REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 76851 DE 2021

(Noviembre 26 de 2021)

Por la cual se resuelve un recurso de apelación

Radicación No. 18-193960

VERSIÓN PÚBLICA

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES

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

CONSIDERANDO:

PRIMERO: Que mediante oficio radicado con el número 18-193960 de fecha 26 de julio de 2018, el señor [redacted], presentó ante esta Superintendencia queja contra la CÁMARA DE COMERCIO DE BOGOTÁ identificada con NIT. 860.007.322-9, manifestando lo siguiente:

> El día 17 de julio recibí un correo de la CCB con la base de datos completa de todos los instructores que dictamos clase, el cual tiene dos adjuntos, uno de ellos la base de datos de los conferencistas que contiene 413 registros con nombres completos, celulares, teléfonos, correos y cursos con fechas.

SEGUNDO: Que mediante Resolución 28906 del 18 de julio de 2019 la Dirección de Investigación de Protección de Datos personales resolvió abrir investigación y formular pliego de cargos contra la CÁMARA DE COMERCIO DE BOGOTÁ identificada con NIT. 860.007.322-9, por presunta vulneración a las normas de protección de datos personales contenidas en la Ley 1581 de 2012.

TERCERO: Que una vez efectuado el análisis de los documentos que obran en el expediente, la Dirección de Investigación de Protección de Datos Personales mediante Resolución No. 81697 del 21 de diciembre de 2020, resolvió lo siguiente:

> **RESUELVE**
>
> **ARTÍCULO PRIMERO: Imponer** una sanción pecuniaria a la **CÁMARA DE COMERCIO DE BGOTÁ** identificada con el Nit 860.007.322-9 de **OCHENTA MILLONES OCHO MIL NOVECIENTOS VEINTINUEVE PESOS M/CTE ($80.008.929)** equivalente a **(2.247)** unidades de valor tributario vigentes, por la violación a lo dispuesto en el literal d) del artículo 17 de la Ley 1581 de 2012 en concordancia con lo establecido en el literal g) del artículo 4 de la misma Ley y el artículo 2.2.2.25.6.1 del Decreto único Reglamentario 1074 de 2015.
>
> **PARÁGRAFO:** El valor de la sanción pecuniaria que por esta resolución se impone, deberá consignarse en efectivo o cheque de gerencia en el Banco Popular, Cuenta No. 050000249, a nombre de Dirección del Tesoro Nacional – Fondos Comunes, Código Rentístico No. 350300, Nit. 899999090-2. El pago deberá efectuarse dentro de los cinco (5) días hábiles siguientes a la ejecutoria de esta resolución y acreditarse en la ventanilla de Tesorería de esta Superintendencia con el original de la consignación, donde le expedirán el recibo de caja aplicado a la resolución sancionatoria. Vencido este plazo se cobrarán intereses por cada día de retraso, liquidados a la tasa del 12% efectivo anual.

VERSIÓN PÚBLICA

Por la cual se resuelve un recurso de apelación

ARTÍCULO SEGUNDO: Ordenar a la **CÁMARA DE COMERCIO DE BOGOTÁ** identificada con el Nit. 860.007.322-9 cumplir las instrucciones impartidas por esta Dirección en el presente acto administrativo, según lo expuesto en su parte motiva, la cual consiste en aportar una certificación expedida por un auditor externo en la que consten:

- La realización de capacitaciones periódicas a sus trabajadores, en relación con el cumplimento de las normas de protección de datos personales, contenidas en la Ley 1581 de 2012. En particular, las temáticas concernientes a la seguridad de la información, de acuerdo con la labor desempeñada y conforme al tipo de tratamiento que realicen a los datos administrados por la **CÁMARA DE COMERCIO DE BOGOTÁ** en calidad de Responsable; y,

- Los procedimientos implementados para impedir el acceso de personal externo no autorizado a los archivos que contengan registros de datos personales.

