REPUBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 38261 DE 2021

(22 JUNIO DE 2021)

VERSIÓN PÚBLICA

"Por la cual se resuelve un recurso de reposición y se concede el recurso de apelación"

Radicación **19-139735**

EL DIRECTOR DE INVESTIGACIÓN DE 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, el numeral 8 del artículo 17 del Decreto 4886 de 2011 y

CONSIDERANDO

PRIMERO: Que mediante Resolución 20809 del 15 de abril de 2021[1], la Dirección de Investigación de Protección de Datos Personales resolvió imponer una sanción pecuniaria a la sociedad **BANCO DE BOGOTÁ,** identificada con Nit. 860.002.964-4, por un valor de **CINCUENTA MILLONES TREINTA Y DOS MIL CUATROCIENTOS VEINTICUATRO PESOS M/CTE ($50.032.424)** equivalente a **MIL TRESCIENTOS SETENTA Y OCHO (1.378) UVT**, por la violación a lo dispuesto en el literal d) del artículo 17, en concordancia con los literales f) y g) del artículo 4 de la misma Ley 1581 de 2012.

SEGUNDO: Que, la Resolución 20809 del 15 de abril de 2021 se notificó por aviso N°7362 el día 27 de abril de 2021, a la sociedad **BANCO DE BOGOTA**, según consta en la certificación expedida por la Secretaría General de esta Superintendencia, radicada bajo el número 19-139735-33 del 3 de mayo de 2021.

TERCERO: Que, dentro del término concedido para el efecto, mediante escrito radicado el 11 de mayo de 2021, bajo el número 19-139735-34, la sociedad **BANCO DE BOGOTA**, a través de apoderado general, interpuso recurso de reposición y en subsidio de apelación contra la Resolución 20809 del 15 de abril de 2021, con los siguientes argumentos:

*"(…)**I. Oportunidad del recurso:***

La Resolución fue notificada mediante aviso recibido el día 26 de abril de 2021. De conformidad con el articulo 69 del CPACA, la notificación se considerará surtida al finalizar el día siguiente al de la entrega del aviso en el lugar de destino, esto es, el día 27 de abril de 2021.

Por su parte, el artículo 76 del CPACA prevé que los recursos de reposición y apelación deberán interponerse por escrito en la diligencia de notificación personal, o dentro de los diez (10) días siguientes a ella, o a la notificación por aviso. Dicho plazo inició el 28 de abril de 2021 y finaliza el día 11 de noviembre de 2021.

Por lo anterior, el presente recurso es presentado dentro de la oportunidad legal respectiva.

1. ***La existencia de riesgos operativos y fallas humanas en cualquier empresa no puede evitarse en un ciento por ciento.***

Tal y como fuera expresado por el Banco en el escrito de descargos, la conducta censurada por la SIC no fue deliberada ni mucho menos reiterada, como tampoco el producto de la omisión gravemente culposa del Banco en la aplicación de controles que garanticen la privacidad y protección de los datos personales de sus clientes.

Los hecho materia de investigación los explica un error humano cometido por parte (sic) la persona encargada de atender las reclamaciones tanto del quejoso [redacted] *como de* [redacted]*, quien, a raíz de la homonimia en el apellido de ambos*

[1] Actuación radicada el 16 de abril de 2021, bajo el número 19-139735-00025

clientes cuyas reclamaciones estaba gestionando y atendiendo, envió por error la información del segundo de ellos al correo del primero.

Ahora bien, se insiste que ello no se dio como consecuencia de la inexistencia, inoperancia o falta de idoneidad de los controles diseñados y aplicados por el Banco para efectos de garantizar la privacidad y protección de los datos personales de sus clientes, sino que se trató de la materialización de un riesgo operativo, inherente a las actividades en donde participa algún proceso operativo humano, sin que se trate de una conducta repetitiva o un riesgo que, a pesar de haberse materializado con anterioridad, el Banco hubiere sido indiferente frente a este.

