REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 34638 DE 2020

(02 de Julio)

Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

Radicación 18 – 106257

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 mediante Resolución No. 20205 de 10 de junio de 2019[1], la Dirección de Investigación de Protección de Datos Personales, resolvió, entre otras, lo siguiente:

> **ARTÍCULO PRIMERO: Imponer** una sanción pecuniaria a la sociedad **DIRECTV COLOMBIA LTDA.** identificada con el Nit. 805.006.014-0 de doscientos veintitrés millones novecientos trece mil trescientos veinte pesos **M/CTE** ($223.913.320), equivalente a doscientos setenta (270) salarios mínimos mensuales vigentes, por la violación del literal g) del artículo 4 de la Ley 1581 de 2012, en concordancia con el literal d) del artículo 17 y el artículo 13 de la misma Ley.

SEGUNDO. Que la Resolución No. 20205 de 10 de junio de 2019[2], fue notificada mediante aviso a la sociedad **DIRECTV COLOMBIA LTDA** el día 19 junio de 2019.

TERCERO. Que mediante escrito presentado el día 04 de julio de 2019[3], la sociedad **DIRECTV COLOMBIA LTDA** (en adelante la recurrente) mediante Apoderada General interpuso Recurso de Reposición y en subsidio de Apelación contra la Resolución No. 20205 de 10 de junio de 2019 con fundamento en los siguientes argumentos:

I. Ausencia de infracción.

Afirma la recurrente que "DIRECTV COLOMBIA NO INFRINGIÓ LAS OBLIGACIONES CONTENIDAS EN EL LITERAL d) DEL ARTÍCULO 17 Y EL ARTÍCULO 13 DEL MISMO CUERPO NORMATIVO"[4]. Esto, toda vez que la "Compañía cuenta con políticas robustas que permiten garantizar que los datos de nuestros clientes son tratados con las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento (…)"[5]. Lo anterior, según la recurrente, "no implica que

[1] Expediente, folios 152-163.
[2] Expediente, folio 170.
[3] Consecutivo número 18-106257- -00025-0001. Expediente, folios 171 a 196.
[4] Expediente, folio 174.
[5] Expediente, folio 175.

por razones ajenas a la voluntad de la Compañía y de nuestros funcionarios, se presenten casos aislados y excepcionales como el que aquí se analiza"[6].

II. Vulneración de los principios de proporcionalidad y razonabilidad sancionatoria.

Considera la recurrente que, "si bien existió un error en la notificación del paz y salvo, en ningún momento se evalúo el alto grado de responsabilidad de la Compañía en el tratamiento de dicha información, situación que permite entender que **DIRECTV** no se enmarca en el supuesto de la infracción o en su defecto, que el monto de la sanción a imponer debe ser considerablemente bajo, en virtud de los criterios de proporcionalidad"[7]. En este orden de ideas, "es desproporcionado a la falta cometida y a los hechos que la rodean, puesto que la Compañía no se ha visto involucrada en casos de reincidencia; no sacó provecho directo de infracción; el tercero que recibió información tampoco tuvo un beneficio a raíz de los datos que por error recibió; y a que DIRECTV cuenta con políticas claras de tratamiento de datos personales (..)"[8].

III. Error en la liquidación de la multa.

Argumente la recurrente, que "LA LIQUIDACIÓN DE LA MULTA SE DEBIÓ EFECTUAR CONFORME AL SALARIO MÍNIMO LEGAL MENSAL VIGENTE A LA OCURRENCIA DE LOS HECHOS"[9]. Como fundamento de esto, traen a colación el artículo 65 de la Ley 1341 de 2009, la cual dispone que "cualquiera de las infracciones señaladas en lo dispuesto en el artículo 64 del mismo cuerpo normativo, será sancionada, de tal forma que consagra en su inciso segundo que una de las formas para efectuarse puede ser (…) [que] la sanción debe indicarse en salarios mínimos legales mensuales, que serán liquidados conforme al valor legal establecido por el Gobierno Nacional"[10].

CUARTO. Que mediante la Resolución N° 40898 de 30 de agosto de 2019, la Dirección de Investigación de Protección de Datos Personales resolvió el recurso de reposición interpuesto por la recurrente, en donde se confirmó íntegramente la Resolución No. 20205 de 10 de junio 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 en el presente caso no se trata de una actuación relacionada con la garantía del habeas data contenido en el artículo 15 de la Constitución Política y cuyo texto es el siguiente: "*Todas las personas (…) tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*".

---

[6] Expediente, folio 175.
[7] Expediente, folio 178.
[8] Expediente, folio 1178.
[9] Expediente, folio 179.
[10] Expediente, folio 179.

