REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO _41580_ DE 2021

(Julio 6 de 2021)

Radicación 19-172149

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 y el numeral 7 del artículo 16 del Decreto 4886 de 2011 y,

CONSIDERANDO:

Primero. Que mediante oficio radicado con el número 19-172149-00 de 11 de julio de 2018, el señor [redacted], presentó ante esta superintendencia queja en contra de **BANCA DE SERVICIOS FINANCIEROS S.A.S. – BANSERFIN S.A.S.** (en adelante **BANSERFIN**), por una presunta vulneración a su derecho de *habeas data*.

Nombre Completo: BANCA DE SERVICIOS FINANCIEROS SAS
País: COLOMBIA
Departamento: BOGOTÁ
Ciudad: BOGOTA D.C.
Dirección: LEY PROTECCION DATOS PERSONALES
Correo Electrónico: feg@banserfin.com

RECLAMO DIRECTO

Manifiesto que efectué el reclamo directo ante el productor y/o proveedor, de forma ESCRITO, el día 31/07/2019.

Así mismo, me permito indicar que el demandado dio respuesta a mi reclamación el día 01/08/2019, manifestando Respetado Sr [redacted]
Por un error humano e involuntario de nuestra parte, el dia ayer remitimos un correo a su Email personal, que tenia la intencion de darle a conocer las posibilidades vigentes otorgadas por el Fondo de Empleados Granfondo FEG, para normalizar su obligacion y este fue copiado a otros usuarios de la entidad ya mencionada.
Ofrecemos disculpas por la incomodidad que le haya causado esta situacion y le garantizamos que en el futuro nos comunicaremos directamente en forma privada a su correo..

DECLARACIÓN DE VULNERACIÓN CONCRETA DE LOS DERECHOS COMO CONSUMIDOR O USUARIO

HECHOS

1. Las partes de este proceso tienen una relación derivada de: Cobro de cartera obligacion FEG
2. El derecho que como consumidor o usuario ha sido vulnerado es: Habeas Data Ley 1581
3. Las circustancias que rodearon el asunto materia de la demanda se concretan en: Falta al articulo 17 de la ley 1581 de 2012 dond ese permitio el acceso no autorizado almacenada en la base de datos de BANSERFIN, toda vez que quedron al descubierto direcciones de 265 correos electronicos, permitiendo con ello que terceras personas no autorizadas tuviesen acceso a estos datos de naturaleza privada y que potencialmente hagan uso indebido de estos, permitiendo la circulacion indiscriminada de informacion personal y en inoservancia de edidas minimas como el uso de la opcion de destinatario oculto integrada a todos los servicios de correo actuales

Imagen 1. Queja presentada ante esta Superintendencia radicada bajo el número 19-172149-00 de fecha 01 de agosto de 2019.

Segundo. Que mediante Resolución 56820 de 24 de octubre de 2019, el Director de Investigación de Protección de Datos Personales resolvió iniciar una investigación administrativa y formular cargos, con el fin de establecer si **BANSERFIN** infringió las normas sobre protección de Datos personales, en especial las establecidas en: (i) El literal d) del artículo 17 de la Ley 1581 de 2012, en concordancia con los literales f) y g) del artículo 4 de la misma Ley, y con el inciso final del artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015 y **(ii)** El literal n) del artículo 17 de la Ley 1581 de 2012, en concordancia con el artículo 25 de la misma normatividad, y a literal g) del capítulo segundo de la Circular Externa No 02 del 3 de noviembre de 2015 que *"Adiciona el Capítulo Segundo en el Título V de la Circular Única de esta Superintendencia, sobre el Registro Nacional de Datos - RNBD".*

Tercero. Que mediante escrito con número de radicado 19-172149-12 **BANSERFIN** presentó los respectivos descargos de conformidad con lo establecido en el artículo 47 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Cuarto. Que mediante Resolución 33121 de 30 de junio de 2020, el Director de Investigación de Protección de Datos Personales, de conformidad con lo establecido en el artículo 41 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, corrigió la Resolución 56820 de 24 de octubre de 2020, modificando a un cargo único el formulado a **BANSERFIN** e iniciando una investigación administrativa sancionatoria al **FONDO DE EMPLEADOS GRANFONDO – FEG** (en adelante **FONDO FEG**), así:

> *"**ARTÍCULO PRIMERO: ABRIR INVESTIGACIÓN** y en consecuencia **FORMULAR PLIEGO DE CARGOS** contra la sociedad **BANCA DE SERVICIOS FINANCIEROS S.A.S.** identificada con NIT. 900.069.458-1, por la presunta contravención de lo dispuesto en:*
>
> - *El literal b) del artículo 18 de la Ley 1581 de 2012, en concordancia con los literales f) y g) del artículo 4 de la misma Ley.*
>
> ***ARTÍCULO SEGUNDO: ABRIR INVESTIGACIÓN** y en consecuencia **FORMULAR PLIEGO DE CARGOS** contra el **FONDO DE EMPLEADOS GRANFONDO,** identificado con NIT. 800.097.913-8, por la presunta contravención de lo dispuesto en:*
>
> - *El literal i) del artículo 17 de la Ley 1581 de 2012, en concordancia con los literales f) y g) del artículo 4 de la misma Ley.*
> - *El literal n) del artículo 17 de la Ley 1581 de 2012, en concordancia con el artículo 25 de la misma normatividad, y a literal g) del capítulo segundo de la Circular Externa No. 02 del 3 de noviembre de 2015 que "[Adiciona el Capítulo Segundo en el Título V de la Circular Única de esta Superintendencia, sobre el Registro Nacional de Bases de Datos]".*

Quinto. Que una vez agotada la etapa probatoria y efectuado el análisis de los escritos de descargos[1] y de los diferentes medios probatorios allegados oportunamente al expediente, la Dirección de Investigación de Protección de Datos Personales, mediante Resolución 78239 de 4 de diciembre de 2020, resolvió:

> *"**ARTÍCULO PRIMERO: IMPONER** una sanción pecuniaria a la sociedad **BANCA DE SERVICIOS FINANCIEROS S.A.S.**, identificada con Nit. 900.069.458-1 de **QUINCE MILLONES DE PESOS M/CTE ($15.000.000) equivalente a 421,2654815 (UVT)** Unidad de Valor Tributario, por la violación alo dispuesto en el literal b) del artículo 18, en concordancia con los literales f) y g) del artículo 4 de la Ley 1581 de 2012.*
>
> *(…)*
>
> ***ARTÍCULO TERCERO: IMPONER** una sanción pecuniaria a la sociedad **FONDO DE EMPLEADOS GRANFONDO – FEG.**, identificada con Nit. 800.097.913-8 de **VEINTE MILLONES DE PESOS M/CTE ($20.000.000) equivalente a 561,6873087 (UVT)** Unidad de Valor Tributario, por la violación a lo dispuesto en:*
>
> *i) El literal i) del artículo 17, en concordancia con los literales f) y g) del artículo 4 de la Ley 1581 de 2012 y,*
>
> *ii) El literal n) del artículo 17, en concordancia con el artículo 25 de la Ley 1581 de 2012, y literal g)del capítulo segundo de la Circular Externa No. 02 del 3 de noviembre de 2015 que "Adiciona elCapítulo Segundo en el Título V de la Circular Única de esta Superintendencia, sobre el RegistroNacional de Bases de Datos –RNBD".*

Sexto. Que en el término legal establecido para el efecto[2], mediante escritos radicados con los números 19-172149-44 de 21 de diciembre de 2020 y 19-172149-46 de 31 de diciembre de 2020, el Representante Legal de **BANSERFIN,** y el apoderado especial de **FONDO FEG** interpusieron recurso de reposición y en subsidio de apelación contra la Resolución No. 78239 de 4 de diciembre de 2020.

1. El Representante Legal de **BANSERFIN,** sustentó el recurso en los siguientes términos:

> ***a) NO FUERON TENIDOS EN CUENTA LOS ARGUMENTOS JURÍDICOS, FACTICOS Y PROBATORIOS QUE SE ARRIMARON EN LA RESPUESTA AL PLIEGO DE CARGOS.***
>
> *Respetuosamente consideramos que su despacho no tuvo en cuenta los objetivos, debidamente probados y sustentados fundamentos soportes que arrimamos como respuesta al pliego de cargos en contra de nuestra entidad, para finalmente imponernos una sanción idéntica a la impuesta al Fondo de Empleados Gran Fondo por el cargo primero (como se puede evidenciar en el numeral decimo tercero de la parte motiva de la*

[1] **BANSERFIN** presentó su escrito de Descargos el día 27 de julio de 2020, con el número radicado 19-172149-24. Por su parte **FEG**, presentó su escrito el día 11 de agosto de 2020, con el número radicado 19-172146-26.

