REPUBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO _14242_ DE 2022

(Marzo 23 de 2022)

Por la cual se resuelve un recurso de apelación

Radicación 19-139735

VERSIÓN PÚBLICA

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 (modificado por el artículo 6 del Decreto 92 de 2022), el numeral 3 del artículo 74 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo,

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

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

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."

TERCERO. Que mediante la Resolución Nº 38261 del 22 de junio del 2021 la Dirección de Investigación de Protección de Datos Personales decidió, "*CONFIRMAR integralmente el contenido de la Resolución N° 20809 del 15 de abril de 2021*".

CUARTO. Que el Titular [redacted] mediante correo electrónico radicó un complemento de información, en los siguientes términos:

"*Buen día. Confirmo recibido de la información.*

Sea esta la oportunidad de agradecer nuevamente a la Superintendencia de Industria y Comercio por su colaboración y trámite para el presente asunto. Sin duda este tipo de resultados permitirá evitar la recurrencia de estos desafortunados hechos con otros ciudadanos.

Quisiera respetuosamente solicitar la posibilidad de seguir al tanto del proceso.

En cualquier caso, reitero mi disposición para seguir colaborando con cualquier información adicional que se llegue a necesitar".

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

CONSIDERACIONES DEL DESPACHO

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

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011[2] (modificado por el Decreto 92 de 2022) establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destaca la siguiente:

"(…)

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

(…)"

2. DEL DEBER Y DEL PRINCIPIO DE SEGURIDAD

Sin seguridad no hay debido Tratamiento de Datos Personales. Por eso, la Ley 1581 de 2012 establece lo siguiente:

"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;(…)"[3]

En desarrollo de lo anterior, la Ley impone a los Responsables y Encargados del Tratamiento los siguientes deberes:

"*Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*; (…)"[4]

---

[2] 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.
[3] Cfr. Literal g) del artículo 4 de la Ley 1581 de 2012.
[4] Cfr. Literales d) y b) de los artículos 17 y 18 de la Ley 1581 de 2012.

"*Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares*" [5]

El principio y el deber de seguridad tienen un criterio eminentemente preventivo, lo cual obliga a los Responsables o Encargados del Tratamiento a adoptar las medidas necesarias para evitar posibles afectaciones a la seguridad de los datos. Pero si las medidas de seguridad fallan, las organizaciones deben estar preparadas para mitigar los riesgos y daños que se pueden causar a los derechos y libertades fundamentales de los Titulares y a las organizaciones.

Estos riesgos y daños pueden ser de gravedad y probabilidad variables, materiales o inmateriales, en particular, si esos incidentes generan situaciones de discriminación; divulgación de información o aspectos íntimos de los Titulares o daños a su dignidad, buen nombre o reputación; y afectación de datos de carácter sensible de niños, niñas y adolescentes o de personas con algún grado de discapacidad, grupos de personas en situación de especial vulnerabilidad, o en riesgo de exclusión social, o de seguridad, o cualquier otro perjuicio económico o social.

Adicionalmente, si las organizaciones no toman a tiempo las medidas técnicas y organizativas, aquellos eventos que afecten los Datos Personales pueden entrañar daños y perjuicios materiales o inmateriales para sus Titulares. De ahí que la importancia de la gestión de los incidentes de seguridad deba ser desde: i) el diseño de las actividades del Tratamiento; ii) el complemento de las políticas de seguridad de la información y protección de Datos; y iii) la ética corporativa de las empresas.

Las medidas de seguridad deben ser apropiadas considerando varios factores como: (i) los niveles de riesgo del Tratamiento para los derechos y libertades de los Titulares de los datos; (ii) la naturaleza de los datos; (iii) las posibles consecuencias que se derivarían de una vulneración para los Titulares, y la magnitud del daño que se puede causar a ellos, al Responsable y a la sociedad en general; (iv) el número de Titulares de los datos y la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles, (vii) el estado de la técnica, y (viii) el alcance, contexto y finalidades del Tratamiento de la información.