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. 20205 de 10 de junio 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.

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011[11] 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. DEL PRINCIPIO Y DEL DEBER DE SEGURIDAD EN EL DEBIDO TRATAMIENTO DE DATOS PERSONALES.

Sin seguridad no existe debido tratamiento de datos personales. La seguridad no se logra con la mera redacción de políticas sino con la implementación real de las mismas en todas las actividades que involucran tratamiento de datos personales.

La recurrente fundamenta la presunta ausencia de infracción, en la existencia de *"(…) políticas robustas que permiten garantizar que los datos de nuestros clientes son tratado con las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*[12] De igual forma, insiste, que "*no hay lugar a que la SIC pretenda tener como vulnerada la normatividad ya mencionada, con base en circunstancias que no son recurrentes en nuestra Compañía, sino que por el contrario constituyen un caso aislado*"[13].

Respecto del principio y el deber de seguridad en el tratamiento de datos personales, existe una amplia regulación. No obstante, se destacan las siguientes:

Literal g) Artículo 4 de la Ley 1581 de 2012:

---

[11] 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.
[12] Folio 175.
[13] Folio 175.

"*En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*
(…)

g) *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.*

Literal d) Artículo 17 de la Ley 1581 de 2012:

"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"

Artículo 26 del decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015)

"*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)*

Por su parte, 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*."*[14] (Destacamos).

[14] Corte Constitucional. Sentencia C – 748 del 2011. M.P. JORGE IGNACIO PRETELT CHALJUB

La protección de datos personales no puede entenderse satisfecho con la mera generación de políticas escritas dirigidas al cumplimiento del derecho. Lo anterior, implica que, a la luz del principio de responsabilidad demostrada, 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. Del mismo modo, el reto de las organizaciones frente al principio de seguridad va mucho más allá de la mera expedición de documentos o redacción de políticas.

El material probatorio que obra en el expediente permite comprobar que la recurrente cuenta con: una política de privacidad, una política de protección de la Información de la compañía y de la privacidad individual, una relativa a la protección de datos de carácter privado, norma de tratamiento de la información, manual de atención y trámite de PQRS´s, política de navegación y programa de protección de datos personales NIMYTY.

La recurrente ha redactado documentos para cumplir con el principio y el deber de seguridad[15]. En ese sentido, afirma lo siguiente "*Contrario a lo indicado en la imputación establecida por el ente sancionador, DIRECTV es una Compañía que cuenta con políticas robustas que permiten garantizar que los datos de nuestros clientes son tratados con las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento (…)*"[16].

DIRECTV COLOMBIA LTDA no demostró ha adoptado medidas apropiadas y efectiva para cumplir el principio y el deber de seguridad. En este caso, sólo ha implementado medidas formales, las cuales son insuficientes para garantizar un tratamiento seguro de los datos personales.

Exigencia	Cumplimiento
¿Demuestra DIRECTV haber **documentado** una política para garantizar el principio de seguridad en el tratamiento de datos personales?	Si (folios 14-80).
¿Demuestra DIRECTV haber **implementado** las políticas para garantizar el principio de seguridad en el tratamiento de datos personales?	No.
¿Demuestra DIRECTV haber **monitoreado** el cumplimiento de las políticas para garantizar el principio de seguridad en el tratamiento de datos personales?	No.

En el presente caso quedó demostrado que la recurrente remitió un certificado de paz y salvo con información de carácter personal a un tercero no autorizado. En otras palabras, no cumplió el deber y el principio de seguridad porque permitió que un tercero no autorizada conociera información privada de otra persona. En otras palabras, no adoptó las medidas de seguridad necesarias para impedir la consulta, uso o acceso no autorizado de esos datos. Al contrario, lo que hizo la recurrente fue facilitar esa conductas al remitir datos personales de naturaleza privada a un tercero no autorizado por el Titular del Dato.

La protección de datos personales no puede entenderse satisfecha con la mera redacción de políticas. No se trata de garantizar seguridad en el papel sino en la práctica. En el

[15] Cfr. Folios 19, 28, 29, 30, 32, 35
[16] Folio 175.

presente caso, la recurrente no sólo falló en garantizar la seguridad en el tratamiento de datos sino que fue el responsable de dicha falencia.

Por todo lo expuesto, no son de recibo los argumentos de la recurrente.

3. PROPORCIONALIDAD DE LA SANCIÓN.

La recurrente afirma que a multa impuesta por esta autoridad es claramente desproporcionada. Asimismo, manifiesta que resulta lesiva y excesiva, si se compara con la conducta desplegada por la investigada, lo que la hace vulnerar los principios constitucionales, así como las garantías procesales del administrado.