[2] Conforme a constancia suscrita por la Coordinadora del Grupo de Notificaciones y Certificaciones de esta Superintendencia, radicada en el sistema de trámites bajo el número 19-172149-43 del 17 de diciembre de 2020, la Resolución 78239 del 4 de diciembre de 2020 fue notificada a **BANSERFIN** de manera electrónica el 7 de diciembre de 2020 y por aviso a **FEG** el 17 de diciembre de 2020.

resolución de sanción), cuando siempre hemos dado oportuna respuesta, estricta sujeción a los requerimientos de la SIC sobre el caso que nos ocupa, dicho en otros términos dentro del trasegar del proceso hemos desplegado con absoluta corrección y respeto una conducta responsable, de total colaboración, información, transparencia y allanamiento a los cargos y requerimientos de la SIC y de su despacho sin que todos estas conductas que tienen un claro efecto de atenuación en el reproche sancionatorio hayan sido tenidos en cuenta a la hora de imponer una sanción que es tan gravemente onerosa para nuestra entidad.

B) LA SANCIÓN ECONÓMICA RESULTA DESPROPORCIONADA EN CONTRASTE CON LA RESPONSABILIDAD DE BANSERFIN S.A.S., SU TAMAÑO Y ROL COMO ENCARGADO

En armonía con lo señalado en el numeral anterior, no se entiende como una MINIPYME del tamaño de Banserfin S.A.S. en su condición de encargado de la información obtenga una sanción pecuniaria de idéntica cuantía respecto al cargo primero del "Fondo de Empleados Granfondo" cuyo tamaño, rol de responsable y conductas previas concomitantes y posteriores a este proceso distan de las nuestras. Lo cierto es que la magnitud la presunta vulneración que acaeció y dio lugar al proceso que nos ocupa, así como el obrar de buena fe y estricta sujeción por parte de Banserfin S.A.S. a los lineamientos legales y disposiciones administrativas de la SIC no deberían tener una consecuencia económica tan alta, máxime cuando de quedar dicha decisión en firme el grado de afectación económica a una MINIPYME de nuestro tamaño y en época de Coronavirus podría potencialmente poner en riesgo la existencia de la empresa y de los puestos de trabajo que de ella se derivan, por un error humano involuntario, debidamente informado, subsanado, reconocido y mitigado.

Queremos informar que como consecuencia de la implementación de la emergencia sanitaria, nuestra empresa fue afectada sensiblemente en sus ingresos de operación desde el mes de marzo de 2020, pero en un esfuerzo sin precedentes, decidimos apoyar a nuestro personal y por ello, debido al deterioro de nuestra situación económica hemos sido beneficiarios del programa PAEF del Gobierno Nacional, lo cual evidencia la transparencia y esfuerzo de nuestra empresa para mantener los puestos de trabajo de nuestros colaboradores, solo buscando contribuir en algo, a la lesión tan enorme a toda la fuerza laboral del País.

C) NO HUBO UN PERJUICIO FORMAL NI MATERIAL A LOS DATOS PERSONALES O DERECHOS DEL QUEJOSO

Como se puede evidenciar claramente del trasegar factico y probatorio del caso objeto de sanción, de la conducta desplegada por la funcionaria de nuestra entidad que remitió por error un correo masivo con la invitación general y abstracta de estar al corriente de obligaciones económicas, nunca hubo una vulneración formal ni material efectiva a los datos del quejoso ni de ninguna persona en particular, no se pusieron en riesgo ningún tipo de dato financiero o personal por el simple hecho que jamás fueron revelados, se reconoció de forma inmediata y expedita el error subsanándolo, se sancionó a la funcionaria y se reforzaron todos los procesos, políticas, controles, manuales y formatos que aportamos en el proceso de calificación de la falta, con el fin univoco de cumplir con nuestros deberes legales y proscribir la posibilidad de que una situación por pequeña que sea como la que ocurrió se volviera a repetir.

En conclusión y más allá de asumir nuestra responsabilidad, la consecuencia sancionatoria impuesta desborda a nuestro humilde juicio el hecho sancionable que, a nuestro entender, con un requerimiento y seguimiento por parte de la S.I.C. y su delegatura al cumplimiento de nuestros deberes como encargados hubiese sido suficiente y logrado el cometido de cumplimiento a los preceptos de protección de datos personales, lo que aunado los inexistentes daños y perjuicios generados a persona alguna daría lugar para que la sanción económica sea reducida o disminuida en un porcentaje significativo.

D) BANSERFIN S.A.S. RECONOCIÓ SU RESPONSABILIDAD Y SE ALLANÓ A LOS REQUERIMIENTOS DE LA SIC

Desde el momento mismo en que se surtió por parte de la delegatura la investigación preliminar del caso nos fue citada por parte de la S.I.C. una serie de normas y fundamentos que señalaban que la potencial sanción a la que nos veríamos expuestos se mitigaría conforme a la conducta de colaboración, información y asunción de nuestra responsabilidad, pero aun independientemente de este hecho el obrar de Banserfin S.A.S. a lo largo de todo el proceso, ha sido de buena fe, de la más absoluta colaboración y sujeción a los requerimientos del ente investigador y sancionador (en contraste con el Fondo de Empleados Granfondo, quien básicamente recibió la misma sanción teniendo un tamaño , rol y responsabilidad aun mayor), razón por la que acudimos a estos antecedentes objetivos, reglado y documentados para que se valore la revocatoria de la sanción económica o la disminución de su cuantía en un porcentaje importante y que se adecue de una forma mas razonable a nuestra situación y conductas atenuantes.

E) CONDUCTA MARGINAL, INVOLUNTARIA PRODUCTO DE UN ERROR HUMANO EN EL CASO QUE NOS OCUPA.

Salvo la situación objeto de la sanción que nos convoca, nunca se ha presentado en Banserfin S.A.S. una queja, incumplimiento, reclamo o desconocimiento de ninguna naturaleza a los deberes que le atañen como encargado de datos personales, esta situación de envió involuntario por parte de una de nuestra funcionaria de un correo electrónico con información general y abstracta que no alude a datos personales o financieros de ningún tipo es completamente marginal y no obedece a un proceder sistemático o grave de incumplimiento a nuestros deberes, razón por la que consideramos que estos antecedentes, la ausencia de reincidencia, de daños , perjuicios o de desconocimiento alguno de nuestros deberes deberían ser razones más que suficientes para revocar la sanción económica o disminuirla de forma ostensible.

2. Por su parte la apoderada especial de **FONDO FEG** sustento el recurso manifestando lo que sigue a continuación:

A. VIOLACIÓN DEL PRINCIPIO DE LEGALIDAD EN MATERIA SANCIONATORIA ADMINISTRATIVA.

La sanción impuesta a mi poderdante por parte de la Superintendencia de Industria y Comercio, por la presunta violación del literal i) del artículo 17 de la Ley 1581 de 2012, se deriva de una interpretación que en concepto de la entidad es armónica con los principios establecidos por la normatividad aplicable al caso, entre ellos los principios de acceso y circulación restringida y el principio de seguridad; sin embargo, al justificar la sanción impuesta con la existencia de los principios mencionados, y no con base en una exigencia de conducta concreta de la norma, configura una flagrante violación a los principios de legalidad y tipicidad en materia sancionatoria administrativa.

Al respecto, debemos remitirnos al tenor literal de la norma por la cual se imputa el cargo primero en el presente proceso administrativo sancionatorio, es decir, el literal i) de la Ley 1581 de 2012, que establece como obligación para el responsable del tratamiento de datos:

> *Artículo 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *(…)*
>
> *i) **Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.***

*Así, la norma en que la Autoridad de Protección de Datos fundamenta su sanción menciona la obligación de **exigir al encargado** del tratamiento en todo momento el respeto y privacidad de la información del titular. Sin embargo, tal exigencia no se limita a un estándar o una actividad específica para su cumplimiento, pudiéndose cumplir contractual o extracontractualmente, de diferentes maneras.*

*Cabe resaltar que mi poderdante realizó una revisión de la experiencia de **BANCA DE SERVICIOS FINANCIEROS S.A.S.** para seleccionarla como la empresa que colaboraría con los servicios de cobranza de las obligaciones que los asociados al Fondo de Empleados, al acreditar entre otras cosas, su trayectoria y experiencia, tratándose de una entidad especializada en este tipo de servicios y constituida desde febrero de 2006, tal y como consta en el registro mercantil.*

Ahora bien, mi poderdante aportó pruebas tendientes a demostrar que la exigencia mencionada por la norma, se consagró contractualmente exigiendo a su contratista la estricta confidencialidad y las condiciones de seguridad de la información que mi poderdante le entregara en calidad de encargado. La obligación mencionada era de tracto sucesivo y no de ejecución instantánea, es decir, esa obligación sería exigible en todo momento durante la vigencia del contrato so pena de un incumplimiento contractual.