Para este caso que nos ocupa, el gestor de las PQR tuvo acceso al contenido de ambas PQR cuya atención se le encargó; lastimosamente copió la información de una de ellas y la agregó en la respuesta que iba a dar a la otra, como consecuencia de una confusión por el apellido que era idéntico para ambos reclamantes.

Ahora bien, se insiste, que no se trata de una conducta deliberada u el producto de un riesgo que a pesar de haber sido identificado por el Banco, no fue atendido en la oportunidad debida mediante la generación de un control para la misma. Se trató de una conducta humana, la cual no resulta infalible y que, aún existiendo controles, resulta físicamente imposible evitar la materialización de riesgos asociados a errores humanos en un ciento por ciento.

Por lo anterior, consideramos que no resulta cierto que se afirme que el Banco no ha establecido controles idóneos para dar cumplimiento a las normas sobre privacidad y protección de datos personales, en la medida en que la existencia de tales controles no puede significar que en un ciento por ciento pueda y deban ser evitados, pues no existe un sistema de administración de riesgos operativos que garantice que los errores humanos no puedan presentarse.

2. *Graduación de la sanción - Antecedentes de la SIC en la imposición de sanciones por cargos idénticos*

De manera subsidiaria, y en el remoto caso de que la SIC no acogiere o acogiere parcialmente los argumentos anteriormente expuestos, solicitamos tener en cuenta los siguientes aspectos para efectos de que la sanción impuesta sea reducida en forma sustancial, a saber:

(i) *Banco de Bogotá no suministró en forma deliberada información personal al quejoso.*
(ii) *El Banco sí cuenta con controles con el fin de garantizar la protección de los datos de sus clientes.*
(iii) *Aun cuando el Banco cuenta con tales controles, por un error humano, la información que venía dentro de la queja de otro cliente, se adosó al correo que se envió al quejoso, habida cuenta que un mismo gestor de PQR estaba atendiendo ambos casos, quien tuvo confusión a raíz de la homonimia en el apellido de ambos clientes.*

(iv) *El Banco, en los descargos, evidenció las políticas y controles para la protección de los datos de su clientela. Los hechos que motivaron esta actuación no fueron el resultado de la ausencia e inoperancia de dichos controles, pues no se trata de situaciones que hayan sucedido con frecuencia y frente a las que el Banco hubiere sido indiferente. Se trata de un riesgo residual producto de las conductas humanas que, por definición, no pueden ser infalibles.*

(…)

IV. Petición:

*Por las razones antes expuestas, respetuosamente le solicito **REVOCAR** completamente la Resolución número 20809 del 15 de abril de 2021 objeto de impugnación. En subsidio, solicito graduar la sanción impuesta con base en las consideraciones contenidas en el presente escrito.*

*De no accederse a lo solicitado, comedidamente agradezco conceder el recurso de apelación interpuesto como subsidiario.**"***

CUARTO: Competencia de la Superintendencia de Industria y Comercio

La Ley 1581 de 2012 establece que la Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley y sus decretos reglamentarios.

QUINTO: Que una vez revisado el cumplimiento de los requisitos establecidos en el artículo 77 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo y con base en lo expuesto por el apoderado especial de la recurrente, este Despacho procede a realizar las siguientes consideraciones:

Frente a los argumentos presentados por la sociedad **BANCO DE BOGOTA**, se encuentra que los mismos se concretan en los siguientes aspectos **(i)** La existencia de riesgos operativos y fallas humanas en cualquier empresa no puede evitarse en un ciento por ciento. **(ii)** Graduación de la sanción - Antecedentes de la SIC en la imposición de sanciones por cargos idénticos **(iii)** Respecto de las pretensiones

5.1 LA EXISTENCIA DE RIESGOS OPERATIVOS Y FALLAS HUMANAS EN CUALQUIER EMPRESA NO PUEDE EVITARSE EN UN CIENTO POR CIENTO.

El recurrente inicia el recurso manifestando que el hecho que dio origen a la presente investigación versa *de*