Todas las medidas de seguridad deben ser objeto de revisión, evaluación y mejora permanente.

Los incidentes de seguridad pueden generarse por diferentes razones como, entre otras, las siguientes:

- Inexistencia de políticas preventivas de seguridad
- Errores o negligencia humana.
- Casos fortuitos.

[5] Cfr. Literales n) y k) de los artículos 17 y 18 de la Ley 1581 de 2012. El Capítulo II, Título V de la Circular Única de la Superintendencia de Industria y Comercio describe la violación a los códigos de seguridad y la existencia de riesgos en la administración de la información de los Titulares como cualquier "violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base [sic] de datos [sic] física o automatizada administrada por el Responsable del Tratamiento o por su Encargado".

- Actos maliciosos o criminales.
- Fallas en los sistemas de la organización.
- Procedimientos defectuosos.
- Fallas en las operaciones.
- Alteración; destrucción; robo o pérdida de archivos físicos.

Todos los incidentes de seguridad deben ser tomados seriamente y evaluados por parte de las organizaciones. Los que inicialmente parezcan irrelevantes podrían ser significativos o graves respecto de los derechos y las libertades de los Titulares de la información.

En su recurso de apelación, la sociedad recurrente afirma lo siguiente:

> *"(...) 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".*

Esa afirmación no basta para desvirtuar la violación al Régimen de Protección de Datos Personales. En este caso, la transgresión se materializó el día 24 de julio de 2018, cuando un funcionario del **BANCO DE BOGOTÁ S.A.**, 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.

[redacted]

Anexo 6. Descargos.
Tercera respuesta emitida por el banco de Bogotá de fecha 24 de julio de 2018

En otras palabras, la recurrente remitió un correo con información de carácter personal a un tercero no autorizado. Por ende, incumplió el deber de seguridad porque permitió que un tercero no autorizado conociera información semiprivada de otra persona. Se destaca que en el presente caso **no se censuran las condiciones técnicas/tecnológicas de seguridad de la información tratada por la sociedad investigada**. El **reproche recae sobre la negligencia humana de personal de la recurrente y las falencias administrativas para evitar hechos como los que dieron origen a la actuación administrativa**.

Contrario a lo afirmado por la recurrente, es frecuente que el error humano se constituya como causa primigenia de fallas de seguridad asociados a Datos personales. Por tanto, es indispensables que se realicen esfuerzos idóneos para garantizar que todos los colaboradores de la organización actúen de manera muy profesional, diligente y proactiva para que la regulación se cumpla de manera real y no formal con la efectividad y rigurosidad requerida.

Por último, es cierto que la probabilidad de que se materialice una brecha nunca es cero. Es por lo que, una vez que se hayan tomado las medidas necesarias para mitigar los riesgos asociados con el incidente, las organizaciones deberán ejecutar un plan de monitoreo permanente y de prevención para evitar futuros eventos que puedan afectar los datos personales y los derechos de las personas titulares de esa información.

Una vez se hayan tomado las medidas necesarias para mitigar los riesgos asociados con el incidente de seguridad, las organizaciones deberán ejecutar un plan de prevención para evitar futuros eventos que puedan afectar los Datos Personales que han tratado.

Esto genera los siguientes retos al interior de las organizaciones como, entre otros, los siguientes:

- Revisar las condiciones del Tratamiento.
- Realizar auditorías internas, externas o mixtas.
- Robustecer las políticas, procesos y procedimientos.
- Ajustar las evaluaciones de impacto en Datos personales.
- Establecer esquemas de trabajo a corto, mediano y largo plazo. Así como los roles y responsabilidades.
- Generar apoyo y compromiso de la Alta Gerencia para desplegar los cambios que se requieran al interior de las organizaciones.