*Acorde con la importancia que tenía para FEG la obligación en materia de confidencialidad y seguridad de la información, la decisión inmediata, oportuna y radical ante el impase: la terminación del contrato con la sociedad **BANCA DE SERVICIOS FINANCIEROS S.A.S.** Lo anterior evidencia, nuevamente, la exigencia al encargado de la información.*

*Al respecto, el verbo "exigir" es definido por parte de la Real Academia de la Lengua Española como "Pedir imperiosamente algo a lo que se tiene derecho", acción que fue efectuada por parte de mi poderdante, a través del establecimiento de obligaciones en materia de confidencialidad y seguridad de la información en cabeza **BANCA DE SERVICIOS FINANCIEROS S.A.S.**, que no solo se perfeccionaba con la simple estipulación de la obligación, sino que también amenazaba con acciones legales a mi poderdante para la terminación unilateral del contrato y la reclamación de perjuicios.*

Teniendo en cuenta que la norma establece la obligación de "Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular", no es posible predicar de esta conducta que sea un tipo en blanco, o que permita su remisión a otra norma para poder concluir el incumplimiento de esta obligación, y por ende, la norma no establece un estándar de exigencia para cumplir, simplemente se debe exigir al encargado del tratamiento por cualquier medio el cumplimiento de las medidas de seguridad y confidencialidad de la información, y el medio que consideró mi poderdante fue la estipulación contractual de obligaciones en materia de protección de datos en los términos del hecho tercero, así como la imposición de las consecuencias ante su incumplimiento.

Con base en lo anterior, resulta cuestionable la tarifa legal impuesta por la autoridad cuando reprocha y justifica la sanción en lo siguiente:

"Por lo anterior, la sociedad FONDO DE EMPLEADOS GRANFONDO - FEG", en calidad de Responsable, debió aportar a la investigación los informes de auditoria realizadas a la sociedad BANCA DE SERVICIOS FINANCIEROS S.A.S., encargada del tratamiento de datos personales, respecto "del servicio ofrecido y en especial a la seguridad de los procesos relacionados con los servicios prestados".

Lo anterior porque de la norma que establece la obligación para mi poderdante de exigir en todo momento el cumplimiento de las condiciones de seguridad de la información no se establece la obligación explícita de

realizar auditorias, sino que resulta una interpretación extensiva de la norma por parte del funcionario que impone la sanción, aspecto violatorio del principio de legalidad.

(…)

Con base en lo anterior, la sanción impuesta por parte de la Superintendencia de Industria y Comercio carece de dos elementos relevantes desarrollados por el Tribunal Constitucional, a saber:

i) Permitir que el concepto de "exigir" inmerso en el literal i) de la Ley 1581 de 2012 pueda interpretarse de manera amplia y subjetiva por parte del funcionario administrativo que impone la sanción, implica que la norma "deja abierto el campo para la arbitrariedad de la administración en la imposición de las sanciones o las penas", teniendo en cuenta que la norma establece de manera general la obligación de exigir, y no un concepto de exigir como sinónimo de auditar.

ii) La interpretación por parte del funcionario que aplica la sanción implica la violación del primer requisito para el cumplimiento del principio de legalidad en el ámbito del derecho administrativo sancionador, es decir, "los elementos básicos de la conducta típica que será sancionada", toda vez que la norma establece la obligación de exigir al encargado el cumplimiento de las condiciones confidencialidad y seguridad en la información, mas no las acciones concretas a través de las cuales se debe exigir dicho cumplimiento, siendo este un aspecto interpretativo y subjetivo que configura la violación al principio de legalidad y tipicidad de la sanción administrativa.

Con base en las anteriores consideraciones, se solicita se revoque la sanción impuesta a mi apoderada, toda vez que se encuentra demostrado que mi apoderada cumplió con la obligación de exigir a través del contrato de prestación de servicios de cobranza el cumplimiento de las condiciones de seguridad y confidencialidad de la información, obligaciones de tracto sucesivo a través de la vigencia del contrato. Tal estipulación contractual fue, en estricto sentido, una de las múltiples maneras existentes para exigir el cumplimiento de una obligación, que difiere con el concepto de exigencia como sinónimo de auditoría que la Superintendencia de Industria y Comercio impone en el acto impugnado.

B. INDEBIDA VALORACIÓN PROBATORIA EN RELACIÓN CON LA DOCUMENTACIÓN APORTADA

Dentro de los fundamentos utilizados por parte de la administración en materia de protección de datos, se menciona que los formatos aportados "están sin diligenciar, con esto se evidencia una conducta negligente de la sociedad FONDO DE EMPLEADOS GRANFONDO – FEG, al aportar preformas generales para desvirtuar el cargo formulado. Por lo tanto, al no acreditar los documentos que suscribió con la sociedad BANCA DE SERVICIOS FINANCIEROS S.A.S. se evidencia el incumplimiento de su deber de "Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular"".

Dicha aseveración le atribuye efectos totalmente contrarios a los que se pretendían acreditar a través de la documentación aportada, toda vez que al allegar los documentos que a continuación se refieren, lo que se pretendía era demostrar la implementación de todo un Plan de Gestión de Datos Personales al interior del Fondo, demostrando interés y compromiso con el cumplimiento de las prerrogativas exigidas en la Ley 1581 de 2012 y las normas que la desarrollan.

Los documentos que se aportaron en la respuesta al pliego de cargos fueron los siguientes:

- *Formato de Asociación: Por medio del cual se pretenden demostrar las condiciones en las cuales los asociados autorizan el tratamiento de datos personales.*
- *Manual de Políticas y Procedimientos de Tratamiento de Datos: Por medio del cual se pretenden demostrar las condiciones generales, las finalidades, los canales de atención a los titulares de los datos personales, derechos de los titulares, nuestras medidas de seguridad para la protección de la información de nuestros titulares, entre otros.*
- *Oferta Mercantil de Compra de Servicios de Gestión de Cobranza y Otros Servicios que Fondo FEG le encargue: Por medio del cual se pretende demostrar las condiciones contractuales que regulen el acuerdo entre FEG y BANCA DE SERVICIOS FINANCIEROS S.A.S. entre las cuales se estipula la obligación de mantener las condiciones de confidencialidad y seguridad de la información encargada, las consecuencias jurídicas de su incumplimiento, y por ende, el cumplimiento del literal i) del artículo 17 de la Ley 1581 de 2012.*
- *Orden de Venta de Servicios de Gestión de Cobranza y Otros Servicios: Por medio de la cual se evidencia la aceptación por parte de BANCA DE SERVICIOS FINANCIEROS S.A.S. de la oferta mercantil anteriormente reseñada y por ende, el perfeccionamiento de un contrato de tracto sucesivo, con obligaciones exigibles a lo largo de la vigencia del contrato.*
- *Formato de Contrato de Transmisión de Datos Proveedores: Por medio del cual se evidencian las actuales condiciones contractuales por medio de la cual transmitimos información con nuestros aliados en calidad de encargados del tratamiento de la información, en ningún momento pretende ser soporte de las relaciones comerciales en materia de protección de datos entre FEG y BANCA DE SERVICIOS FINANCIEROS S.A.S., relación que se encuentra mediada únicamente por la oferta mercantil y la orden de venta mencionadas anteriormente.*
- *Acuerdo de Confidencialidad y deber de secreto: Por medio del cual se pretende demostrar nuestras actuales condiciones para trabajadores, asociados y cualquier vinculado que tenga acceso a la información de nuestros titulares en relación con la protección de la seguridad y confidencialidad de la información.*
- *Terminación de Contrato: Pretende demostrar la aplicación de las consecuencias jurídicas establecidas en el contrato con base en el incumplimiento del contrato derivado de la denuncia que dio inicio a la presente investigación administrativa.*

Como se puede evidenciar, la finalidad de los documentos que la entidad sancionadora menciona como muestras de negligencia, era la de demostrar el estado actual de la documentación e implementación de todo un Plan de Gestión de Datos Personales, en los términos de la política de tratamiento que sobre el mismo tema tiene la entidad. Sin embargo, sorpresivo resultó el análisis de un formato cuyo reproche fue la falta de diligenciamiento, asunto apenas lógico si se trataba de un ejemplo y cuya prueba era relevante por los campos y lo que significaba la documentación misma, no por los datos de alguno de los asociados que pudiese estar en el formato ejemplificado.