> *"(…) un error humano cometido por parte la persona encargada de atender las reclamaciones tanto del quejoso* [redacted] *como de* [redacted]*, quien, a raíz de la homonimia en el apellido de ambos clientes cuyas reclamaciones estaba gestionando y atendiendo, envió por error la información del segundo de ellos al correo del primero."*

Igualmente, sostiene que

> *"Ahora bien, se insiste que ello no se dio como consecuencia de la inexistencia, inoperancia o falta de idoneidad de los controles diseñados y aplicados por el Banco para efectos de garantizar la privacidad y protección de los datos personales de sus clientes, sino que se trató de la materialización de un riesgo operativo, inherente a las actividades en donde participa algún proceso operativo humano, sin que se trate de una conducta repetitiva o un riesgo que, a pesar de haberse materializado con anterioridad, el Banco hubiere sido indiferente frente a este.*
>
> *(…)*
>
> *Ahora bien, se insiste, que no se trata de una conducta deliberada u el producto de un riesgo que a pesar de haber sido identificado por el Banco, no fue atendido en la oportunidad debida mediante la generación de un control para la misma. Se trató de una conducta humana, la cual no resulta infalible y que, aún existiendo controles, resulta físicamente imposible evitar la materialización de riesgos asociados a errores humanos en un ciento por ciento."*

Al respecto, para esta Dirección, el hecho de que lo sucedido sea catalogado por la recurrente como una situación de *" homonimia en el apellido de ambos clientes cuyas reclamaciones estaba gestionando y atendiendo",* no desvirtúa la violación al Régimen de Protección de Datos Personales, que en este caso se materializó el día 24 de julio de 2018, cuando un funcionario del **BANCO DE BOGOTA**, estando en ejercicio de sus funciones, remitió vía correo electrónico, información referente a teléfono, correo electrónico y número de cuenta de ahorros del señor [redacted] al correo electrónico de otro Titular, cuya PQR no se relacionaba en nada con dicho asunto.

En el presente caso quedó demostrado que la recurrente remitió un correo con información de carácter personal a un tercero no autorizado. En otras palabras, no cumplió el deber de seguridad porque permitió que un tercero no autorizado conociera información semiprivada de otra persona, es decir, es claro que la recurrente 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 conducta al remitir datos personales de naturaleza semiprivada a un tercero no autorizado por el Titular del Dato.

Además de lo anterior, para este Despacho, este tipo de situaciones no pueden ser normalizadas, ni aceptadas, como se deduce de las argumentaciones del recurrente cuando afirma que este *"(...) Se trató de una conducta humana, la cual no resulta infalible y que, aún existiendo controles, resulta físicamente imposible evitar la materialización de riesgos asociados a errores humanos en un ciento por ciento (...)"*[2], ya que los responsables de tratamiento de datos personales deben conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.

Ahora bien, en el presente caso no se censuran las condiciones técnicas/tecnológicas de seguridad de la información tratada por la sociedad investigada; por el contrario, la censura recae en las condiciones humanas y administrativas, como también en los procesos uso y circulación de la información, en los cuales se debe garantizar la seguridad de la misma, las cuales fallaron en el presente caso porque la información personal de un tercero fue compartida sin su autorización al ser enviada al correo electrónico del denunciante.

Adicionalmente, contrario a lo afirmado por el recurrente, es frecuente que el error humano se constituya como causa primigenia de fallas de seguridad asociados a datos personales; razón por la cual, resulta imperioso ir más allá de la deficiente justificación otorgada por la sociedad investigada y, en su lugar, propender por la real demostración de los controles con la que cuenta el **BANCO DE BOGOTA**, de forma que si es posible que el banco pueda prever este tipo de situaciones y se mitiguen los riesgos de seguridad, estableciendo mecanismos de seguridad necesarios para impedir que terceros tengan acceso a la información personal con el fin de adulterarla, consultarla, usarla o acceder a ella.