Así, es indispensable considerar algunos ejemplos de medidas a implementar con posterioridad a la ocurrencia de un incidente de seguridad:

- **Reforzar los programas de capacitación y educación del personal.**
- Identificar y mejorar los controles internos que no tuvieron el efecto esperado en la contención de la brecha de seguridad.
- Identificar y eliminar *malware* (programa maligno) o desactivar cuentas de usuarios vulnerables.
- Realizar un contraste con las medidas adoptadas para solucionar el incidente de seguridad en cuestión, y garantizar un análisis pormenorizado de las soluciones que pudieron haberse adoptado.
- Actualizar el antivirus de la organización.
- Analizar con el antivirus todo el sistema operativo, incluidas aquellas secciones que no se vieron afectadas.
- Garantizar que la estrategia adoptada encuentre un balance entre la continuidad del negocio y el riesgo intrínseco en los activos que se hayan visto afectados por el incidente de seguridad.
- Elaborar un informe final tendiente a recopilar la información, plazos de actuación y medidas adoptadas, de cara a una revisión por terceras personas.

La seguridad genera confianza. Si falla, es clave estar muy bien preparados y entrenados para actuar frente a los incidentes de seguridad de manera inmediata, profesional e inteligente.

Teniendo en cuenta lo anterior, y en especial lo que ordena el principio y el deber de seguridad, así como lo que implica el cumplimiento del Principio de Responsabilidad Demostrada -*Accountability*, este Despacho considera que no son de recibo los argumentos expuestos por la sociedad recurrente.

3. DE LA PROPORCIONALIDAD DE LA SANCIÓN

Según la Corte Constitucional, "*es innegable que a través del derecho administrativo sancionador se pretende garantizar la preservación y restauración del ordenamiento jurídico, mediante la imposición de una sanción que no sólo repruebe sino que también prevenga la realización de todas aquellas conductas contrarias al mismo. Se trata, en esencia, de un poder de sanción ejercido por las autoridades administrativas que opera ante el incumplimiento de los distintos mandatos que las normas jurídicas imponen a los administrados y aún a las mismas autoridades públicas*"[6].

Refiriéndose a la "*constitucionalidad del régimen sancionatorio administrativo aplicado a la protección del dato*", la Corte Constitucional precisó que la facultad investigativa y sancionatoria de esta entidad,

> "(…) *es una manifestación del jus punendi, razón por la que está sometida a los siguientes principios: (i) el principio de legalidad, que se traduce en la existencia de una ley que la regule; es decir, que corresponde sólo al legislador ordinario o extraordinario su definición. (ii) El principio de tipicidad que, si bien no es igual de riguroso al penal, sí obliga al legislador a hacer una descripción de la conducta o del comportamiento que da lugar a la aplicación de la sanción y a determinar expresamente la sanción. (iii) El debido proceso que exige entre otros, la definición de un procedimiento así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (v) La independencia de la sanción penal; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal*"[7].

La resolución recurrida fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Estos se encuentran consagrados 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 por parte del Banco de Bogotá de la regulación sobre tratamiento de datos personales[8].

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:

- Los supuestos fácticos y jurídicos que motivaron el acto administrativo apelado; y
- 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.

Por este motivo, es necesario reiterar lo siguiente:

---

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

[7] Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.21.3.1

[8] Se comprobó que la sociedad BANCO DE BOGOTÁ infringió abiertamente las normas sobre protección de datos personales consagradas 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.

En primer lugar, el monto de la multa impuesta al Banco de Bogotá 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. Precisamente, 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.

No sobra señalar que la sanción impuesta a la sociedad recurrente tiene como propósito que el Responsable **en el futuro no incurra en violaciones al derecho al debido Tratamiento de Dato personales** y, en su defecto, cumpla a cabalidad con las disposiciones de la Ley 1581 de 2012 y demás normas que rigen el sistema de protección de Datos personales en la República de Colombia.

En todo caso, la multa impuesta es proporcional si se tiene en cuenta que el momento límite de las sanciones establecido en el artículo 23 de la Ley 1581 de 2012 es de dos mil (2000) salarios mínimos legales mensuales vigentes, por lo que, para este caso, dicha multa, equivale a 2,7% del monto máximo permitido por la Ley.