Al respecto, encontramos la vulneración de las siguientes garantías procesales:

***La presunción de inocencia**, toda vez que a pesar de que mi poderdante allegó las pruebas para demostrar que exigió a su contraparte contractual el mantenimiento de las condiciones de seguridad y confidencialidad de la información a través del contrato, la Superintendencia asume que mi poderdante nunca tuvo comunicaciones o reuniones con **BANCA DE SERVICIOS FINANCIEROS S.A.S.** , cuando la realidad es que dichas reuniones para la evaluación del cumplimiento del contrato (incluyendo la normatividad en materia de protección de datos) sí tuvieron lugar en múltiples momentos, pero no se evidencia intención alguna por parte de la Superintendencia de Industria y Comercio de ahondar en este tipo de información, invirtiendo la carga probatoria, aspecto violatorio de la presunción de inocencia.*

***Solicitar, aportar y controvertir pruebas,** garantía que se ve afectada cuando la Superintendencia de Industria y Comercio exige una tarifa legal probatoria para demostrar la exigencia por parte de mi poderdante a **BANCA DE SERVICIOS FINANCIEROS S.A.S.** del cumplimiento de las condiciones de seguridad y confidencialidad en la información, tarifa legal que en ningún caso se encuentra regulada en la normatividad aplicable, es decir, no existe norma alguna que obligue a demostrar el cumplimiento de la obligación contenida en el literal i) del artículo 17 de la Ley 1581 de 2012 a través de actas de auditoría específicamente, aspecto que pareciera exigir la entidad sancionadora cuando menciona: "Por lo anterior, la sociedad FONDO DE EMPLEADOS GRANFONDO – FEG en calidad de responsable, debió aportar a la investigación los informes de auditoría realizadas a la sociedad BANCA DE SERVICIOS FINANCIEROS S.A.S., encargada del tratamiento de datos personales (…)".*

C. VIOLACIÓN AL PRINCIPIO DE PROPORCIONALIDAD EN LA TASACIÓN DE LA PENALIDAD.

Sin perjuicio de la inocencia de mi poderdante, en la sanción impuesta por parte de la Autoridad de Protección de datos se evidencia una violación al principio de proporcionalidad en la tasación de la sanción, teniendo en cuenta que:

- *BANCA DE SERVICIOS FINANCIEROS S.A.S. fue la sociedad que envió el correo electrónico censurado por la SIC, por ende, es la persona jurídica implicada directamente en la violación de las normas de protección de datos personales.*

- *Si bien mi poderdante, un fondo de empleados perteneciente al sector solidario y cuyas sanciones pecuniarias se pagan con el dinero de todos los asociados, tuvo una participación limitada a la contratación de BANCA DE SERVICIOS FINANCIEROS S.A.S., que si bien puede y está adoptando acciones de mejora continua bajo el principio de responsabilidad demostrada, incluyendo el previo nombramiento de un oficial de protección de datos encargado de todos estos procesos de mejora, no resulta ajustado al principio de justicia y equidad, que le sea impuesta la misma sanción que a la persona que directamente permitió la violación de la seguridad de la información.*

Para reconocer concretamente el contenido de la violación al principio de proporcionalidad, debemos reconocerlo como concepto que busca la prohibición de todo sactificio (sic) innecesario o desproporcionado. Lo que se pone de manifiesto fundamentalmente en "el principio de prohibición de exceso".[3][5]

En la presente actuación administrativa, la Corte Constitucional ha desarrollado un test para determinar si una actividad de la administración respeta el postulado de proporcionalidad, a través de la Sentencia C-673 de 2001[4][6], por medio de la cual establece como requisitos:

El análisis del fin buscado por la medida, que implica la legitimidad del objetivo que motiva la restricción.
El estudio del medio empleado. Lo que significa la adopción de una medida que produzca un menor sacrificio para otros valores, principios y derechos que tengan un mayor valor constitucional que aquéllos que se pretenden satisfacer a través de su desarrollo, es obligación de las autoridades administrativas preferirla, conforme

lo ordena categóricamente el contenido normativo del citado principio de proporcionalidad.
El examen de la relación entre el medio y el fin. Lo que se traduce en la ponderación entre el principio que se protege y el que se sacrifica y la debida correspondencia entre la falta y la sanción.

Con relación a lo anterior, se debe tener en cuenta que las empresas están en un continuo mejoramiento en virtud del principio de responsabilidad demostrada (accountability), y que lejos de inferir negligencia de mi poderdante en cuanto a la protección de datos personales, lo que se evidencia es la existencia de un Oficial de Protección de Datos Personales, encargado de verificar y continuar con la ejecución del Plan de Gestión de Datos Personales evidenciado a través de nuestra Política de Tratamiento de Datos Personales,

---

[3] [5] Schmidt-Assmann, Eberhard. La teoria del derecho administrativo como sistema. Objeto y fundamentos de la construcción sistemática. Marcial pons, Madrid, 2009 p. 89.
[4] [6] Corte Constitucional de Colombia, Sala Plena. (10 de febrero de 2016) Sentencia C 673 DE 2011. [Mp. Manuel José Cepeda Espinosa

(…)

(…) la administración en materia de protección de datos asevera que "aunque los 265 titulares hubiesen otorgado dicha autorización, del análisis de su contenido, no está ni podría estarlo, la divulgación masiva y descontrolada de los datos personales de los ciudadanos, como en este caso, el correo electrónico", cuando en realidad, resulta probado en el expediente que: i) fue una falla excepcional en la seguridad del encargado del tratamiento, inexistente en años de relación contractual con FEG; ii) aún así el encargado adoptó las medidas tendientes a capacitar a su personal y evitar que se vuelva a presentar un problema de seguridad en su información; iii) debido a la desconfianza que generó dicha vulneración en la seguridad de la información, mi poderdante finalizó el contrato con ***BANCA DE SERVICIOS FINANCIEROS S.A.S.*** *por incumplimiento de las obligaciones del contrato de servicios de cobranza y (iv) el contenido del correo no ponía en evidencia un estado específico de sus destinatarios, mucho menos algo que atentara contra su honra o dignidad, o información sensible, tratándose más bien de una nota informativa dirigida a destinatarios unidos por el vínculo de asociados.*

Teniendo en cuenta que: i) no se tiene evidencia de anteriores actuaciones administrativas por parte de la Superintendencia de Industria y Comercio en contra de mi poderdante que permitan inferir la reiteración de conductas violatorias del Régimen de Protección de Datos Personales; ii) mi representada cuenta con la implementación de todo un sistema de protección de datos personales; iii) la conducta reprochable implica una menor participación en la vulneración a las condiciones de seguridad y confidencialidad de la información, ***esta representación considera que la sanción es desproporcionada.***

Con base en los argumentos anteriormente relacionados, se concluye lo siguiente:

- *Se encuentra demostrado que mi apoderada cumplió con la obligación de exigir a través del contrato de prestación de servicios de cobranza el cumplimiento de las condiciones de seguridad y confidencialidad de la información, por medio de las obligaciones de tracto sucesivo durante de la vigencia del contrato.*

- *A nivel probatorio, existe violación de las siguientes garantías procesales:*

  I. La presunción de inocencia, al presumir la culpabilidad de mi poderdante sin otorgarle el valor probatorio a las pruebas que se allegaron en relación con el cumplimiento de la obligación de exigir el cumplimiento de las condiciones de seguridad y confidencialidad de la información encargada.

  II. La posibilidad de solicitar, aportar y controvertir pruebas, al suprimirle valor probatorio a cualquier prueba aportada por mi poderdante que no fuera una auditoría, exigiendo una tarifa legal inexistente en la legislación en materia de protección de datos, y basando su sanción en principios y no en conductas tipificadas concretamente, y violando el principio de libertad probatoria.

- *La imposición de una sanción en contra de mi poderdante a través del presente proceso es violatoria del principio de proporcionalidad en las actuaciones administrativas sancionatorias, toda vez que los hechos que se investigan no ponen en riesgo los bienes jurídicos tutelados por parte del marco regulatorio de protección de datos personales, toda vez que mi representada cuenta con un Sistema de Gestión de Protección de Datos Personales encabezado por un Oficial de Protección de Datos Personales que se encarga de verificar el cumplimiento de las medidas establecidas en su Política de Tratamiento de Datos Personales.*

- *La imposición de una sanción en contra de mi poderdante a través del presente proceso es violatoria del principio de proporcionalidad toda vez que contrario a lo que afirma la administración, en cuanto a la existencia de fallas en la seguridad descontroladas, lo cierto es que mi poderdante adoptó todas las medidas tendientes a evitar que en el futuro se presente una situación similar, tanto con nuestros empleados, asociados y vinculados, como con nuestros aliados en calidad de encargados de la información de la cual somos responsables.*

- *Es violatorio del principio de proporcionalidad el hecho de que la sanción impuesta a mi representada sea superior a la sanción impuesta a la entidad BANCA DE SERVICIOS FINANCIEROS S.A.S. que en calidad de encargada del tratamiento de la información para los servicios de cobranza obró con culpa al permitir la divulgación de 265 cuentas de correo electrónico, aspecto que no se encontraba en la esfera de voluntad de FONDO DE EMPLEADOS GRANFONDO – FEG.*

Séptimo. Que mediante Resolución 16847 de 26 de marzo de 2021, el Director de Investigación de Protección de Datos Personales resolvió los recursos de reposición interpuestos por **BANSERFIN** y **FONDO FEG**, confirmando la Resolución 78239 de 4 de diciembre de 2020, y concediendo el recurso de apelación.