Esta orden deberá ser cumplida por la **CÁMARA DE COMERCIO DE BOGOTÁ** dentro del término de ciento veinte (120) días hábiles, siguientes a la ejecutoria de la presente decisión.

De lo anteriormente ordenado la **CÁMARA DE COMERCIO DE BOGOTÁ** deberá remitir a este Despacho dicha certificación, donde consten las acciones correctivas adoptadas

PARÁGRAFO PRIMERO: La **CÁMARA DE COMERCIO DE BOGOTÁ** identificada con el Nit. 860.0 07.322-9, deberá acreditar el cumplimiento de lo ordenado en el presente artículo ante esta Superintendencia dentro de los cinco (5) días hábiles siguientes a la expiración del plazo previsto para su acatamiento.

CUARTO: Que mediante escrito del 5 de enero de 2021 la CÁMARA DE COMERCIO DE BOGOTÁ, a través de su apoderado, interpuso recurso de reposición y en subsidio el de apelación contra la Resolución No. 81697 del 21 de diciembre de 2020, solicitando se revoque la decisión basada en los siguientes argumentos:

"La actuación en contra de LA CÁMARA parte de un hecho puntual y totalmente aislado en la dinámica de la entidad, consistente en el envío de un correo electrónico que a pesar de tratarse de una comunicación interna entre una funcionaria con su superior, resulto erróneamente dirigido a un grupo de "colaboradores-capacitadores expertos" como se han conocido al interior de la entidad, llevando lamentablemente como adjunto un archivo en formato Excel de uso estrictamente doméstico, el cual contenía los datos de contacto de los receptores y que estaba siendo utilizado por parte de la funcionaria para hacer el seguimiento de la aceptación a la invitación a las capacitaciones que pensando únicamente en el exclusivo beneficio de ellos, se les estaba cursando para la época.

A partir de este hecho que, sin pretender desestimar su importancia, hubiera pasado desapercibido al tratarse de personas que son parte de la "familia" de LA CÁMARA, muchos de los cuales se conocen entre sí a partir de sus labores con la entidad, el señor [redacted] identificado con cédula de ciudadanía número [redacted], pretermitiendo el conducto regular que las mismas normas de protección de datos personales establecen en materia de reclamos ante la advertencia de un posible incumplimiento a sus dictámenes, según lo prescribe el artículo 15 de la Ley 1581 de 2012, puso en conocimiento de esa Autoridad el asunto consistente en esa remisión del correo electrónico en el que se adjuntaba una base de datos de conferencistas que incorporaba "413 registros con nombres completos, celulares, teléfonos correos y cursos con fechas".

A partir de ello, se inició por esa Superintendencia la investigación basada en un único cargo, que aunque es por todos conocido vale la pena refrescar: "La presunta contravención por parte de la investigada al deber de conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración consulta uso o acceso no autorizado o fraudulento, fundamentado en las siguientes normas":

(…)

A. Frente a la imputación fáctica No. 1. " 8.2.1 Del deber de conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"

VERSIÓN PÚBLICA

Por la cual se resuelve un recurso de apelación

- *Indica esa Superintendencia, después de hacer un análisis respecto de la calidad de datos privados atribuible a los correos electrónicos y teléfonos de personas naturales, análisis que vale anotar, comparto en su totalidad, que "(….) en el caso denunciado por el señor* [redacted] *ante esta Superintendencia, se observa que el día 17 de julio de 2018, una funcionaria de la CÁMARA DE COMERCIO DE BOGOTÁ, estando en el ejercicio de sus funciones, le remitió un correo electrónico, en cuyo cuerpo, por una parte se encuentran las direcciones de correo electrónico de múltiples "conferencistas que (…) habían confirmado su asistencia e (sic) la gestión telefónica relacionada el 18 y 19 de junio" , y de la otra, se adjunta una base de datos en formato Excel "de los conferencistas que no han participado en taller de metodologías" la cual contiene información referente a nombres y apellidos, número celular, número de teléfono fijo y correo electrónico de 413 personas.(…)"*

Como tantas veces encuentro que se ha repetido a lo largo de instancias anteriores de esta actuación estimado doctor Salazar, en efecto, en la fecha indicada por el denunciante le fue remitido un correo electrónico con la información que manifiesta haber sido incorporada, lo que constituyó un error operativo y completamente involuntario que resultó violatorio de las normas de protección de datos personales.