Resulta útil mencionar, que, según la información reportada por la sociedad en el Registro Nacional de Bases de Datos, el **BANCO DE BOGOTÁ S.A.** trata Datos personales de tres millones ciento sesenta y seis mil cuatrocientos noventa y un (3.148.987) clientes. Lo cual lo obliga a ser extremadamente diligente y a garantizar la efectividad real (no formal) de los derechos de los Titulares de los Datos.

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.

Finalmente, resulta pertinente resaltar lo siguiente:

- La multa impuesta mediante la **Resolución 20809 del 15 de abril de 2021** ($50.032.424) equivale al 2,7% del máximo legal permitido por el artículo 23 de la Ley 1581 de 2012.
- El monto de dicha sanción es el resultado del análisis del daño y/o puesta en peligro de los intereses jurídicos tutelados en el trámite de la primera instancia de esta actuación administrativa. Así como del incumplimiento de los deberes impuestos por la Ley 1581 de 2012 a los Responsables del Tratamiento de los Datos personales.
- La Resolución recurrida fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Asimismo, también fue el resultado de la valoración fáctica y probatoria de la primera instancia que llevó a concluir y comprobar la vulneración al derecho de *habeas data* del Titular y en particular los mandatos legales señalados.
- Las sanciones que se imponen dentro de esta clase de procesos no derivan de los daños o perjuicios causados a los Titulares por incumplir la regulación sobre tratamiento de Datos personales. Es decir, las normas que protegen el derecho de *habeas data* o protección de Datos personales no se refieren a la responsabilidad civil de los Responsables del Tratamiento de Datos.
- No debe olvidarse que el respeto de los Derechos Humanos es un elemento esencial de la democracia[9]*.* 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.

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

Así las cosas, 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 y la misma se adoptó conforme a derecho.

4. LOS PRECEDENTES SANCIONATORIOS NO HACEN PARTE DE LOS CRITERIOS DE TASACIÓN Y GRADUACIÓN DE LAS SANCIONES ESTABLECIDO EN LA LEY 1581 DE 2012

En el recurso de reposición y en subsidio de apelación, la recurrente titula su segundo argumento en lo siguientes términos, "*Graduación de la sanción – Antecedentes de la SIC en la imposición de sanciones por cargos idénticos*". Si bien no desarrolla dicho postulado, sea esta la oportunidad para que el Despacho reitere la doctrina establecida en la Resolución Nº 47280 de julio 28 de 2021.

En primer lugar, los criterios de graduación de las sanciones son los señalados por el artículo 24 de la Ley Estatutaria 1581 de 2012. **Allí no se menciona las sanciones previas como factor de graduación de la sanción.** En efecto, dicha norma dice lo que sigue a continuación:

> ***"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".*

Sobre este artículo, la Corte Constitucional señaló que,

> "(…) *este precepto se ajusta a la Constitución, en la medida en que corresponde al legislador establecer parámetros para que las autoridades, al momento de aplicar determinada sanción, puedan hacer graduaciones dependiendo de factores o circunstancias del investigado o de su actuación. En ese sentido, el precepto analizado consagra* ***en los primeros 5 literales, circunstancias de agravación de la sanción, mientras el último, el literal f) consagra una causal de disminución***[10]*".* (Destacamos).

Como se observa, la Ley Estatutaria 1581 de 2012 no establece una tabla de montos o una "*tarifa legal*" por cada infracción a una norma, sino que ordena que se consideren los criterios precitados a la luz de las particularidades de cada caso concreto.

En segundo lugar, las decisiones de la administración no necesariamente deben ser iguales en abstracto. Pues, todo dependerá de los supuestos fácticos, el material probatorio y las circunstancias de cada caso. En este sentido, la Corte Constitucional ha establecido que "*la igualdad es un concepto relacional por lo que no puede aplicarse en forma mecánica o automática, pues no solo exige tratar igual a los iguales, sino también desigualmente las situaciones y sujetos desiguales"*[11]

En todo caso, la imposición de cada multa no es un acto caprichoso o arbitrario sino ajustado a derecho siguiendo lo establecido en el precitado artículo 24 y teniendo en cuenta las particularidades de cada actuación administrativa.