Octavo. Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho procede a resolver el recurso de apelación interpuesto contra la Resolución 78239 de 4 de diciembre de 2020, de conformidad 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 [5] 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.

De conformidad con lo establecido en el literal g) del artículo 4 de la Ley 1581 de 2012, *"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"*;

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

Sin seguridad no existe debido tratamiento de datos personales. La relevancia y alcance del deber de seguridad ha sido puesto de presente en los siguientes términos:

> *"La seguridad es un proceso dinámico en constante evolución y prueba. Se quiere que exista un nivel de seguridad apropiado en las diferentes etapas del tratamiento de datos personales en donde las medidas de seguridad sean objeto de evaluación y revisión.*
>
> *Dichas medidas deben estar enfocadas para mitigar los siguientes riesgos: acceso no autorizado a los datos personales, pérdida, destrucción (accidental o no autorizada), contaminación (por virus informático) uso fraudulento, consulta, copia, modificación, adulteración, revelación, comunicación, o difusión no autorizados.*
>
> *Para establecer las medidas se deben tener en cuenta, entre otras, las técnicas de seguridad existentes en general y para sectores específicos, los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse, la probabilidad y severidad del daño obtenido, la sensibilidad de la información y el contexto en el que es realizado el tratamiento y las eventuales consecuencias negativas para los titulares de los datos.* (…)
>
> *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 de los datos. El acceso, la consulta y el uso no autorizado o fraudulento así como la manipulación y pérdida de la información son los principales riesgos naturales y humanos que se quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa o técnica."* [6]

---

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

[6] Cfr. REMOLINA ANGARITA, Nelson. 2013. Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012. 1 ed. Bogotá: Legis Editores. Págs. 216-217

Concordante con lo anterior, el principio de circulación restringida establece que el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los Datos personales, de las disposiciones de la presente ley y la Constitución Política Nacional. En este sentido, el Tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley.

En el presente caso, **BANSERFIN**, en su calidad de Encargado del Tratamiento de información a nombre del Responsable **FONDO FEG**, de conformidad con lo establecido en el artículo 18 literal b) de la Ley 1581 de 2012 tiene el deber de *"conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".*

De acuerdo con la denuncia interpuesta y las pruebas que fueran allegadas a la presente actuación administrativa, quedó demostrado que se envió el mismo mensaje a 265 cuentas de correo electrónico exponiendo Datos personales a cada uno de los usuarios que recibieron la citada comunicación. **BANSERFIN** tenía el deber de adoptar las medidas técnicas, humanas y administrativas que evitaran su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los Datos personales que se encontraba manejando en calidad de Encargado, en este sentido debió implementar los respectivo controles que hubiesen impedido la ocurrencia de la conducta que se investiga.

De las pruebas aportadas a la presente actuación, encuentra este Despacho que las medidas sobre seguridad adoptadas por parte de **BANSERFIN** solo tuvieron lugar una vez se puso en conocimiento el inicio de la presente actuación administrativa, por lo que, no son de recibo las exculpaciones presentadas dentro del recurso de apelación.

Por otra parte, los Responsables del Tratamiento de Datos personales, de conformidad con lo establecido en el literal i) del artículo 17 de la Ley 1581 de 2012 **deben exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular**.

Respecto del citado deber, la apoderada de **FONDO FEG** (quien actúa en calidad de Responsable en la presente actuación), indicó que *"tal exigencia no se limita a un estándar o una actividad específica para su cumplimiento, pudiéndose cumplir contractual o extracontractualmente, de diferentes maneras"*

Señaló además que *"mi poderdante aportó pruebas tendientes a demostrar que la exigencia mencionada por la norma, se consagró contractualmente exigiendo a su contratista la estricta confidencialidad y las condiciones de seguridad de la información que mi poderdante le entregara en calidad de encargado. La obligación mencionada era de tracto sucesivo y no de ejecución instantánea, es decir, esa obligación sería exigible en todo momento durante la vigencia del contrato so pena de un incumplimiento contractual".*

Efectivamente, este Despacho pudo establecer que a través de la orden de servicios suscrita entre **FONDO FEG** y **BANSERVIR**, se estableció como obligación contractual la de ***"[d]ar tratamiento*** [sic] ***de confidencialidad a toda la información a la que tenga acceso con ocasión de los servicios prestados; no divulgar, emitir, publicar o comunicar directa o indirectamente a terceros la información que con ocasión de la prestación de los servicios llegare a conocer".***

- **OBLIGACIONES A CARGO DE EL DESTINATARIO**

En caso de ser aceptada la presente Oferta Mercantil mediante la expedición de la correspondiente orden de venta de servicios, EL DESTINATARIO se obliga especialmente para con FONDO FEG a lo siguiente:

- Cumplir con las recomendaciones e instrucciones que le imparta FONDO FEG, con relación a los servicios objeto de la presente Oferta Mercantil.
- Desarrollar de manera diligente, oportuna y a entera satisfacción de FONDO FEG el objeto de la presente Oferta Mercantil.
- Dar tratamiento de confidencialidad a toda la información a la que tenga acceso con ocasión de los servicios prestados; no divulgar, emitir, publicar o comunicar directa o indirectamente a terceros la información que con ocasión de la prestación de los servicios llegare a conocer.
- Permitir a FONDO FEG la realización de auditorías de calidad, en el momento que así sea solicitado.
- Informar oportunamente a FONDO FEG cualquier circunstancia de orden legal, fuerza mayor o caso fortuito, que le impida cumplir con la prestación oportuna del servicio.
- Abstenerse de utilizar sin previa autorización de FONDO FEG, el nombre o marcas propiedad de FONDO FEG.
- Prestar los servicios requeridos por FONDO FEG, en las condiciones y horarios definidos por éste.
- Garantizar la preparación, experiencia e idoneidad del personal que participa en la prestación del servicio; capacitando a su personal para asegurar un alto nivel de desempeño y efectividad.
- Asumir los costos de ajuste, instalación y operación necesarios para el cumplimiento de la prestación de los servicios objeto de la presente oferta mercantil.
- Proveer un grupo de personal técnico de soporte y monitoreo para garantizar la correcta ejecución de los servicios que preste EL DESTINATARIO en virtud de la presente oferta mercantil, en los términos y condiciones definidos por FONDO FEG.
- Realizar y entregar a FONDO FEG, los reportes y/o informes que se soliciten en cualquier momento durante la prestación de los servicios. Estos informes se pedirán de acuerdo con las necesidades de información de FONDO FEG y no representarán costo adicional a cargo de FONDO FEG.
- Tener disponible un Coordinador o Gerente de Cuenta en cualquier momento a través de Teléfono Celular, quien responderá las llamadas a más tardar en treinta (30) minutos.

Igualmente, en el mismo contrato se estipuló que **FONDO FEG** podría en cualquier tiempo, *"realizar visitas a las instalaciones de EL DESTINATARIO para efectuar evaluaciones del servicio ofrecido y en especial a la seguridad de los procesos relacionados con los servicios prestados por EL DESTINATARIO".*

17. SEGUIMIENTO Y AUDITORIA

En caso de ser aceptada la presente oferta mercantil, mediante la expedición de la correspondiente orden de venta de servicios por parte de EL DESTINATARIO, FONDO FEG o el tercero designado por éste, podrán en cualquier tiempo, realizar visitas a las instalaciones de EL DESTINATARIO para efectuar evaluaciones del servicio ofrecido y en especial a la seguridad de los procesos relacionados con los servicios prestados por EL DESTINATARIO.

Las revisiones de los Auditores autorizados por FONDO FEG podrán efectuarse en las oficinas de EL DESTINATARIO y/o en el sitio en que se preste el servicio. La auditoria podrá estar acompañada por un funcionario de EL DESTINATARIO, quien le prestará su mayor colaboración para realizar la labor encomendada. En caso de no requerirse la visita, FONDO FEG podrá solicitar por escrito la información requerida para su evaluación, siempre que esté relacionada con el servicio ofrecido.

Estarán a disposición de FONDO FEG, los controles y formas que utiliza EL DESTINATARIO para registrar ordinariamente sus operaciones.

EL DESTINATARIO atenderá oportunamente las observaciones, requerimientos de control y reclamos justificados que hiciere FONDO FEG como resultado de tales revisiones. Si EL DESTINATARIO rehúsa facilitar el acceso a los auditores de FONDO FEG, o rehúsa atender reclamos razonables, cualquier suma en discusión no será reconocida si se debiere a la falencia observada, sin perjuicio de las demás consecuencias derivadas de la presente oferta mercantil.

Evidentemente, dentro del contrato suscrito entre **BANSERFIN** y **FONDO FEG** se establecieron cláusulas relacionadas con la protección de la información, sin embargo, no resultan ser del todo suficientes para cumplir con el mandato constitucional.

