuntos resueltos previamente por este operador, además se tendrán en cuenta los supuestos fácticos y jurídicos planteados en la queja o denuncia del Titular.

En cuarto lugar, es claro que la **Resolución N°19012 del 31 de mayo de 2019** fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Los cuales están contemplados en el artículo 3 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, *“debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad”*. De ahí que, la decisión emitida se ajuste a Derecho, pues fue producto de la aplicación del mandato legal y constitucional (artículo 209). 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.

En quinto lugar, la ley ordena a esta entidad que gradúe las sanciones teniendo en cuenta los criterios previstos en los artículos 23 y 24 de la Ley 1581 de 2012. En este orden de ideas, la Superintendencia de Industria y Comercio obró dentro los máximos permitidos por el artículo 23 de la Ley 1581 de 2012, y fue precisamente dentro de tales límites que impuso la sanción.

Al respecto, nótese que la recurrente considera que en su caso no hubo una correcta aplicación de los criterios de graduación de la infracción porque (folio 61):

De conformidad con lo anteriormente planteado, se advierte que la Superintendencia de Industria y Comercio en cuanto a los casos que tiene bajo investigación en materia de *habeas data*, debe observar además de los criterios generales, los criterios específicos que contiene la norma anteriormente precitada, y de esta manera motivar y justificar la sanción que impone en cada caso concreto.

Con esto en mente, en Sentencia C -748 del 2011, la Corte Constitucional determinó la constitucionalidad del artículo 24 de la Ley 1581 de 2012 en los siguientes términos:

“Este precepto se ajusta a la Constitución, en la medida en que corresponde al legislador establecer parámetros para que las autoridades, al momento de aplicar determinada sanción, puedan hacer graduaciones dependiendo de factores o circunstancias del investigado o de su actuación. En ese sentido, el precepto

Por la cual se resuelve un recurso de apelación

analizado consagra en los primeros 5 literales, circunstancias de agravación de la sanción, mientras el último, **el literal f) consagra una causal de disminución**". (Subrayado fuera de texto).

Así las cosas, como COLOMBIA TELECOMUNICACIONES S.A. E.S.P. no reconoció de forma expresa la infracción antes de la imposición de la multa, no se dio aplicación a la causal de disminución referida.

En relación a las circunstancias de agravación, establecidas en los primeros cinco literales del artículo 24 de la Ley 1581 de 2012, la Delegatura dio aplicación al criterio de agravación establecido en literal c) de la citada norma porque no es la primera vez que la recurrente es sancionada por la misma infracción. Esto pone de presente que no existe un debido tratamiento de datos personales dentro de dicha organización

En efecto, lo siguiente manifestó en la **Resolución N°19012 del 31 de mayo de 2019** (folio 43 reverso):

11.1.2 Reincidencia en la comisión de la infracción

Se tendrá en cuenta el criterio de agravación de la sanción contenido en el literal c) del artículo 24 de la Ley 1581 de 2012 en la medida en que con anterioridad a esta actuación la sociedad investigada ha sido sancionada en otra ocasión por la misma conducta violatoria de la Ley. Es decir que se observa reincidencia en el incumplimiento del deber garantizar el pleno y efectivo ejercicio del derecho de *Habeas Data*. Por lo anterior, este Despacho aumentará la sanción en un valor equivalente a DIEZ (10) salarios mínimos legales mensuales vigentes **adicionales**, para un total de **TREINTA (30)** salarios mínimos legales mensuales vigentes.

En efecto, enseguida se destaca las siguientes sanciones emitidas:

- **Expediente: 17-189716:**

Por medio de la Resolución No. 61063 de 24 de agosto de 2018 este Despacho sancionó a la sociedad **COLOMBIA TELECOMUNICACIONES S.A. E.S.P** por no haber atendido la solicitud del Titular de no recibir llamadas de contenido comercial por más de un año, en virtud de la petición presentada por éste el 19 de febrero de 2015.