Como fundamento de la sanción por este hecho, indica la Superintendencia en la hoja 11 de la resolución sancionatoria: "(…) Sobre el particular, se resalta que el archivo Excel no estaba protegido con contraseña de acceso, ni con formato no editable, pese a que la entidad investigada informó que cuenta con una política en tal sentido (…)."

Más adelante, en la hoja 13 del mismo documento indica que los "(…)"

Finalmente, sobre este caso puntual, concluye la Superintendencia en la hoja 14 de su resolución sancionatoria "(…) la entidad investigada no tomó precaución alguna frente a los factores de riesgo asociados a la potencial fuga de la información, máxime cuando el archivo Excel "base de datos de conferencistas" no estaba protegido con una contraseña que impidiera el acceso a personal no autorizado (…)"

Al respecto, doctor Salazar quiero manifestar de forma respetuosa mi divergencia con la apreciación de esa Superintendencia, particularmente frente a lo indicado en torno a la falta de verificación en la práctica de las políticas establecidas por la entidad para la custodia de la información, así como a lo mencionado respecto a una falta de adopción de medidas de seguridad para los archivos que se comparten por parte de la entidad.

Este desacuerdo que me permito expresar lo evidencio en algo que esa Superintendencia ha omitido valorar en sus análisis respecto del origen de este archivo particular, su objetivo exclusivo y su característica principal de ser de transitoria existencia.

En efecto, como bien se puede establecer a partir de los apartes de los descargos iniciales reproducidos por esa Superintendencia en su documento sancionatorio, este archivo estaba constituido por un Excel con una vida útil totalmente transitoria, cuya única razón de existir era la de contribuir a que unos, muy pocos, funcionarios de LA CÁMARA interesados en el tema pudieran hacer el seguimiento de la aceptación a las invitaciones que se estaban realizando a sus más cercanos "colaboradores – capacitadores expertos". Es decir, carecía de cualquier vocación circulatoria interna y mucho menos había alguna pretensión para que se reprodujera hacia el exterior de la entidad, a lo que se añade que su utilización era absolutamente efímera y restringida.

Ahora bien. ¿Era éste un archivo editable y carecía de contraseñas para su uso? Efectivamente, y eso se explica en que como ya se indicó, su destinación no era la de circular. Se trataba de un archivo que se buscaba que fuera constantemente modificado y actualizado por parte de la auxiliar administrativa en cuyo computador reposaba durante el período en el que se surtía la convocatoria, de ahí que no resulta conducente que se indilguen a LA CÁMARA fallas de seguridad o que se haga una mención en la resolución sancionatoria de esa Superintendencia a que no se están cumpliendo las seguridades que se presentan para archivos cuya vocación es la de ser compartidos, pues, sin ninguna duda, esas no son las seguridades que se deban aplicar a archivos que como el que hoy es objeto de cuestionamientos, solo son temporales y

de circulación restringida cuya principal esencia consiste en que sean editables, modificables y actualizables por el funcionario que los trata.

De esta manera el argumento en torno a que en la práctica no se están cumpliendo las medidas de seguridad tantas veces reiterado en la resolución sancionatoria para argumentar que LA CÁMARA no está atendiendo en la práctica los lineamientos establecidos en su documentación, no resulta apropiado para hacer la medición de la responsabilidad de la entidad en este caso.

De aquí que me permita reiterar que, en mi opinión, la Superintendencia incurre en un error de apreciación de los hechos y de aplicación de la norma al caso en concreto al pretender que sus vigilados impongan a archivos creados por un funcionario en su computador para hacer un seguimiento a una invitación los criterios de seguridad establecidos para las bases de datos que tienen como finalidad su circulación.