Respecto de los deberes relacionados con la seguridad del Dato, la Corte Constitucional[7], manifestó:

> ***"(iii)*** *Adoptar las medidas para garantizar* ***la seguridad del dato****, a efectos de que no se pierda, no se adultere, no se utilice o acceda por fuera de la autorización, lo cual es desarrollado en el literal d) en concordancia con el principio de seguridad en la transferencia del dato. Por tanto,* ***el responsable está obligado a exigir*** *y* ***controlar las condiciones de seguridad que está empleando el encargado del tratamiento*** *-literal a), como informar oportunamente a la autoridad encargada de la protección del dato sobre violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los*

[7] Sentencia C – 748 del 6 de octubre de 2011

titulares- literal n); siendo estos deberes, sin lugar a dudas, también desarrollo del principio de seguridad jurídica".

En línea con lo anterior, la misma corporación indicó:

"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."[8] *(Destacamos).*

La protección de Datos personales no puede entenderse satisfecha con la estipulación de cláusulas contractuales, el principio de seguridad no finaliza ahí, debe existir una constante evaluación de los riesgos que puedan presentarse con el Tratamiento de los Datos personales por parte del Encargado, en este caso, **BANSERFIN**. Así las cosas, el no haber allegado una prueba que indicara que **FONDO FEG** en su calidad de Responsable, realizó las acciones pertinentes que hubieran permitido contrarrestar cualquier tipo de situación que aumentara el riesgo de infracción al régimen de protección de Satos personales, vulnera el deber exigido en el literal i) del artículo 17 de la Ley 1581 de 2012.

Por otra parte, la apoderada de **FONDO FEG**, respecto a la valoración probatoria indicó que, *"la finalidad de los documentos que la entidad sancionadora menciona como muestras de negligencia, era la de* ***demostrar el estado actual de la documentación e implementación de todo un Plan de Gestión de Datos Personales, en los términos de la política de tratamiento que sobre el mismo tema tiene la entidad****. Sin embargo, sorpresivo resultó el análisis de un formato cuyo reproche fue la falta de diligenciamiento, asunto apenas lógico si se trataba de un ejemplo y cuya prueba era relevante por los campos y lo que significaba la documentación misma, no por los datos de alguno de los asociados que pudiese estar en el formato ejemplificado".*

Consideró entonces que, con el proceder de la primera instancia, fueron vulnerados en primer lugar su presunción de inocencia y en segundo lugar la garantía de solicitar, aportar y controvertir pruebas, en la medida que se exige una tarifa legal probatoria para demostrar la exigencia por parte de **FONDO FEG** hacía **BANSERFIN** respecto del cumplimiento de las condiciones de seguridad y confidencialidad en la información, tarifa legal que en ningún caso se encuentra regulada en la normatividad aplicable.

Pues bien, en lo que tiene que ver con la presunción de inocencia, resulta necesario aclarar que, dada su naturaleza de presunción legal, es deber de quien considera se ha faltado a esta, probar el hecho que, en su concepto, constituye mala fe.

Así las cosas, sí **FONDO FEG** actuó o no bajo el principio de la buena fe, no es, ni ha sido punto de discusión, u objeto de investigación en la presente actuación, sencillamente porque lo que se investiga es el incumplimiento a los deberes que como Responsable del Tratamiento de información está llamado a cumplir. Aunado a lo anterior, el hecho que haya actuado de buena fe no puede tomarse como un eximente de su responsabilidad, y que, en consecuencia, no esté llamado legalmente a responder. No basta obrar de buena fe sino que se debe ser diligente y profesional en todas las actividades, especialmente aquellas que involucren derechos humanos.

Como es sabido, la regulación de la República de Colombia no solo ordena a quien trate Datos personales a implementar las *"medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*"[9] y a "*conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"* [10]. Sino que les exige "*(…) ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012"*[11]*.*

[8] Ibidem
[9] Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012
[10] Cfr. Literal d) del artículo 17 de la Ley Estatutaria 1581 de 2012
[11] Cfr. Artículo 26 del decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015)

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

> "*219. El principio de responsabilidad demostrada, conocido en el derecho comparado como accountability en la protección de datos personales, es incorporado por la legislación interna por el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2013 (sic). El artículo 26 de esa normativa determina que los responsables del tratamiento de datos personales deberán demostrar, a petición de la Superintendencia de Industria y Comercio, entidad que obra como autoridad colombiana de protección de datos, que han implementado medidas apropiadas y efectivas para cumplir con las citadas normas jurídicas. Esto de manera proporcional a: (i) la naturaleza jurídica del responsable y, cuando sea el caso, su tamaño empresarial; (ii) la naturaleza de los datos personales objeto de tratamiento; (iii) el tipo de tratamiento; y (iv) los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares del dato personal. Con este fin, los responsables deben informar a la SIC acerca de los procedimientos usados para el tratamiento de datos. A esta medida se suma lo previsto en el artículo 27 ejusdem, que estipula la obligación del responsable de establecer políticas internas que garanticen: (i) la existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable; (ii) la adopción de mecanismos internos para poner en práctica dichas políticas; y (iii) la previsión de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, respecto de cualquier aspecto del tratamiento de datos personales.*
>
> ***El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de demostrar ante la autoridad de datos*** *que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal*."[12] (Destacamos)

Así las cosas, la recurrente tiene el deber de demostrar que adoptó medidas de seguridad apropias, útiles y eficientes.

En esa medida, lo que fue objeto de investigación durante la presente actuación fue la conducta desplegada por la sociedad recurrente, la cual se considera reprochable a la luz del deber que le correspondía cumplir.

Ahora, como se dijo en líneas anteriores, exigir al Encargado **en todo momento** el cumplimiento de las condiciones de seguridad y privacidad de la información del Titular, no se trata solo de establecer cláusulas contractuales, el Responsable debe ser dinámico y conducir las acciones necesarias para el cumplimiento del citado deber, circunstancias que pueden ser demostradas a través de cualquier medio probatorio.

Razones que, para este Despacho son suficientes para confirmar el acto administrativo recurrido.

---

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

3. POTESTAD SANCIONADORA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Frente al procedimiento para imponer las sanciones, el artículo 22 de la Ley 1581 de 2012 señala que, *"La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes (…)".*

El artículo 23[13], por su parte, establece las sanciones que podrá imponer esta entidad a los Responsables y Encargados del Tratamiento de Datos.

Respecto de la "Potestad sancionatoria", la Corte Constitucional ha señalado:

> *"El poder sancionador estatal ha sido definido como "un instrumento de autoprotección, en cuanto contribuye a preservar el orden jurídico institucional mediante la asignación de competencias a la administración que la habilitan para imponer a sus propios funcionarios y a los particulares el acatamiento, inclusive por medio punitivos, de una disciplina cuya observancia contribuye a la realización de sus cometidos.*
>
> *Esa potestad 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 toros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (iv) El principio de proporcionalidad que se traduce en que la sanción debe ser proporcionalidad a la falta o infracción administrativa que se busca sancionar. (v) La independencia de la sanción penal; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal."*[14]

En el mismo sentido, y en relación con los principios[15] señalados, dicha corporación por medio de la Sentencia C-948 de 2002 manifestó:

> *"En la doctrina[36][16]se postula, así mismo, sin discusión que la administración o las autoridades titulares de funciones administrativas lo sean de potestad sancionadora y que ésta en cuanto manifestación del ius puniendi del Estado está sometida a claros principios generalmente aceptados, y en la mayoría de los casos proclamados de manera explicita en los textos constitucionales. Así, a los principios de configuración del sistema sancionador como los de legalidad (toda sanción debe tener fundamento en la ley), tipicidad (exigencia de descripción especifica y precisa por la norma creadora de las infracciones y de las sanciones, de las conductas que pueden ser sancionadas y del contenido material de las sanciones que puede imponerse por la comisión de cada conducta, así como la correlación entre unas y otras) y de prescripción (los particulares no pueden quedar sujetos de manera indefinida a la puesta en marcha de los instrumentos sancionatorios), se suman los propios de aplicación del sistema sancionador, como los de culpabilidad o responsabilidad según el caso – régimen disciplinario o régimen de sanciones administrativas no disciplinarias- (juicio personal de reprochabilidad dirigido al autor de un delito o falta[37][17]), de proporcionalidad o el denominado non bis in ídem".*

Ahora, al hacer referencia al principio de legalidad en materia de protección del derecho de habeas data, la Corte Constitucional mediante Sentencia C-1011 de 2008, manifestó:

---

[13] **ARTÍCULO 23. SANCIONES.** La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:
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;
b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;
c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;
d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

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

[15] "Los principios señalados en el CPACA tienen un carácter normativo y vinculante, a diferencia de la naturaleza orientadora que se predicaba en el CCA. La aplicabilidad general de los principios previstos en el artículo 3° del CPACA, como desarrollo directo de la Constitución Política, conlleva a que dichos principios deban observarse para cualquier actuación administrativa, incluidas las reguladas en leyes especiales. Así las cosas, el intérprete deberá utilizarlos directamente o hacer un ejercicio de integración normativa, entre los principios de la actuación administrativa previstos en la ley especial y los señalados en el CPACA". Laverde A. JUAN MANUEL. Manual de Procedimiento Administrativo Sancionatorio. Ed. Legis S.A. Bogotá Colombia Segunda Edición 2018.p. 51

[16] [36] Juan Alfonso Santamaría Pastor. Principios de Derecho Administrativo. Volumen II. Ed. Centro de Estudios Ramón Areces. Madrid. Tomo II. Segunda Edición. 2000.