Frente a la vulneración del deber mencionado, este Despacho sancionó a la citada sociedad por la suma de **CIENTO OCHENTA (180)** salarios mínimos legales mensuales vigentes, por el incumplimiento del deber contemplado en el literal a) del artículo 17, en concordancia, con el literal e) del artículo 8 de la Ley 1581 de 2012, así como del artículo 2.2.2.25.6 del Decreto Único 1074 de 2015.

En este orden de ideas, los criterios de agravación establecidos en los literales b), d) y e) del artículo 24 de la Ley 1581 de 2012 no se tuvieron en cuenta debido a que:

- Dentro de la actuación realizada no se encontró que la investigada hubiera obtenido beneficio económico alguno por la comisión de la infracción;
- No hubo resistencia u obstrucción a la acción investigativa de la Superintendencia y;
- No hubo renuencia o desacato a cumplir las órdenes e instrucciones del Despacho.

Por la cual se resuelve un recurso de apelación

En sexto lugar, es relevante tener presente que COLOMBIA TELECOMUNICACIONES S.A. E.S.P. trata datos de más de veintiocho millones de ciudadanos. Lo cual, genera la obligación de ser extremadamente diligente y garantizar la efectividad real (no formal) de los derechos de los Titulares de los datos. Esta es parte de la información que reportó esa sociedad en el Registro Nacional de Bases de Datos:

Nº de Radicado	Nombre de la Base de Datos	Cantidad de Titulares
16-201490--000000-000	Success Factors	5.131
16-201648--000000-000	Ttecnicos	23.500
16-202441--000000-000	Enlace Movistar	5.389
16-203309--000000-000	Adquira	1.500
16-203435--000000-000	Sales Force	165
16-203772--000000-000	Control Ingresos	30.000
16-204297--000001-000	SCL	23.243.180
16-204320--000000-000	ATIS	5.543.833
	Total:	28.852.698

Siendo esta la situación, la Delegatura confirma que, para la dosificación punitiva, además de lo expuesto hasta el momento, se consideró: el tamaño de la empresa, sus ingresos operacionales, patrimonio y en general, su información financiera. Lo anterior, de tal manera que la sanción tuviera un efecto disuasorio más no confiscatorio. Esto, como se pudo esbozar en la resolución apelada en los siguientes términos (folio 43 reverso):

También se tendrán en cuenta para la dosificación de la sanción, el tamaño de la empresa, sus ingresos operacionales, patrimonio y, en general, su información financiera, de tal forma que la sanción resulte disuasoria más no confiscatoria. Así como, la conducta de la investigada durante el trámite de la investigación administrativa.

Por último, afirma lo siguiente la recurrente (folio 62) :

En cuanto al perjuicio, dentro del presente caso no se evidencia de manera clara el daño causado al usuario puesto que tales afirmaciones no han pasado de ser aseveraciones no demostradas ni por el usuario ni por la SIC, puesto que no se logró establecer materialmente el daño y su valor.

Esta Delegatura no comparte la anterior apreciación de la recurrente porque la misma trata de restarle importancia no sólo a los Derechos Humanos sino también a las situaciones particulares de personas que se sienten agobiadas o fastidiadas de ser desatendidas por los Responsables de sus datos.

Al respecto, resulta que esta clase de procesos versan sobre una responsabilidad administrativa de la cual, pueden derivar multas y/o sanciones con el fin de promover y garantizar el cumplimiento del Régimen General de Protección de Datos Personales con el único propósito de amparar el derecho fundamental²⁷ a la protección de datos²⁸.

²⁷ El derecho fundamental a la protección de datos personales, derecho humano (universal, inalienable, indivisible, irrenunciable e imprescriptible) que fue positivizado por el Constituyente Primario en el artículo 15 de la Constitución de 1991, y que en muchas ocasiones es conexo a otros derechos fundamentales de gran relevancia constitucional como la dignidad humana, el buen nombre, la intimidad, etc.