Este punto fue advertido desde la primera comunicación que se envió a la Superintendencia de Industria y Comercio por parte de LA CÁMARA. En ella claramente se informaron de los perfiles de los cargos que podían en un momento dado acceder al archivo y cuáles eran sus atribuciones, incluyendo las correspondientes a la auxiliar administrativa que cometió el lamentable error operativo que conllevó el envío no Autorizado de la información. Estas eran de "lectura, adición y/o modificación", no de remisión.

Estoy seguro, doctor Salazar, de que en esa misma Autoridad existen un sinnúmero de documentos y archivos que se crean por funcionarios para el desarrollo de sus actuaciones, archivos cuyo destino es adelantar las funciones propias de la entidad y que no deben ser compartidos con terceros. Sobre esos archivos ¿Está al alcance de esa Superintendencia impedir que un funcionario, en un momento dado, actuando buena fe, tome por error el archivo que ha elaborado para hacer seguimiento a una invitación en cumplimiento de sus funciones, tareas y encargos y lo publique mediante un correo electrónico? Sin duda, no.

En esa medida ¿podría ese Ente Gubernamental o cualquier otra institución ser juzgada por cuenta de una errada actuación de un funcionario particular, como la sucedida? Igualmente. Sin duda, no.

Si esto es así, entonces ¿Qué razones conducen a que a LA CÁMARA se la esté juzgando de forma tan severa por un hecho como el narrado, si lo acontecido es sólo el resultado de una circunstancia que cualquier empresa por más diligente que sea no está en la posibilidad de prever?.

Desconocemos la existencia de alguna entidad que respecto de un archivo interno de gestión creado únicamente para el seguimiento de la invitación a una capacitación por parte sus funcionarios, haya implementado claves de seguridad para su acceso o el cifrado de los datos, e igualmente desconocemos la norma que lo obligue de manera que se pueda establecer un incumplimiento a partir de su inobservancia.

- *Por otro lado, la Superintendencia indica: "(…) Igualmente, la entidad investigada dentro del "Anexo 3. Comunicados internos en materia de protección de datos personales y Seguridad de la información" tiene un acápite denominado "Buen uso del correo electrónico" publicado el 07 de mayo de 2018 (…) Respecto de este documento menciona la superintendencia en la hoja 14 de la resolución sancionatoria "(…) De la lectura del acápite denominado "Buen uso del correo electrónico" y las pautas para el envío de correos electrónicos se desprende que ninguno refiere la protección para evitar el uso, acceso o consulta no autorizada (…)".*

En este aspecto, olvida esa Superintendencia tomar en cuenta dentro de sus análisis que este no es el único documento con que se cuenta. En esa medida, haciendo parte del "Manual de Lineamientos y Prácticas Gestión de seguridad de la Información" también allegado a ese Despacho, en su oportunidad, se expresa en la página 24 frente al uso de correo electrónico que: "(…) Toda información generada con los diferentes programas computacionales (ejemplo. Office, Project, Access, WordPad, entre otros), que requiera ser enviada fuera de la entidad, y que por sus características de integridad deba ser protegida, debe estar en formatos no editables o debidamente protegida para modificaciones (contraseñas o cifrado) "(…). Es de

anotar que este manual es conocido y expresamente aceptado por cada uno de los funcionarios que hacen parte de LA CÁMARA.

De esta manera, el argumento expresado por esa Superintendencia en relación con la inexistencia de pautas para evitar el uso, acceso o consulta no autorizada, no resulta de recibo, en la medida en que con lo mencionado se logra demostrar que esos lineamientos que extraña esa Autoridad Gubernamental, si existían para el tiempo en que se presentaron los hechos y son de obligatoria aplicación por parte de toda la planta de personal de LA CÁMARA.