En este punto, resulta necesario traer a colación apartes de la sentencia C-748 de 2011 de la Corte Constitucional, sobre el principio y deber de seguridad[3]

> *"(...)*
>
> ***Principio de seguridad:*** *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.*
>
> *De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto "diluvio de datos", a través del cual día a día la masa de datos personales existente, objeto de tratamiento y de ulterior transferencias, no cesa de aumentar. Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riegos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre.*
>
> *En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales" o "SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de "parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos".*
>
> *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.*
>
> *(…)"*

---

[2] Radicado 19-139735-34 del 11 de mayo de 2021

[3] Cfr. Corte Constitucional, sentencia C 748 del 2011 de fecha 6 de octubre de 2011, M.P.: Jorge Ignacio Pretelt Chaljub Considerando 2.6.5.2. Análisis de la constitucionalidad de los preceptos

Expuesto lo anterior, es claro que el principio de seguridad tiene un criterio especialmente preventivo, lo cual obliga a los Responsables y/o Encargados a adoptar medidas apropiadas y efectivas para evitar afectaciones a la seguridad de la información de los Titulares.

Proteger la información es una condición crucial del tratamiento de datos personales. Una vez recolectada debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos responsables y encargados del tratamiento. El acceso, la consulta y el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos que se quieran mitigar a través de las medidas de seguridad de naturaleza humana, física, administrativa, técnica o de cualquier otra índole.

Respecto lo anterior, esta Superintendencia ha sido enfática en señalar que las disposiciones contenidas en los artículos 2.2.2.25.6.1 y siguientes del Decreto Único Reglamentario 1074 de 2015, en relación con la adopción de políticas y procedimientos efectivos para el adecuado cumplimiento de la Ley 1581 de 2012 implican que concurran una serie de presupuestos que permitan evidenciar que los procedimientos implementados, en la práctica sean reales, efectivos, útiles y demostrables.

Así, la regulación colombiana le impone al Responsable y al Encargado del tratamiento la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia *"existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante*[4]*.* Adicionalmente, los Responsables y Encargados del tratamiento no son dueños de los datos personales que reposan en sus bases de datos o archivos. En efecto, ellos son meros tenedores que están en el deber de administrar de manera correcta, apropiada y acertada la información de las personas porque su negligencia o dolo en esta materia afecta los derechos humanos de los titulares de los datos.

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

El artículo 26[5] *-titulado DEMOSTRACIÓN-* establece que *"[l]os 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 que pone en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación en cita. 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.

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la *'Guía para implementación del principio de responsabilidad demostrada (accountability)"*[6]*.* El término *'accountability"* a pesar de los diferentes significados ha sido entendido en el campo de la protección de datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

---

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

[5] El texto completo del artículo 36 del decreto 1377 de 2013 ordena lo siguiente: Articulo 25. 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:

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 eran empresa, de acuerdo con la normativa vigente.

La naturaleza de los datos personales objeto del tratamiento.

El tipo de Tratamiento.

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 debería suministrar a esta una descripción de tos 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 tal 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 tos datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas*

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

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

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

El principio de responsabilidad demostrada -*accountability*- demanda implementar acciones de diversa naturaleza[7] 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 implementen medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia. Dichas medidas deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

El principio de responsabilidad precisa menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido tratamiento de los datos personales. El éxito 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.

Así las cosas, la protección de datos personales no puede entenderse cumplida con la simple implementación de políticas, se trata de garantizar la seguridad de los datos en la práctica. 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.

Por lo anterior, este Despacho reitera que, en aras de demostrar el cumplimiento del principio de responsabilidad demostrada, no basta con que los procesos o documentos estén elaborados y dispuestos para consulta y aceptación de los empleados de la **BANCO DE BOGOTA**, como lo quiere hacer ver el recurrente. El éxito de la aplicación y efectiva implementación de este principio dependerá del compromiso y demostración real por parte de todos los miembros de la organización, pero especialmente, de los directivos de las organizaciones, ya que sin su dirección y apoyo, todo esfuerzo será insuficiente para diseñar, implementar, revisar, actualizar y evaluar los programas de gestión de datos personales.

El principio de responsabilidad demostrada se articula con el concepto de "compliance" en la medida que este hace referencia *"al conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos"*[8].