²⁸ Las sanciones impuestas en función del derecho administrativo sancionatorio pretenden asegurar el orden público y el correcto funcionamiento de la administración. Al respecto ver: Corte Constitucional, Sala Plena,

Por la cual se resuelve un recurso de apelación

De esta manera, la vulneración del derecho de *habeas data* no solo afecta al Titular, también pone en riesgo los derechos de toda la sociedad. Por esto, las sanciones mencionadas 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*”²⁹. 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 democracia³⁰. 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.

Aunque las razones anteriores son suficientes para confirmar la **Resolución N°19012 del 31 de mayo de 2019**, esta Delegatura considera pertinente destacar lo siguiente respecto de:

- i. Responsabilidad Demostrada (*Accountability*) y “*Compliance*” en el Tratamiento de Datos Personales, y
- ii. Responsabilidad Personal de los Administradores

7. RESPONSABILIDAD DEMOSTRADA (*ACCOUNTABILITY*) Y “*COMPLIANCE*” EN EL TRATAMIENTO DE DATOS PERSONALES.

La regulación colombiana le impone al responsable o al encargado del tratamiento, la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica, ni limitarse únicamente a la formalidad. Por el contrario, debe ser real y demostrable. Al respecto, nuestra jurisprudencia ha determinado que “*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante*”³¹.

Adicionalmente, es importante resaltar que los responsables o encargados del tratamiento de los datos, no se convierten en dueños de los mismos como consecuencia del almacenamiento en sus bases o archivos. En efecto, al ejercer únicamente la mera tenencia de la información, solo tienen a su cargo el deber de administrarla de manera correcta, apropiada y acertada. Por consiguiente, si los sujetos mencionados actúan con negligencia o dolo, la consecuencia directa sería la afectación de los derechos humanos y fundamentales de los titulares de los datos.

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

C-703 de 2010, Magistrado Ponente Gabriel Eduardo Mendoza, Considerando 5; Corte Constitucional, Sala Plena, C-010-03, Magistrada Ponente Clara Inés Vargas.

²⁹ Organización de las Naciones Unidas (1948). Declaración Universal de los Derechos Humanos.

³⁰ Artículo 3 de la Carta Democrática Interamericana la cual se puede consultar en: http://www.oas.org/OASpage/esp/Documentos/Carta_Democratica.htm

³¹ Cfr. Corte Constitucional, sentencia T-227 de 2003.

Por la cual se resuelve un recurso de apelación

El artículo 26³² *-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 tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales.

El artículo 27 *-Políticas Internas Efectivas-*, exige que los responsables del tratamiento de datos implementen medidas efectivas y apropiadas que garanticen, entre otras: “(...) 3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento.”³³

Ahora, respecto de la supresión del dato, el artículo 18 señala que los procedimientos para dicho efecto, deben incluirse en la política de tratamiento de información y ser comunicados a los titulares de los datos³⁴. El artículo 22, por su parte, establece que el responsable o encargado del tratamiento debe adoptar “las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean (...) actualizados, rectificadas o suprimidos (...)”³⁵. Conforme con esta disposición, y sin necesidad de mayor análisis, es

³² El texto completo del artículo 26 del Decreto 1377 de 2013 ordena: “*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”

³³ El texto completo del artículo 27 del Decreto 1377 de 2013 señala: “*Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:* 1. *La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto.* 2. *La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.* 3. *La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento. La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tomada en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto”.*

³⁴ El texto completo del artículo 18 del Decreto 1377 de 2013 señala: “*Procedimientos para el adecuado tratamiento de los datos personales. Los procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización deben darse a conocer o ser fácilmente accesibles a los Titulares de la información e incluirse en la política de tratamiento de la información.”*

³⁵ El texto completo del artículo 22 del Decreto 1377 de 2013 ordena: “*Del derecho de actualización, rectificación y supresión. En desarrollo del principio de veracidad o calidad, en el tratamiento de los datos personales deberán adoptarse las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable*

Por la cual se resuelve un recurso de apelación

evidente la exigencia de la norma en el sentido de asegurarle al titular la posibilidad de supresión de sus datos, pues al tratarse de una obligación legal de resultado, deberá proceder la eliminación definitiva del dato personal cuando sea procedente y permitida por el ordenamiento jurídico.