---

[10] Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.23.3.
[11] Cfr. Corte Constitucional, sentencia C-106 de 2004. M.P. Dra. Clara Inés Vargas Hernández

Con apoyo en estos argumentos, se reitera que los precedentes sancionatorios no hacen parte de los criterios de tasación y graduación de las sanciones establecido en la Ley 1581 de 2012.

5. LA ACTIVIDAD EMPRESARIAL DEBE SER RESPETUOSA DE LOS DERECHOS HUMANOS.

El artículo 2 de la Constitución de la República de Colombia de 1991 señala que son fines esenciales del Estado, entre otros, "*garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución*". De aquí se desprende la exigencia de obtener resultados positivos y concretos del conjunto de disposiciones mencionadas. En este caso en particular, del derecho constitucional a la protección de datos previsto en el artículo 15 superior.

La efectividad de los derechos humanos es un asunto de gran importancia en la sociedad a tal punto que es una exigencia de naturaleza constitucional y del más alto nivel en el ordenamiento jurídico. Por eso, el artículo 2 continúa ordenando a las "*autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares*".

Las normas que hablan de la protección de datos en el sentido que se estudia, deben ser interpretadas de manera armónica con el ordenamiento jurídico del cual hacen parte y sobre todo con su Constitución Política. Así, su artículo 333 que "la actividad económica y la iniciativa privada son libres, dentro de los límites del bien común". Dicho "bien común" se refiere a cuestiones relevantes para una sociedad como, entre otros, la protección de los derechos humanos porque son imprescindibles para que cualquier ser humano sea tratado como una "persona" y no como un objeto o cosa.

En línea con lo anterior, nuestra Carta Política recalca que la "libre competencia económica es un derecho de todos que supone responsabilidades" y que la "empresa, como base del desarrollo, tiene una función social que implica obligaciones". Como se observa, la actividad empresarial no puede realizarse de cualquier manera y en el mundo empresarial no tiene cabida jurídica la afirmación según la cual el "fin justifica los medios". En efecto, no se trata de una libertad ilimitada, sino de una actividad "restringida" porque no sólo debe ser respetuosa del bien común, sino que demanda el cumplimiento de obligaciones constitucionales y legales.

El bien común a que se refiere el precitado artículo 333 exige que la realización de cualquier actividad económica garantice, entre otras, los derechos fundamentales de las personas. Es por eso que la Constitución pone de presente que la participación en el mercado supone responsabilidades y que efectuar actividades empresariales implica cumplir rigurosamente las obligaciones previstas en la ley.

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

Ahora, según el artículo 22 de la Ley 222 de 1995[12] 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****".* (Destacamos).

[12] 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"

~~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 cumplimiento en todas las actividades que realiza su empresa u organización.

El artículo 24[13] de la Ley 222 de 2995, presume la culpa del administrador "*en los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos*". Dicha presunción de responsabilidad exige que los administradores estén en capacidad de probar que han obrado con lealtad y la diligencia de un experto. Es decir, como un *"buen hombre de negocios",* tal y como lo señala su artículo 23.

Adicionalmente, no debe perderse de vista que los administradores responden "*solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros*"[14]. Las disposiciones referidas, prevén unos elementos de juicio ciertos, (i) el alto nivel de responsabilidad jurídica y económica en cabeza de os administradores, y (ii) el enorme profesionalismo y diligencia que debe rodear su gestión en el tratamiento de datos personales.

CONCLUSIONES

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

- El principio y el deber de seguridad tienen un criterio eminentemente preventivo, lo cual obliga a los Responsables o Encargados del Tratamiento a adoptar las medidas necesarias para evitar posibles afectaciones a la seguridad de los datos.