Lo dicho, aun cuando, como ya lo he expresado, en este caso se trataba de un archivo que ni siquiera tenía vocación circulatoria.

- *Por otro lado, indica la Superintendencia respecto a las capacitaciones que se han brindado a los funcionarios de LA CÁMARA en materia de protección de datos personales y seguridad de la información que: "(…) El argumento expuesto en líneas precedentes y las piezas probatorias aportadas por la entidad investigada en torno a las mentadas capacitaciones, son del total recibo de este Despacho; sin embargo, se observa que las mismas se llevaron a cabo con posterioridad al acontecimiento de los hechos materia de investigación. Los controles de asistencia evidencian que la primera capacitación se realizó el día 02 de agosto de 2019, dentro del marco de un ciclo de capacitaciones programado por la CÁMARA DE COMERCIO DE BOGOTÁ para sus funcionarios (…)*

Desconozco frente a esta argumentación, que llevó a esa Superintendencia a considerar que las mencionadas eran las únicas acciones que en materia de capacitaciones y divulgación de la información se habían realizado frente a los funcionarios.

Si se observa en la respuesta inicial al pliego de cargos formulado, esa Entidad podrá encontrar que la evidencia a las capacitaciones que se anexa se encontraba formando parte de las acciones de mitigación que se tomaron a partir del reconocimiento por parte de LA CÁMARA de los hechos presentados.

De esa manera, es claro que LA CÁMARA, encontrándose comprometida con la protección de los datos personales a los que accede, ha realizado múltiples encuentros y capacitaciones que le permiten asegurarse de que cada uno de sus funcionarios ha recibido, conoce y acepta las políticas desarrolladas por parte de la entidad en materia de protección y seguridad de la información.

Así lo prueba el informe de auditoría externa practicada por la firma multinacional EY en diciembre de 2017, es decir con anterioridad al acaecimiento de los hechos, uno de cuyos apartes me permitimos transcribir y cuyo apartado del texto original se anexa para su conocimiento (Anexo 4):

"(…) resumen ejecutivo de hallazgos y acciones remediales recomendadas. (…) Durante la auditoría identificamos que la CCB ha implementado un conjunto de medidas encaminadas a cumplir con el RCPDP, en línea con el principio de responsabilidad demostrada. A continuación enunciamos las más importantes:

1. Ha realizado capacitaciones a los colaboradores relacionadas con la seguridad de la información y datos personales.
2. Realiza reuniones periódicas con el objeto de determinar términos de respuesta y atención a Peticiones, quejas y reclamos recibidos (…)" (Resaltado fuera del texto).

Para el caso concreto de la funcionaria que realizó el envío erróneo de las bases de datos que constituye el fundamento de la presente actuación, con anterioridad a la fecha de ocurrencia del hecho, había tenido, solo para dar una muestra del último semestre de 2017 y primer semestre de 2018, entre otras, las acciones de formación que me permito listar y cuyos documentos se anexan para su conocimiento (Anexo 5)

(…)

VERSIÓN PÚBLICA

Por la cual se resuelve un recurso de apelación

B. Frente a la imputación fáctica No. 2. "8.2.2 De la aplicación del principio de responsabilidad Demostrada"

Indica la Superintendencia en la hoja 15 de la resolución sancionatoria "(…) esta Superintendencia ha sido enfática en señalar que las disposiciones contenidas en los artículos 2.2.2.25.6.1 y siguientes del Decreto 1074 de 2015, en relación con la adopción de políticas y procedimientos efectivos para el adecuado cumplimiento de la Ley 1581 de 2012 implican que concurran una serie de presupuestos que permitan evidenciar que los procedimientos implementados, en la práctica son reales y efectivos.

"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 -titulado DEMOSTRACIÓN- establece que "los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012(…)".