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*”³⁶(*accountability*)³⁷.

El término “*accountability*”³⁸, a pesar de tener 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.

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

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 naturaleza³⁹ para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los responsables y encargados del tratamiento adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

Dichas acciones o 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 del mismo, 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

haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento”.

³⁶ El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

³⁷ “El término “*accountability*” puede ser traducido por *rendición de cuentas*. Esta voz inglesa, que, en su uso cotidiano, significa ‘responsabilidad’, ha comenzado a emplearse en política y en el mundo empresarial para hacer referencia a un concepto más amplio relacionado con un mayor compromiso de los Gobiernos y empresas con la transparencia de sus acciones y decisiones (...) el término *accountability* puede ser traducido por *sistema o política de rendición de cuentas* o, simplemente, por *rendición de cuentas* (...)” Recuperado de <https://www.fundeu.es/recomendacion/rendicionde-cuentas-y-norendimientomejor-que-accountability-1470/> el 22 de abril de 2019.

³⁸ Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.

³⁹ Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humana y de gestión. Asimismo involucran procesos y procedimientos con características propias en atención al objetivo que persiguen.

Por la cual se resuelve un recurso de apelación

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.

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que, *“la autorregulación sólo [sic] redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que **no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales**”*⁴⁰. (Énfasis añadido)

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, idóneas y suficientes, que permitan garantizar: i) los derechos de los titulares de los datos personales y ii) una gestión respetuosa de los derechos humanos.

Aunque no es espacio para explicar cada uno de los aspectos mencionados en la guía⁴¹, es destacable que el principio de responsabilidad demostrada se articula con el concepto de *compliance*, en la medida que este hace referencia a la autogestión o *“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”*⁴².

También se ha afirmado que, *“compliance es un término relacionado con la gestión de las organizaciones conforme a las obligaciones que le vienen impuestas (requisitos regulatorios) o que se ha autoimpuesto (éticas)”*⁴³. 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”*⁴⁴.

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

⁴⁰ Cfr. Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Mayo de 5 de 2006. En aquel entonces, la RIPD expidió un documento sobre autorregulación y protección de datos personales que guarda cercana relación con “accountability” en la medida que la materialización del mismo depende, en gran parte, de lo que internamente realicen las organizaciones y definan en sus políticas o regulaciones internas.

⁴¹ El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

⁴² Cfr. World Compliance Association (WCA). <http://www.worldcomplianceassociation.com/> (última consulta: 6 de noviembre de 2018).

⁴³ 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/>

⁴⁴ *Idem*.

Por la cual se resuelve un recurso de apelación

compromiso con la legalidad. Lo mismo sucede con “*accountability*” respecto del tratamiento de datos personales.

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 ejecuten, entre otros, un “*sistema de administración de riesgos asociados al tratamiento de datos personales*”⁴⁵ 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*”⁴⁶.

8. RESPONSABILIDAD DE LOS ADMINISTRADORES EN EL TRATAMIENTO DE DATOS PERSONALES.

Según el artículo 22 de la Ley 222 de 1995⁴⁷ la expresión administradores comprende al “*representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones*”. Cualquiera de ellos tiene la obligación legal de garantizar los derechos de los titulares de los datos y de cumplir la Ley 1581 de 2012 y cualquier otra norma concordante. Por esto, el numeral segundo del artículo 23 de la Ley 222 de 1995 determina que los administradores deben “*obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios*”, y además, en el ejercicio de sus funciones deben “*velar por el estricto cumplimiento de las disposiciones legales o estatutarias*” (énfasis añadido).