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. Mediante la resolución 20205 de 2019 se precisó lo siguiente:

> 9.1.1 *La dimensión del daño o peligro a los intereses jurídicos tutelados por la ley*
>
> De la lectura del artículo 24 de la Ley 1581 de 2012, resulta claro que para que haya lugar a la imposición de una sanción por parte de esta Dirección, basta que la conducta desplegada por la investigada haya puesto en peligro los intereses jurídicos tutelados por la Ley 1581 de 2012. La norma, pues, hace una distinción entre el daño concretado y el peligro o riesgo a los intereses jurídicos tutelados por la Ley 1581 de 2012, entre otros, la protección del derecho fundamental a la protección de datos personales y *habeas data*.
>
> En el caso sub-examine, con base en el literal a) del artículo 24 de la Ley 1581 de 2012, esta Dirección evidencia que los cargos comprobados en contra de la sociedad **DIRECTV COLOMBIA LTDA.** afectaron de forma real y concreta los derechos fundamentales del denunciante, [redacted] cuando se comunicó su información personal a un tercero, sin la debida autorización.

En segundo lugar, el monto de la multa impuesta no fue el máximo permitido (2000 salarios mínimos legales mensuales –SMLM-) sino de 270 SMLM que es equivalente al 13,5%.

En tercer lugar, y sin perjuicio de lo anterior, es claro que la Resolución N° 20205 de 10 de junio 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 protección de datos del Titular del Dato.

En tercer lugar, es pertinente precisar que las sanciones que se imponen dentro de esta clase de procesos, no derivan de los daños o perjuicios causados a los titulares por el uso ilegal de su información. Es decir, las normas que protegen el derecho de protección de datos no se refieren a la responsabilidad civil de los Encargados o Responsables del Tratamiento de 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 fundamental[17] a la protección de datos[18].

Finalmente, la vulneración del derecho de la protección de datos 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"*[19]. 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[20]. 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 y los expuestos en las resoluciones 20205 y 40898 de 2019, no se acogerán las consideraciones de la recurrente en la medida en que la sanción impuesta obedece a las particularidades propias de esta actuación administrativa.

4. LA MULTA SE IMPUSO TENIENDO EN CUENTA LO QUE ORDENA LA LEY 1581 DE 2012

Según la recurrente, "LA LIQUIDACIÓN DE LA MULTA SE DEBIÓ EFECTUAR CONFORME AL SALARIO MÍNIMO LEGAL MENSUAL VIGENTE A LA OCURRENCIA DE LOS HECHOS". Como fundamento de esto, cita el artículo 65 de la Ley 1341 de 2009.

Este argumento no es procedente porque la Ley Estatutaria 1581 de 2012 no solo es una norma de mayor jerarquía, sino posterior y especial la cual ordena lo siguiente:

> ***ARTÍCULO 23. SANCIONES.*** *La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*

---

[17] 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.

[18] 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.

[19] Organización de las Naciones Unidas (1948). Declaración Universal de los Derechos Humanos.

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

> *a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000)* ***salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción****. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó; (...). (Destacamos)*

Como se observa, la norma expresamente ordenes que las multas se impongan en ***salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción****.* Por eso, no son de recibo los argumentos de la recurrente.

Aunque las razones anteriores son suficientes para confirmar la Resolución recurrida, 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

5. 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*"[21].

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.

El artículo 26[22] -*Demostración*- establece que, "*los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria*

---

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

[22] 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:*

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*."[23]

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*[24]*(accountability)*[25]".

El término "*accountability"*[26], 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

---

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"

[23] 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 tenida 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".*

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

[25] *"El término inglés 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.

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

(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 naturaleza[27] 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 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***

[27] 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.

persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales"[28]. (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 guía[29], 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*"[30].

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)"* [31]. 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*"[32].

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.

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*"[33] que

---

[28] 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.

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

[30] Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com/ (última consulta: 6 de noviembre de 2018).

[31] 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/

[32] *Idem.*

[33] Cfr. Superintendencia de Industria y Comercio (2015) "*Guía para implementación del principio de responsabilidad demostrada (accountability)*", págs 16-18.

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*"[34].

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

Según el artículo 22 de la Ley 222 de 1995[35] 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 24[36] 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*". 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.

---

[34] *Ibidem*.

[35] 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"

[36] 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.
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".