A lo anterior, añade en la hoja 17 del mismo documento "(…) Precisado lo anterior, el sistema de administración de riesgos que adopte la empresa debe tener en cuenta las etapas de identificación, medición, control y monitoreo, así como el cumplimiento de unos requisitos de formación y educación de todos los empleados de la organización, y un protocolo de respuesta en el manejo de violaciones e incidentes. Particularidades que se encuentran contenidas en el cúmulo de documentos aportados por la entidad investigada, pero que se desvirtúan por los argumentos hasta aquí expuestos por este Despacho y reforzados por el material probatorio contenido en el "Anexo 7 Información cruzada entre la funcionaria y su jefe en donde se reconoce el error involuntario cometido en contra de las políticas de nuestra entidad", las cuales ponen de manifiesto que la auxiliar administrativa no solo no se percató del incidente, sino que no tenía claras las acciones a surtir con posterioridad a la ocurrencia del mismo y debió esperar las instrucciones suministradas por la señora [redacted] *Coligiéndose de lo expuesto, la importancia que reviste que el robusto andamiaje documental con el que cuenta la entidad investigada en materia de protección de datos personales y seguridad de la información, esté acompañado de mecanismos de monitoreo y verificación que permitan anticipar situaciones como la que se presentó en el caso objeto de estudio y de que las medidas implementadas no solo sean pertinentes, adecuadas y útiles, sino que funcionen correctamente.*

En definitiva esa Superintendencia basa su conclusión de incumplimiento del principio de responsabilidad demostrada por parte de LA CÁMARA en que, según se pude entender de todo lo dicho, no se tomaron por parte de la entidad las acciones pertinentes para que el personal de la misma conociera el protocolo de violaciones e incidentes y actuara de conformidad y por otra parte en considerar que no se habían puesto en práctica las medidas para la mitigación de los riesgos que conlleva el tratamiento de datos personales.

Sobre este aspecto encuentro que, al contrario de lo que indica esa Superintendencia es precisamente el material probatorio allegado el que permite reiterar que para la fecha de la ocurrencia de los hechos LA CÁMARA, además de contar con toda una serie de políticas para el tratamiento de la información, las ponía en conocimiento de todos funcionarios.

El correo electrónico en que se basa la Superintendencia para suponer que la funcionaria desconocía como actuar ante un incidente de seguridad, consiste en una comunicación, apenas lógica entre un empleado con su jefe, que se da normalmente en todas las entidades ya sean privadas o no. ¿Si un funcionario comete un error que puede tener impacto sobre la entidad, no resulta lo mas lógico que no obstante todos los protocolos existentes, lo primero que haga sea comunicárselo a su superior con el fin de pedir su direccionamiento?, ¿No causaría una molestia más grande al interior de una entidad que ante un hecho como el que se presentó, un funcionario omita comunicarle tal circunstancia a su superior y empiece a actuar por su propia cuenta, así sea siguiendo los protocolos por todos conocidos?. Agradezco que sobre este particular se haga por parte de esa Superintendencia una reflexión más profunda con base en lo aquí expresado.

Sin embargo, he de ratificar que los funcionarios de LA CÁMARA, como parte de su vinculación a la entidad, son provistos con el documento de seguridad cuya lectura y compresión se hace

obligatoria al momento de su contratación, de lo cual se deja constancia con la firma por su parte del documento de conocimiento y aceptación del mismo. Se anexa para su conocimiento copia de la comunicación en tal sentido firmada por la auxiliar involucrada en los hechos (anexo 6).

Adicionalmente, como ya se tuvo la oportunidad de mencionarlo, se realizan constantes tareas de capacitación en las diferentes materias que tienen que ver con la privacidad y la seguridad de la información, sólo como una muestra de lo que manifiesto pongo en su consideración lo instruido frente al adecuado uso del correo electrónico, en la capacitación desarrollada el 8 de mayo de 2018, esto es, justo antes de la fecha de ocurrencia de los hechos. De lo transcrito agradezco observar detenidamente los puntos 4, 5, 6, 7 y 8. Igualmente se adjunta el correo enviado y recibido por la funcionaria en la fecha indicada con esta capacitación (Anexo 7)

De esta manera respetuosamente, solicito a esa Superintendencia realizar un análisis sobre el acervo probatorio que da muestras de las acciones que se han tomado por parte de LA CÁMARA para impedir que por parte de sus colaboradores se presente cualquier tipo de vulneración a la normatividad vigente en materia de protección de datos personales y que en caso de presentarse tengan el conocimiento adecuado para adelantar las acciones institucionales más pertinentes.