En vista de lo anterior, la regulación no exige cualquier tipo de cumplimiento de la ley, sino uno calificado. Es decir, ajustado o con exactitud a lo establecido en la norma. Velar por el estricto cumplimiento de la ley exige que los administradores actúen de manera muy profesional, diligente y proactiva para que en su organización la regulación se cumpla de manera real y no formal, con la efectividad y rigurosidad requeridas.

Por eso, los administradores deben cuidar al detalle y con perfecta seguridad este aspecto. No basta solo con ser guardianes, deben ser promotores de la correcta y precisa aplicación de la ley. Esto, desde luego, los obliga a verificar permanentemente si la ley se está o no cumpliendo en todas las actividades que realiza su empresa u organización.

El artículo 24⁴⁸ de la Ley 222 de 1995, presume la culpa del administrador “*en los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos*”.

⁴⁵ Cfr. Superintendencia de Industria y Comercio (2015) “*Guía para implementación del principio de responsabilidad demostrada (accountability)*”, págs 16-18.

⁴⁶ *Ibidem*.

⁴⁷ Ley 222 de 1995 “Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones”

⁴⁸ Artículo 24, Ley 222 de 1995 “*Responsabilidad de los administradores. El artículo 200 del Código de Comercio quedará así: Artículo 200. Los administradores responderán solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros.*

No estarán sujetos a dicha responsabilidad, quienes no hayan tenido conocimiento de la acción u omisión o hayan votado en contra, siempre y cuando no la ejecuten.

En los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos, se presumirá la culpa del administrador.

De igual manera se presumirá la culpa cuando los administradores hayan propuesto o ejecutado la decisión sobre distribución de utilidades en contravención a lo prescrito en el artículo 151 del Código de Comercio y demás normas sobre la materia. En estos casos el administrador responderá por las sumas dejadas de repartir o distribuidas en exceso y por los perjuicios a que haya lugar.

Por la cual se resuelve un recurso de apelación

Esta presunción de responsabilidad, exige que los administradores estén en capacidad de probar que han obrado con lealtad y la diligencia de un experto. Es decir, como un “*buen hombre de negocios*”, tal y como lo señala su artículo 23.

Adicionalmente, no debe perderse de vista que los administradores responden “*solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros*”⁴⁹. Las disposiciones referidas, prevén unos elementos de juicio ciertos, i) el alto nivel de responsabilidad jurídica y económica en cabeza de los administradores, y ii) el enorme profesionalismo y diligencia que debe rodear su gestión en el tratamiento de datos personales.

En virtud de lo expuesto, se considera necesario y consistente con la ley el exhorto que se hizo mediante la resolución recurrida.

9. DE LA APLICACIÓN DEL ARTÍCULO 49 DE LA LEY 1955 DE 2019.

Establece el artículo 49 de la Ley 1955 de 2019 lo siguiente:

“ARTÍCULO 49. CÁLCULO DE VALORES EN UVT. *A partir del 1 de enero de 2020, todos los cobros, sanciones, multas, tasas, tarifas y estampillas, actualmente denominados y establecidos con base en el salario mínimo mensual legal vigente (smmlv), deberán ser calculados con base en su equivalencia en términos de la Unidad de Valor Tributario (UVT). En adelante, las actualizaciones de estos valores también se harán con base en el valor de la UVT vigente.*

PARÁGRAFO. *Los cobros, sanciones, multas, tasas, tarifas y estampillas, que se encuentren ejecutoriados con anterioridad al 1 de enero de 2020 se mantendrán determinados en smmlv”. (negrilla fuera de texto)*

Por su parte el artículo 87 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, dispone lo siguiente:

ARTÍCULO 87. FIRMEZA DE LOS ACTOS ADMINISTRATIVOS. *Los actos administrativos quedarán en firme:*