- La recurrente remitió un correo electrónico con información de carácter personal a un tercero no autorizado. Por ende, incumplió el deber de seguridad porque permitió que ese tercero conociera información semiprivada de otra persona.

- En el presente caso no se censuran las condiciones técnicas/tecnológicas de seguridad de la información tratada por la sociedad investigada. El reproche recae sobre la negligencia humana de personal de la recurrente y las falencias administrativas para evitar hechos como los que dieron origen a la actuación administrativa.

- Sin seguridad no hay debido Tratamiento de Datos personales. Así las cosas, los Responsables del Tratamiento deben ser diligentes y muy profesionales con el Tratamiento seguro de los mismos.

- Todas las medidas de seguridad deben ser objeto de revisión, evaluación y mejora permanente.

---

[13] El texto completo del artículo 24 de la ley 222 de 1995 dice lo siguiente: "*Artículo 24. 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 socia1 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."

[14] Cfr. Parte inicial del artículo 24 de la ley 222 de 1995

- Los precedentes sancionatorios de esta Superintendencia de Industria y Comercio no hacen parte de los criterios de tasación y graduación de las sanciones establecido en la ley 1581 de 2012.

- Las decisiones de la administración no necesariamente deben ser iguales en abstracto. Pues, todo dependerá de los supuestos fácticos, el material probatorio y las circunstancias de cada caso. En este sentido, la Corte Constitucional ha establecido que "*la igualdad es un concepto relacional por lo que no puede aplicarse en forma mecánica o automática, pues no solo exige tratar igual a los iguales, sino también desigualmente las situaciones y sujetos desiguales"*[15]

- La multa impuesta mediante la **Resolución 20809 del 15 de abril de 2021** ($50.032.424) equivale al 2,7% del máximo legal permitido por el artículo 23 de la Ley 1581 de 2012.

- Según la información reportada por la sociedad en el Registro Nacional de Bases de Datos, el **BANCO DE BOGOTÁ S.A.** trata Datos personales de tres millones ciento sesenta y seis mil cuatrocientos noventa y un (3.148.987) clientes. Lo cual lo obliga a ser extremadamente diligente y a garantizar la efectividad real (no formal) de los derechos de los Titulares de los Datos.
- **La seguridad genera confianza.** Si falla, es clave estar muy bien preparados y entrenados para actuar frente a los incidentes de seguridad de manera inmediata, profesional e inteligente.

De esta forma y de acuerdo con lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho **confirma la Resolución 20809 del 15 de abril de 2021.**

En mérito de lo expuesto, este Despacho

RESUELVE

ARTÍCULO PRIMERO. CONFIRMAR la **Resolución 20809 del 15 de abril de 2021**, de conformidad con lo expuesto en la parte motiva del presente acto administrativo.

ARTÍCULO SEGUNDO. NOTIFICAR personalmente el contenido de la presente resolución a la sociedad **BANCO DE BOGOTÁ S.A.** identificada con el Nit. 860.002.964-4, a través de su representante legal y de su apoderado, entregándole copia de esta e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO TERCERO. COMUNICAR el contenido de la presente resolución al Titular [redacted], identificado con C.C. [redacted].

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

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá D.C., marzo 23 de 2022

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES

NELSON REMOLINA ANGARITA
Firmado digitalmente por NELSON REMOLINA ANGARITA
Fecha: 2022.03.23 14:33:58 -05'00'

NELSON REMOLINA ANGARITA

ALC

[15] Cfr. Corte Constitucional, sentencia C-106 de 2004. M.P. Dra. Clara Inés Vargas Hernández

Notificación

Sociedad: BANCO DE BOGOTÁ S.A.
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
Correo electrónico: rjudicial@bancodebogota.com.co
Dirección: Calle 36 Nro. 7-47 piso 15 y 4
Ciudad: Bogotá, D.C.
País: República de Colombia

Comunicación

Titular: [redacted]
Identificación: C.C. No. [redacted]
Correo electrónico: [redacted]