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*"[37]. 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, es imperativo que el representante legal de la recurrrente adopte medidas pertinentes, útiles, efectivas y verificables con el fin de:

1. Respetar y garantizar los derechos de los titulares de los datos.
2. Evitar que se repitan hechos como los que dieron origen a la presente actuación.
3. Dar estricto cumplimiento de las disposiciones legales y estatutarias sobre tratamiento de datos personales.
4. Aplicar el principio de responsabilidad demostrada, observando las recomendaciones de la Superintendencia de Industria y Comercio incorporadas en la "Guía para implementación del principio de responsabilidad demostrada (accountability)"[38]. Especial énfasis se debe hacer en utilizar mecanismos de monitoreo y control que permitan comprobar la efectividad de las medidas adoptadas para garantizar en la práctica las seguridad de los datos.

7. 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:

---

[37] Cfr. Parte inicial del artículo 24 de la Ley 222 de 1995.

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

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 N° 20205 de 2019, indicando el equivalente Unidades de Valor Tributario (UVT)[39], de conformidad con lo establecido en el artículo 49 de la Ley 1955 de 2019.

8. CONCLUSIÓN

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

a) Sin seguridad no existe debido tratamiento de datos personales. La seguridad no se logra con la mera redacción de políticas sino con la implementación real de las mismas en todas las actividades que involucran tratamiento de datos personales. No se trata de garantizar seguridad en el papel sino en la práctica.

b) En el presente caso quedó demostrado que la recurrente remitió un certificado de paz y salvo con información de carácter personal a un tercero no autorizado. En otras palabras, no cumplió el deber y el principio de seguridad porque permitió que un tercero no autorizado conociera información privada de otra persona. En otras palabras, no adoptó las medidas de seguridad necesarias para impedir la consulta, uso o acceso no autorizado de esos datos. Al contrario, lo que hizo la recurrente fue facilitar esa conductas al remitir datos personales de naturaleza privada a un tercero no autorizado por el Titular del Dato.

c) En el presente caso, la recurrente no sólo falló en garantizar la seguridad en el tratamiento de datos sino que fue el responsable de dicha falencia.

d) 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,

[39] 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

ni mucho menos que el monto de la multa deba ser igual o inferior al de los daños y perjuicios.

e) Se confirmó que la recurrente efectivamente incurrió en las irregularidades por las cuales fue sancionada. Para efectos de la graduación de la sanción se aplicaron los criterios pertinentes del artículo 24 de la Ley 1581 de 2012.

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 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. 20205 de
2019.

Para efectos de la notificación se procederá conforme lo ordena el artículo 4[40] 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. 20205 de 10 de junio de 2019, de conformidad con lo expuesto en la parte motiva del presente acto administrativo:

> "**ARTÍCULO PRIMERO: IMPONER** una sanción pecuniaria a la sociedad **DIRECTV COLOMBIA LTDA.** Identificada con el Nit. 805.006.014-0 de DOSCIENTOS VEINTITRÉS MILLONES NOVECIENTOS TRECE MIL TRESCIENTOS VEINTE PESOS M/cte. ($223.913.320), equivalentes a 6288,463504 Unidades de Valor Tributario (UVT) por la violación del literal g) del artículo 4 de la Ley 1581 de 2012, en concordancia con el literal d) del artículo 17 y el artículo 13 de la misma ley."

ARTÍCULO SEGUNDO. CONFIRMAR en todas sus partes la Resolución No. 20205 de 10 de junio de 2019, de conformidad con lo expuesto en la parte motiva del presente acto administrativo y las modificaciones realizadas en la presente Resolución.

---

[40] 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."

ARTÍCULO TERCERO. Notificar personalmente el contenido de la presente resolución a **DIRECTV COLOMBIA LTDA**, identificada con el Nit. 805.006.014-0 a través de su representante legal o su apoderado o quien haga sus veces, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO CUARTO. Comunicar el contenido de la presente decisión al señor [redacted] identificado con la Cédula de Ciudadanía No. [redacted] o a su apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO QUINTO. Comunicar el contenido de la presente resolución 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., 02 de Junio de 2020

El Superintendente Delegado para la Protección de Datos Personales

NELSON REMOLINA ANGARITA

ALC

Notificación

Sociedad:	DIRECTV COLOMBIA LTDA
Identificación:	Nit. 805.006.014-0
Representante legal:	MARIANO DIAZ De VIVAR
Identificación:	C.E. 957957
Dirección:	Avenida carrera 45 (Autonorte) N°103-60
Ciudad:	Bogotá D.C.
Correo electrónico:	herari@directvla.com.co
Apoderada:	[redacted]
Identificación:	
Dirección:	
Ciudad:	
Correo electrónico:	

Reclamante

Señor:	[redacted]
Identificación:	
Correo electrónico:	