- 1. Cuando contra ellos no proceda ningún recurso, desde el día siguiente al de su notificación, comunicación o publicación según el caso.*
- 2. Desde el día siguiente a la publicación, comunicación o notificación de la decisión sobre los recursos interpuestos.*
- 3. Desde el día siguiente al del vencimiento del término para interponer los recursos, si estos no fueron interpuestos, o se hubiere renunciado expresamente a ellos.*
- 4. Desde el día siguiente al de la notificación de la aceptación del desistimiento de los recursos.*
- 5. Desde el día siguiente al de la protocolización a que alude el artículo 85 para el silencio administrativo positivo. (destacamos)*

De conformidad con las normas anteriormente citadas, este Despacho modificará el artículo primero de la Resolución recurrida para indicar en Unidades de Valor Tributario

Si el administrador es persona jurídica, la responsabilidad respectiva será de ella y de quien actúe como su representante legal.

Se tendrán por no escritas las cláusulas del contrato social que tiendan a absolver a los administradores de las responsabilidades antedichas o a limitarlas al importe de las cauciones que hayan prestado para ejercer sus cargos”.

⁴⁹ Cfr. Parte inicial del artículo 24 de la Ley 222 de 1995.

Por la cual se resuelve un recurso de apelación

(UVT)⁵⁰ el valor de la multa impuesta en pesos colombianos, de conformidad con lo establecido en el artículo 49 de la Ley 1955 de 2019.

10. CONCLUSIONES

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

1. **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.** incumplió la Ley 1581 de 2012 porque no atendió oportunamente la solicitud de la Titular del Dato de suprimir su información.
2. Los derechos de las personas deben garantizarse de manera oportuna y correcta. La ley exige a los Responsables del Tratamiento responder dentro de un plazo concreto y no los faculta para hacerlo cuando quieran.
3. **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.** incluyó a la Titular del dato en una *“lista negra”* y, según las pruebas que obran en el expediente, el número de telefonía móvil celular aún permanece en la misma.
4. **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.** es el Responsable del Tratamiento de más de veintiocho (28) millones de personas, razón por la cual no solo debe ser muy profesional y diligente sino que está en la obligación de efectuar un debido Tratamiento de la información de las mismas y garantizar sus derechos.
5. Se confirmó que **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.** infringió abiertamente las normas sobre protección de datos personales consagradas en los literales e) del artículo 8 y a) del artículo 17 de la Ley 1581 de 2012, en concordancia con lo establecido en el artículo 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015.
6. La Delegatura confirmó **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.** ya había sido sancionada en otra ocasión por la misma conducta.
7. 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.
8. La facultad sancionatoria respecto de las normas de Tratamiento de datos personales no buscan indemnizar los eventuales daños y perjuicios causados por el indebido Tratamiento de esta información. Estas sólo hacen alusión a la responsabilidad administrativa de la cual pueden derivar multas y/o sanciones por el mero hecho de incumplir la regulación sobre tratamiento de datos personales. No es necesario que exista un daño o perjuicio para imponer una sanción por dicha razón, ni mucho menos que el monto de la multa deba ser igual o inferior al de los daños y perjuicios.

Así las cosas, una vez analizada toda la actuación administrativa, la información y documentos que conforman el expediente, encuentra el Superintendente Delegado para la Protección de Datos Personales que la resolución objeto de impugnación fue expedida

⁵⁰ De conformidad con lo establecido en la Resolución No. 84 del 28 de noviembre de 2019 expedida por la Dirección de Impuestos y Aduanas Nacionales, el valor de la UVT para el 2020 es de \$35.607

Por la cual se resuelve un recurso de apelación

observando la ley. De esta forma y conforme con lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, se confirmará en su totalidad, la Resolución No. 19012 de 31 de mayo de 2019.