Así las cosas, la identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del "compliance" y de la efectiva aplicación del principio de responsabilidad demostrada (accountability). De ahí que, se considere fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un sistema de administración de riesgos asociados al tratamiento de datos personales, 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.

---

[7] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humanas y de gestión que Involucran procesas y procedimientos

[8] Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com/que-es-compliance.php (última consulta 20 de abril de 2020)

Aunado a lo anterior, el cumplimiento de tal principio implica necesariamente garantizar y velar por el cumplimiento estricto de la normatividad aplicable al caso y poder demostrar que los documentos elaborados han sido diligenciados e implementados para que, a través de estos, se pueda demostrar el cumplimiento de la normatividad consagrada en el régimen de protección de datos personales contenido en la Ley Estatutaria 1581 de 2012.

Además de lo anterior, el cumplimiento de este principio busca que el Responsable del Tratamiento, así como el Encargado del Tratamiento demuestre que dentro de su organización se cuenta con

(i) Una estructura de gobierno corporativo en el sentido de que la formulación de políticas y procedimientos para el tratamiento reflejen una cultura de respeto a la protección de los datos personales;

(ii) Un programa corporativo que tenga controles efectivos, que responde al tamaño y estructura de la organización, destinado al cumplimiento, implementación y consolidación del régimen de protección de datos; y

(iii) Una evaluación y revisión continúa de los controles que lo integran, con el fin de determinar la pertinencia y eficacia del plan de gestión ara lo cual deberán desarrollarse auditorías internas para evaluar, en una fase preliminar, el grado de cumplimiento con la normatividad de protección de datos.

Sin embargo, este Despacho se permite reiterar que no basta con tener una cultura que propenda por el respeto en la teoría (como se demostró en la resolución recurrida), sino que dicha cultura debe materializarse en la práctica a través del efectivo cumplimiento de la Ley 1581 de 2012, más allá de que esta autoridad requiera a la recurrente sobre su cumplimiento, ya que es un deber de la organización dar pleno cumplimiento a tal normatividad y es un derecho constitucional del ciudadano que se le respeten sus datos personales.

Por lo expuesto, no son del recibo de este Despacho las afirmaciones de la recurrente.

5.2 GRADUACIÓN DE LA SANCIÓN - ANTECEDENTES DE LA SIC EN LA IMPOSICIÓN DE SANCIONES POR CARGOS IDÉNTICOS

En el escrito de recurso, la recurrente solicita reducir el monto de la sanción manifestando que

"(…)

> *De manera subsidiaria, y en el remoto caso de que la SIC no acogiere o acogiere parcialmente los argumentos anteriormente expuestos, solicitamos tener en cuenta los siguientes aspectos para efectos de que la sanción impuesta sea reducida en forma sustancial, a saber:*
>
> *I) Banco de Bogotá no suministró en forma deliberada información personal al quejoso.*
> *II) El Banco sí cuenta con controles con el fin de garantizar la protección de los datos de sus clientes.*
> *III) Aun cuando el Banco cuenta con tales controles, por un error humano, la información que venía dentro de la queja de otro cliente, se adosó al correo que se envió al quejoso, habida cuenta que un mismo gestor de PQR estaba atendiendo ambos casos, quien tuvo confusión a raíz de la homonimia en el apellido de ambos clientes.*
> *IV) El Banco, en los descargos, evidenció las políticas y controles para la protección de los datos de su clientela. Los hechos que motivaron esta actuación no fueron el resultado de la ausencia e inoperancia de dichos controles, pues no se trata de situaciones que hayan sucedido con frecuencia y frente a las que el Banco hubiere sido indiferente. Se trata de un riesgo residual producto de las conductas humanas que, por definición, no pueden ser infalibles."*

Dicho argumento de la recurrente se enmarca en la proporcionalidad de la sanción impuesta, por lo que esta Dirección le aclara a esta que al momento de proferir la Resolución 20809 del 15 de abril de 2021 tomó en cuenta los criterios dispuestos en el artículo 24 de la Ley 1581 de 2012, los cuales son:

> ***Artículo 24. Criterios para graduar las sanciones****. Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:*
> *a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;*
> *b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;*
> *c) La reincidencia en la comisión de la infracción;*
> *d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;*
> *e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;*
> *f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar."*

Ahora bien, el Consejo de Estado se ha pronunciado de la siguiente manera en cuanto al principio de proporcionalidad,

> *"(…) El principio de proporcionalidad de la sanción exige que la falta descrita y la sanción correspondiente a la misma resulten adecuadas a los fines de la norma, esto es, a la realización de los principios que gobiernan la función pública. Respecto de la sanción administrativa, la Corte Constitucional ha precisado que este principio 'implica también que ella no resulte excesiva en rigidez frente a la gravedad de la conducta, ni tampoco carente de importancia frente a esa misma gravedad'. (…)"*[9]

> *"(…) la proporcionalidad no está determinada por la argumentación o retórica que alrededor de ella se haga o no en los actos sancionatorios, sino por la relación de la magnitud de la sanción con las características y circunstancias de los hechos que le sirvan de fundamento, atendiendo a los parámetros señalados en el artículo 36 del CCA, esto es, que sea adecuada a los fines de la norma que la autoriza y proporcional a los hechos"*[10]*.*

Es claro entonces que los parámetros que condicionan el ejercicio de las facultades discrecionales por parte de la administración se concretan en la adecuación a los fines de la norma que la autorizan y la proporcionalidad con los hechos que le sirven de causa; criterios que se tuvieron en cuenta en el caso *sub examine*, comoquiera que el valor de la multa impuesta mediante el acto administrativo impugnado obedeció a que la entidad investigada vulneró el literal d) del artículo 17 de la Ley 1581 de 2012, transgrediendo con ello el derecho fundamental a la protección de datos personales del titular.

Así las cosas, el monto de la multa impuesta a la recurrente, es el resultado del análisis del daño y/o puesta en peligro del interés jurídico tutelado en el trámite de esta actuación administrativa.

De tal suerte que, **BANCO DE BOGOTA** al haber enviado el correo al denunciante dejando al descubierto datos personales semiprivados de un tercero, sin tomar las medidas de seguridad necesarias para impedir que esta situación ocurriese, puso en peligro los datos del Titular de la información en este caso del señor [redacted], razón por la cual se le impuso la sanción al Responsable de la información **BANCO DE BOGOTA**.

De lo anotado se colige 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 y de los supuestos fácticos y jurídicos planteados en la queja o denuncia del Titular, así como de las posibles causales de agravación o atenuación encontradas, por lo que las afirmaciones de la recurrente no son de recibo por este Despacho.

Además de lo anterior, vale la pena poner de relieve lo siguiente:

Causar un daño no es un requisito jurídico para que esta entidad pueda imponer multas o impartir órdenes. Acá no estamos frente a un proceso de responsabilidad civil para indemnizar perjuicios sino ante una actuación administrativa para establecer si se cumplió o no la regulación sobre tratamiento de dato personales. Es suficiente desconocer cualquiera de las disposiciones de la Ley 1581 de 2012, para que la administración ejerza su poder sancionatorio dentro del marco legal vigente y observando el debido proceso.

---

[9] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Quinta-Descongestión. Sentencia de 22 de febrero de 2018. Radicación Número: 25000232400020100034801. Consejera Ponente: Rocío Araújo Oñate.
[10] Consejo de Estado, sentencia 25000-23-24-000-2002-00524-01. Consejero de Ponente: Rafael E. Ostau de Lafont Pianeta

Adicionalmente, se reitera que la sanción impuesta además de obedecer a la desatención de los deberes legalmente establecidos en la regulación sobre tratamiento de datos personales resulta proporcional en consideración a: i) los supuestos fácticos y jurídicos que motivaron el acto administrativo recurrido; y ii) los documentos y demás elementos probatorios valorados en el curso de esta actuación administrativa. En todo caso, es fundamental que el operador jurídico realice un análisis conjunto y sistemático de los criterios mencionados. Así como de los elementos y pautas que estime convenientes, con el propósito de ponderar la gravedad de la conducta y la capacidad de pago de la entidad infractora.