[17] [37] Ver Ramón Parada Vásquez. Derecho Administrativo. Tomo I Marcial Pons. Madrid 1996. Luis Morell Ocaña. Curso de Derecho Administrativo. Tomo II "La actividad de las administraciones públicas. Su control administrativo y jurisdiccional". Arandazi. Madrid. 1996.

> *"Para la Corte, en consecuencia, la flexibilidad que puede establecer el legislador en materia de derecho administrativo sancionador es compatible con la Constitución, siempre que esta característica no sea tan amplia que permita la arbitrariedad de la administración. Un cierto grado de movilidad a la administración para aplicar las hipótesis fácticas establecidas en la ley guarda coherencia con los fines constitucionales de esta actividad sancionatoria administrativa, en la medida que le permite cumplir eficaz y eficientemente con las obligaciones impuestas por la Carta. Sin embargo, ha advertido que la flexibilidad del principio de legalidad no puede tener un carácter extremo, al punto que se permita la arbitrariedad de la administración en la imposición de las sanciones o las penas**[203]**"*[18]*.*

Por lo tanto, no puede la administración sobrepasar los límites que le impone el legislador al momento de aplicar una sanción, es decir, que la conducta que está siendo investigada debe tener una connotación sancionable por mandato legal. En este punto es relevante el **principio de tipicidad**, el cual no es otra cosa que *"la exigencia de una descripción específica y precisa por la norma creadora de las infracciones y de las sanciones, de las conductas que pueden ser sancionadas y del contenido material de las sanciones que puede imponerse por la comisión de cada conducta, así como la correlación entre unas y otras"*[19].

Sobre el citado principio de tipicidad, la Corte Constitucional mediante Sentencia 748 de 2011 sostuvo:

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

Se concluye entonces que es suficiente desconocer cualquiera de las disposiciones contempladas en la Ley 1581 de 2012, para que la administración pueda ejercer su potestad sancionatoria, eso sí, en los casos en los que así lo determine la actuación administrativa correspondiente, como consecuencia directa de la trasgresión de las normas que amparan el derecho fundamental de *habeas data*. Principalmente, cuando se trata de las disposiciones que se refieren a los deberes a los que están sujetos los Responsables o Encargados del Tratamiento de la información.

Así las cosas, en el caso bajo estudio, se dan los presupuestos requeridos para determinar que las conductas desplegadas por **FONDO FEG** en su calidad de Responsable y de **BANSERFIN**, en calidad de Encargado, vulneraron las normas de protección del derecho de *habeas data* relacionadas con el principio de seguridad.

Por su parte, el artículo 24, ordena que *"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.

Como se observa, este último establece los factores o elementos de juicio pertinentes que, según las particularidades de cada caso, se deben aplicar para imponer una sanción, respetando las garantías del artículo 29 constitucional[20]. Esos criterios, según la Sentencia C-748 de 2011, hacen referencia a cinco circunstancias de agravación, entre los literales a) y e**), y a una de atenuación o disminución de la sanción, correspondiente al literal f).**

Siendo así, para la correcta adecuación de los hechos y la sanción aplicable, el operador jurídico en materia de protección de Datos personales debe analizar los criterios de graduación que sean pertinentes o, como lo indica el artículo 24 de la Ley 1581 de 2012 que "resulten aplicables" con miras a establecer cómo se usan en el caso concreto y, de esa forma, seleccionar y graduar la sanción que se impondrá.

---

[18] [203] Sentencia C-406 de 2004.
[19] Sentencias C-827 de 2001 y C-343 de 2006.
[20] Artículo 29. El debido proceso se aplicará a toda clase de actuaciones judiciales y **administrativas.** (…) (negrita añadida)

Nótese que la parte final del párrafo primero de dicho artículo no exige la aplicación en abstracto de todos los factores mencionados en el mismo, sino la consideración de aquellos que, según las particularidades de cada caso, sean apropiados.

La Dirección de Protección de Datos Personales al imponer la sanción a **FONDO FEG** respecto del incumplimiento del literal n) del artículo 17 de la Ley 1581 de 2012, tuvo en cuenta la circunstancia de atenuación establecida en el literal f) del artículo 24 citado.

Ahora bien, respecto de la solicitud de disminución de la sanción impuesta por parte de **BANSERFIN**, resulta necesario indicarle que para la aplicación de la citada circunstancia de atenuación, es requisito indispensable el reconocimiento o aceptación expresa de la comisión de la falta, con anterioridad a la imposición de la sanción. Este despacho pudo verificar que **BANSERFIN** no reconoció expresamente haber cometido la vulneración que se le imputa.

Es necesario precisar que las sanciones que se imponen dentro de procesos administrativos sancionatorios no constituyen ninguna cuantificación de perjuicios materiales o morales, es decir no se trata de la estimación de un daño subjetivo, como sucede en el régimen civil de responsabilidad. Por el contrario, las sanciones que impone esta superintendencia, en virtud del artículo 22 y siguientes de la Ley 1581 de 2012, son una consecuencia impuesta en contra de la persona natural o jurídica que viole las disposiciones de la citada ley[21]. Ese efecto negativo tiene como finalidad no solo sancionar por violar las leyes sino promover y garantizar el cumplimiento del Régimen General de Protección de Datos Personales y, de esa forma, proteger el Derecho Fundamental a la Protección de Datos Personales, entre otros[22].

La imposición de sanciones por violación de la Ley 1581 de 2012 tiene como fin central proteger y promover el respeto del derecho fundamental a la protección de Datos personales, derecho humano (universal, inalienable, indivisible, irrenunciable e imprescriptible) que fue positivizado por el en el artículo 15 de la Constitución Política Nacional, 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.

Del mismo modo, la vulneración del Derecho Fundamental a la Protección de Datos Personales no solo afecta los derechos de una persona en particular, sino que, pone en riesgo los derechos fundamentales de toda la sociedad. Por eso, las sanciones de dichas conductas no pueden, ni deben tratarse, como una cuestión insignificante o de poca monta. La transgresión flagrante a los derechos humanos de un ciudadano es, por sí solo, un hecho muy grave que no necesita de forzosos razonamientos para comprender su notoria importancia en la sociedad.

De conformidad con lo indicado, las sanciones impuestas son proporcionales si se tiene en cuenta que el monto 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, las multas impuestas a **BANSERFIN** y a **FONDO FEG** corresponden al 0.85% y al 1.13% respectivamente, del límite dispuesto en la ley.

Finalmente, resulta pertinente resaltar lo siguiente:

I. Las multas impuestas a **BANSERFIN** y a **FONDO FEG** corresponden al 0.85% y al 1.13% respectivamente del máximo legal permitido (2000 salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012).

II. El monto de dicha sanción es el resultado del análisis del daño y/o puesta en peligro de los intereses jurídicos tutelados en el trámite de la primera instancia de esta actuación administrativa. Así como del incumplimiento de los deberes impuestos por la Ley 1581 de 2012 a los Responsables y Encargados del Tratamiento de los Datos personales.

III. La Resolución recurrida fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Asimismo, fue el resultado de la valoración fáctica y

[21] El artículo 22 de la Ley 1581 de 2012 define que la Superintendencia de Industria y Comercio, **una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento**, adoptará las medidas o impondrá las sanciones correspondientes. (negrita añadida). Al respecto dijo la Corte Constitucional en la Sentencia C-748 de 2011: "*Esta norma [el artículo 23] cumple con el principio de tipicidad, **para lo cual debe interpretarse conjuntamente con el artículo 22 de la futura ley estatutaria, que establece la posibilidad de imponer sanciones cuando se hayan incumplido las disposiciones de esta ley.** En este sentido, **el supuesto de hecho que completa la norma jurídica sancionatoria está constituido por la infracción de las disposiciones de la futura ley estatutaria** por la cual se dictan disposiciones generales para la protección de datos personales.*" (negrita añadida)

[22] 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.

probatoria de la primera instancia que llevó a concluir y comprobar la vulneración al derecho de *habeas data* del Titular y en particular de los mandatos legales señalados.