Para efectos de la notificación se procederá conforme lo ordena el artículo 4⁵¹ del Decreto Legislativo 491 del 28 de marzo de 2020.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO. MODIFICAR el ARTÍCULO PRIMERO de la Resolución No. 19012 de 31 de mayo de 2019 de conformidad con lo expuesto en la parte motiva del presente acto administrativo:

“ARTÍCULO PRIMERO: IMPONER una sanción pecuniaria a la sociedad **COLOMBIA TELECOMUNICACIONES S.A. E.S.P** identificada con el Nit. 830.122.566-1 de VEINTICUATRO MILLONES OCHOCIENTOS CUARENTA Y TRES MIL CUATROSCIENTOS OCHENTA PESOS M/cte. (\$24.843.480) equivalente a 697,713371 Unidades de Valor Tributario (UVT), por la violación a lo dispuesto en el literal a) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal e) del artículo 8 de la misma ley y el artículo 2.2.2.25.6 del Decreto Único Reglamentario 1074 de 2015.”

ARTÍCULO SEGUNDO. CONFIRMAR en todas sus partes la Resolución No. 19012 de 31 de mayo de 2019, de conformidad con lo expuesto en la parte motiva del presente acto administrativo y las modificaciones realizadas en la Resolución 59232 del 31 de octubre de 2019.

ARTÍCULO TERCERO. Exhortar al Representante Legal de **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.**, señor FABÍAN ANDRÉS HERNANDEZ RAMIREZ identificado con la Cédula de Ciudadanía No. 93.380.737 para que elimine la “lista negra” cuya existencia fue evidenciada en esta actuación administrativa.

ARTÍCULO CUARTO. Notificar personalmente el contenido de la presente resolución a **COLOMBIA TELECOMUNICACIONES S.A. E.S.P.**, identificada con el Nit. 830.122.566-1a través de su representante legal o su apoderado o quien haga sus veces, entregándole

⁵¹ El artículo 4 del Decreto Legislativo 491 de 2020 ordena lo siguiente: "*Notificación o comunicación de actos administrativos. Hasta tanto permanezca vigente la Emergencia Sanitaria declarada por el Ministerio de Salud y Protección Social, la notificación o comunicación de los actos administrativos se hará por medios electrónicos. Para el efecto en todo trámite, proceso o procedimiento que se inicie será obligatorio indicar la dirección electrónica para recibir notificaciones, y con la sola radicación se entenderá que se ha dado la autorización.*

En relación con las actuaciones administrativas que se encuentren en curso a la expedición del presente Decreto, los administrados deberán indicar a la autoridad competente la dirección electrónica en la cual recibirán notificaciones o comunicaciones."

Por la cual se resuelve un recurso de apelación

copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO QUINTO. Comunicar el contenido de la presente decisión al señor [REDACTED] [REDACTED] identificado con la Cédula de Ciudadanía N° [REDACTED] en su calidad de miembro de junta directiva de **COLOMBIA TELECOMUNICACIONES S.A. E.S.P**, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO SEXTO. Comunicar el contenido de la presente decisión a la señora [REDACTED] [REDACTED] identificada con la Cédula de Ciudadanía N° [REDACTED]. o a su apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., 03 de Julio de 2020

El Superintendente Delegado para la Protección de Datos Personales



NELSON REMOLINA ANGARITA

Por la cual se resuelve un recurso de apelación

Notificación

Sociedad: Colombia Telecomunicaciones S.A. E.S.P.
Identificación: Nit. 830.122.566-1
Representante legal: Fabian Andres Hernandez Ramirez
Identificación: C.C. 93.380.737
Dirección: Transversal 60 No.114A-55
Ciudad: Bogotá D.C.,
Correo electrónico: notificacionesjudiciales@telefonica.com

Apoderado:
Identificación:
Dirección:
Ciudad:
Correo electrónico:

[REDACTED]

Comunicación**Reclamante**

Señora:
Identificación:
Dirección:
Ciudad:
Correo electrónico:

[REDACTED]

Comunicación**Miembro de
Junta Directiva**

Señor:
Identificación:
Dirección:
Ciudad:
Correo electrónico:

[REDACTED]