En primer lugar, el monto de la multa impuesta a la investigada es el resultado del análisis del daño y/o puesta en peligro del interés jurídico tutelado en el trámite de la presente actuación administrativa, pues no se puede dejar de lado la conducta desplegada por el Responsable del Tratamiento al permitir la divulgación de información semiprivada de (1) un titular específicamente del señor [redacted] al denunciante [redacted], a través del correo electrónico [redacted] el 24 de julio del 2018.

En segundo lugar, la Resolución N°. 20809 del 15 de abril de 2021 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 de la Ley por parte de la recurrente.

Finalmente, la vulneración del derecho fundamental a la protección de datos personales no solo afecta a los titulares concernidos, 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.

Así las cosas, la defensa de un derecho fundamental no puede doblegarse ante los intereses económicos de un operador que violentó el ordenamiento jurídico.

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*"[11]. 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[12].

Por último, cabe recordarle a la recurrente que la Ley 1581 de 2012 no estableció en el artículo 23 y siguientes, ni en ninguna otra disposición, un sistema para la tasación de las multas que se pueden imponer por violaciones al Régimen de Habeas Data.

Tan solo dejó establecido que las sanciones económicas pueden oscilar en el rango de 1 a 2000 SMLMV y, por lo tanto, no existe criterio alguno que ate el monto que puede imponer esta Superintendencia a la reunión de uno o varios criterios, sino a la valoración que haga la administración de la gravedad que de cada uno de ellos se desprenda.

Así las cosas, la multa impuesta a la entidad **recurrente** es insignificante para el tope establecido en la norma, ya que porcentualmente la sanción fue del 2.75% del rango previsto permitido por la Ley 1581 de 2012, por lo que la sanción en términos matemáticos de ninguna forma es desproporcionada.

---

[11] Organización de las Naciones Unidas (1948). Declaración Universal de los Derechos Humanos
[12] Artículo 3 de la Carta Democrática Interamericana. Disponible en: http://www.oas.org/OASpage/esp/Documentos/Carta_Democratica.html

5.3 RESPECTO DE LAS PRETENSIONES

La recurrente solicita que se revoque la sanción impuesta o subsidiariamente que se reduzca.

Teniendo en cuenta que fueron desvirtuados los motivos de inconformidad esgrimidos por el **BANCO DE BOGOTA** en su escrito de recurso, esta Dirección no encuentra procedente conceder lo solicitado; razón por la cual, la Resolución 20809 del 15 de abril de 2021se confirmará la decisión adoptada.

Ahora bien, con respecto a reducir el monto de la sanción, teniendo en cuenta lo expuesto, en este acto administrativo, 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.

Por lo tanto, esta Dirección concederá el recurso de apelación interpuesto subsidiariamente por la recurrente y, en consecuencia, trasladará las presentes diligencias al Despacho del Superintendente Delegado para la Protección de Datos Personales.

SEXTO: CONCLUSIÓN

6.1 Respecto de "*la existencia de riesgos operativos y fallas humanas*", se precisa que esta situación no exonera a la sociedad **BANCO DE BOGOTA** de cumplir la Ley 1581 de 2012, por el contrario, la sociedad debe tomar medidas reales y efectivas con el fin de que hechos como este se repitan, con el fin de garantizar el derecho fundamental a la protección de datos personales.

6.2 Respecto de la graduación de la sanción**,** quedó claro que la sanción impuesta obedeció a los parámetros dictados por la Ley 1581 de 2012, teniendo en cuenta que, el daño al derecho fundamental a la protección de datos personales del Titular fue vulnerado por la sociedad al haber expuesto a través del correo electrónico [redacted] el 24 de julio de 2018, datos personales semiprivados del titular [redacted] al denunciante [redacted]

SÉPTIMO: Que analizadas todas las cuestiones planteadas con ocasión del recurso y al tenor de lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirmará en todas sus partes la Resolución 20809 del 15 de abril de 2021 y en consecuencia trasladará la presente actuación al Despacho del Superintendente Delegado para la Protección de Datos Personales.