IV. Las sanciones que se imponen dentro de esta clase de procesos, no derivan de los daños o perjuicios causados a los Titulares por incumplir la regulación sobre Tratamiento de Datos personales. Es decir, las normas que protegen el derecho de *habeas data o* protección de Datos personales no se refieren a la responsabilidad civil de los Responsables y Encargados del Tratamiento de Datos.

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

Recuérdese que, según la Declaración Universal de los Derechos Humanos, *"el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad"*[23]*.* 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[24]*.* Así las cosas, recalcamos, la violación de Derechos Humanos es una conducta gravísima que no solo atenta contra los intereses de un individuo en particular sino de la sociedad en general.

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

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

La regulación colombiana le impone al Responsable del Tratamiento la responsabilidad de garantizar la eficacia de los derechos del Titular del Dato, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia *"existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante"*[25].

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

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

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

---

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

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

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

[26] El texto completo del artículo 26 del decreto 1377 de 2013 ordena lo siguiente: Artículo 26. Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:
1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.
En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de

Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012". Así resulta imposible ignorar la forma en que el Responsable o Encargado del Tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengas como propósito lograr que los postulados legales sean realidades verificables, 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*)"[27].

El término *"accountability"* a pesar de los diferentes significados ha sido entendido en el campo de la protección de Datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

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

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

El principio de responsabilidad demostrada –*accountability*- demanda implementar acciones de diversa naturaleza[28] 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.

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que *"la autorregulación sólo redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que* ***no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales"***[29]. (Destacamos). 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

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"

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

[28] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humanas y de gestión que involucran procesos y procedimientos.

[29] 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.

organizaciones sean proactivos respecto del Tratamiento de la información de manera que por iniciativa propia adopten medidas estratégicas capaces de garantizar los derechos de los Titulares de los Datos personales y su gestión siempre sea respetuosa de los derechos humanos.

Aunque no es espacio para explicar cada uno de los anteriores aspectos mencionados en la guía[30], ponemos de presente que 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"*[31].

También se ha afirmado que *"compliance es un término que hace referencia a la gestión de las organizaciones conforme a las obligaciones que le vienen impuestas (requisitos regulatorios) o que se ha autoimpuesto (éticas)"*[32]. 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[33].

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 pongan en marcha, entre otros, un "*sistema de administración de riesgos asociados al tratamiento de datos personales"*[34] 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"*[35].

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

El artículo 333 establece que *"la actividad económica y la iniciativa privada son libres, dentro de los límites del bien común"*. Este *"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 Constitución Política Nacional 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 solo 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 mencionado, exige que la realización de cualquier actividad económica garantice, entre otras, los derechos fundamentales de las personas. Es por eso que la Constitución Política pone de presente que la participación en el mercado supone responsabilidades y que efectuar actividades empresariales implica cumplir con las obligaciones previstas en la ley.

Según el artículo 22 de la ley 222 de 1995[36] la expresión administradores comprende al *"representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con*

---

[30] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
[31] Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com/ (última consulta: 6 de noviembre de 2018)
[32] 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/
[33] Idem
[34] Cfr. Superintendencia de Industria y Comercio (2015) "*Guía para implementación del principio de responsabilidad demostrada (accountability)*". Págs 16-18
[35] Ibid. P 16
[36] 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"

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)

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[37] 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"[38]. 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.*

En virtud de todo lo anterior se exhorta a los Representantes Legales de **BANCA DE SERVICIOS FINANCIEROS S.A.S. – BANSERFIN S.A.S.** y **FONDO EMPLEADOS GRANFONDO – FEG** para que adopte medidas pertinentes, útiles, efectivas y verificables con miras a:

a) Respetar y garantizar los derechos de los Titulares de los Datos.
b) Evitar que se repitan hechos como los que dieron origen a la presente investigación.
c) Dar estricto cumplimiento de las disposiciones legales y estatutarias sobre Tratamiento de Datos personales.
d) Aplicar el principio de responsabilidad demostrada, observando las orientaciones de la Superintendencia de Industria y Comercio incorporadas en la "Guía para implementación del principio de responsabilidad demostrada (accountability)"[39]. Especial énfasis se debe hacer en utilizar mecanismos de monitoreo y control que permitan comprobar la efectividad de las medidas de seguridad.

---

[37] 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."
[38] Cfr. Parte inicial del artículo 24 de la ley 222 de 1995
[39] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

CONCLUSIONES

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

a. Se confirmó que **FONDO – FEG** en su calidad de Responsable del Tratamiento de la información infringió las normas sobre protección de Datos personales consagradas en el literal d) del artículo 17 de la Ley 1581 de 2012, en concordancia con los literales f) y g) del artículo 4 de la citada Ley, al igual que el literal n) del artículo 17, en concordancia con el artículo 25 de la Ley 1581 de 2012 y el literal g) del capítulo segundo de la Circular Externa No. 02 del 3 de noviembre de 2015, que adiciona el Capítulo Segundo en el Título V de la Circular Única de esta superintendencia, relacionado con el registro de Bases de Datos.

b. Se corroboró que **BANSERFIN** en su calidad de Encargado del Tratamiento de la información infringió las normas sobre protección de Datos personales consagradas en el literal b) del artículo 18 de la Ley 1581 de 2012, en concordancia con los literales f) y g) del artículo 4 de la citada ley, en la medida que

c. **FONDO – FEG,** en su calidad de Responsable del Tratamiento de la información **debe exigir en todo momento** al encargado de la información el respeto a las condiciones de seguridad y privacidad de la información del Titular, situación que, no se limita únicamente al establecimiento de cláusulas contractuales. Asimismo, debió informar a esta autoridad sobre la violación a los códigos de seguridad infringidos por parte **BANSERFIN** en su calidad de Encargado del Tratamiento.

d. Al **FONDO FEG** en el acto administrativo que se revisa, le fue aplicado el criterio de atenuación establecido en el literal f) del artículo 24 de la Ley 1581 de 2012, respecto de la sanción aplicada por la vulneración del literal n) del artículo 17 de la Ley 1581 de 2012.

e. Las multas impuestas mediante la Resolución No. 78239 de 4 de diciembre de 2020 a **BANSERFIN** y **FONDO FEG** equivalen respectivamente al 0.85% ($15.000.000) y 1.13% ($20.000.000) del máximo legal permitido dos mil (2000) salarios mínimos legales mensuales vigentes establecido en el literal a del artículo 23 de la Ley 1581 de 2012.

De conformidad con lo indicado y una vez analizadas las pruebas y documentos allegados a la presente actuación administrativa, encuentra este Despacho que el acto administrativo objeto de impugnación fue expedido observando la Ley. De esta forma y de acuerdo con el artículo 80 del Código de Procedimiento Administrativo y lo Contencioso Administrativo y las consideraciones del Despacho, se confirmará la Resolución 78239 de 4 de diciembre de 2020.

En mérito de lo expuesto, este Despacho,

RESUELVE

Primero. Confirmar en todas sus partes la Resolución 78239 de 4 de diciembre de 2020, de conformidad con lo expuesto en la parte motiva del presente acto administrativo.

Segundo. Notificar personalmente en contenido de la presente decisión a la sociedad **BANCA DE SERVICIOS FINANCIEROS S.A.S. – BANSERFIN S.A.S.** identificada con el NIT. 900.069.458-1, a través de su representante legal o apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

Tercero. Notificar personalmente en contenido de la presente decisión a la sociedad **FONDO DE EMPLEADOS GRANFONDO – FEG** identificada con el NIT. 800.097.913-8, a través de su representante legal o apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

Cuarto. Comunicar la presente decisión al señor [redacted], identificado con la cédula de ciudadanía [redacted]

Quinto. Informar 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., Julio 6 de 2021

El Superintendente Delegado para la Protección de Datos Personales,

NELSON REMOLINA ANGARITA

NTL

NOTIFICACIÓN:

Sociedad: **BANCA DE SERVICIOS FINANCIEROS S.A.S. – BANSERFIN S.A.S.**
Identificación: Nit. 900.069.458-1
Representante legal: **GERMAN ADOLFO HUERFANO MÈNDEZ**
Identificación: C.C. 19.395.834
Dirección: Carrera 18 No. 78 – 40 Oficina 602
Ciudad: Bogotá D.C.
Correo electrónico: info@banserfin.com

Sociedad: **FONDO DE EMPLEADOS GRANFONDO – FEG**
Identificación: Nit. 800.097.913-8
Representante legal: **JORGE HELÍ MORALES MARTINEZ**
Identificación: C.C. 19.274.250

Apoderada: [redacted]
Identificación: C.C. [redacted]
Tarjeta Profesional: [redacted]
Dirección: [redacted]
Ciudad: [redacted]
Correo electrónico: [redacted]

COMUNICACIÓN:

Titular de la Información:

Señor: [redacted]
Identificación: C.C. [redacted]
Dirección: [redacted]
Ciudad: [redacted]
Correo Electrónico: [redacted]