OCTAVO: Que, como consecuencia de la situación actual, y teniendo en cuenta el Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional, se ha restringido el ingreso a las instalaciones de la Superintendencia, en consecuencia, se establecieron las medidas pertinentes para permitir el acceso completo a los expedientes por medios digitales.

Al punto se precisa que, con el fin de garantizar los derechos fundamentales de la sociedad **BANCO DE BOGOTÁ** con Número de Identificación Tributaria 860.002.964-4, **esta Dirección ha concedido el acceso al presente Expediente digital a esta**, por intermedio de su Representante Legal Principal vinculado al correo electrónico de notificación judicial de la sociedad rjudicial@bancodebogota.com.co, quien debe registrarse en calidad de persona natural, exclusivamente con los datos en mención, en el enlace https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php.

En caso de que la sociedad requiera un acceso adicional de consulta del Expediente, deberá dirigir su solicitud en tal sentido desde el correo electrónico de notificación judicial de la sociedad, a los correos electrónicos contactenos@sic.gov.co y habeasdata@sic.gov.co, indicando los nombres y números de identificación de las personas autorizadas, **acreditando para dicho efecto los debidos poderes y/o autorizaciones, según corresponda.**

Finalmente, indicando que la totalidad del Expediente se encuentra digitalizado para su consulta por medios virtuales, si la sociedad **BANCO DE BOGOTÁ** considera estrictamente necesario el acceso del Expediente en físico, deberá enviar un correo electrónico a contactenos@sic.gov.co y habeasdata@sic.gov.co, solicitando la asignación de una cita para revisión física del Expediente en las instalaciones de la Superintendencia de Industria y Comercio en la ciudad de Bogotá D.C., indicando el número de radicado. Lo anterior por cuanto se deben garantizar el ingreso a las instalaciones con las adecuadas medidas de bioseguridad.

En mérito de lo expuesto, este Despacho

RESUELVE

ARTÍCULO PRIMERO: CONFIRMAR integralmente el contenido de la Resolución N° 20809 del 15 de abril de 2021

ARTÍCULO SEGUNDO: CONCEDER el recurso de apelación interpuesto subsidiariamente por la investigada y, en consecuencia, trasladar las presentes diligencias al Despacho del Superintendente Delegado para la Protección de Datos Personales.

ARTÍCULO TERCERO: NOTIFICAR personalmente el contenido de la presente resolución a la sociedad **BANCO DE BOGOTÁ** identificada con el Nit. 860.002.964-4, a través de su representante legal y de su apoderado, entregándoles copia de la misma.

ARTÍCULO CUARTO: COMUNICAR el contenido de la presente resolución al señor [redacted], identificado con **C.C.** [redacted].

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá D.C., 22 JUNIO DE 2021

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

Firmado digitalmente por CARLOS ENRIQUE SALAZAR MUÑOZ
Fecha: 2021.06.22 17:34:35 -05'00'

CARLOS ENRIQUE SALAZAR MUÑOZ

Proyectó: JMBG
Revisó: SRB
Aprobó: CESM

NOTIFICACIÓN:

Entidad: **BANCO DE BOGOTÁ**
Identificación: Nit. 860.002.964-4
Representante Legal: Alejandro Augusto Figueroa Jaramillo
Identificación: C.C. 8.228.877
Apoderado: JOSÉ JOAQUÍN DÍAZ PERILLA
Identificación: C.C 4.040.329
Dirección: Calle 36 Nro. 7-47 piso 15
Ciudad: Bogotá, D.C.-Colombia
Correo electrónico: rjudicial@bancodebogota.com.co

COMUNICACIÓN:
Señor: [redacted]
Identificación: C.C. No. [redacted]
Ciudad: [redacted]
Correo electrónico: [redacted]