C. Frente a la inobservancia de los requisitos de procedibilidad para el inicio de actuaciones ante la Superintendencia de Industria y comercio en materia de protección de datos personales.

Tal y como ya se tuvo la oportunidad de manifestarlo en el escrito inicial de descargos, encuentro que no es un asunto menor el hecho de no dar cumplimiento a los requisitos procedimentales impuestos por las normas de protección de datos personales al momento de solicitar el inicio de una actuación administrativa por parte de un titular de la información.

No quiero dejar mencionar este hecho en la medida en que además de presentarse una desatención a los requerimientos normativos para proceder con el inicio de la investigación administrativa, en la práctica permitir que actuaciones como la adelantada por el señor [redacted] continúen dando lugar al inicio de actuaciones por parte de esa Autoridad tiene dos desafortunadas consecuencias, la primera para los administrados en la medida en que se les niega una posibilidad de aclarar las situaciones acontecidas y llegar a acuerdos con los directos afectados generando, además, todo un desgaste en materia operativa y económica.

La segunda para la propia autoridad, pues al pretermitir la exigencia del requisito de procedibilidad, esto es, la presentación de las solicitudes inicialmente ante el presunto infractor, se genera un movimiento de todo el recurso institucional que podría resultar innecesario, generando desaprovechamiento y desgaste del aparato estatal que debe desviar la atención de sus funcionarios de temas relevantes a tener que dedicarse a resolver casos que pueden ser atendidos por las propias partes involucradas, principalmente tratándose de entidades que, de conocer de algún tipo de inconformidad por parte de los titulares de la información que tratan podrían tener la oportunidad de propiciar acuerdos muy eficientes.

D. Desconocimiento de la existencia de una causal de disminución de la pena.

Señala esa Superintendencia en su resolución sancionatoria que "(…) El criterio de atenuación señalado en el literal f) del artículo 24 de la Ley 1581 de 2012 no se aplicará toda vez que la investigada, en el escrito de descargos presentado el día 09 de agosto de 2019, limitó su ejercicio a la narración de unos hechos que se encuentran suficientemente acreditados en el expediente, pero no reconoció de manera expresa la comisión de la infracción al deber contemplado en el literal d) del artículo 17 de la Ley 1581 de 2012 en concordancia con lo establecido en el literal g) del artículo 4 de la misma ley y el artículo 2.2.2.25.6.1 del Decreto único Reglamentario 1074 de 2015, La entidad investigada indicó expresamente "que, en efecto como bien lo anuncia el denunciante, en la fecha por él indicada le fue remitido un correo electrónico con la información que manifiesta haber sido incorporada, error operativo que de ninguna manera podría enviar (sic) o dejar de aceptar".

No encuentro las razones por las cuales esa Superintendencia llega a esa conclusión para la inaplicabilidad de la causal. De los documentos que aparecen como antecedente, hallo que no

sólo se aceptó la existencia del hecho, sino que, en repetidas ocasiones, dentro del escrito de descargos y en el documento de alegatos de conclusión, se hizo alusión al error operativo e involuntario presentado y las acciones de mitigación efectuadas a partir de su reconocimiento.

Traigo a colación los siguientes apartes de los documentos correspondientes a los que tuve acceso:

- *Documento de descargos:*

Página 3. "Estimado doctor Salazar, sea lo primero indicar que, en efecto, como bien lo anuncia el denunciante, en la fecha por él indicada le fue remitido un correo electrónico con la información que manifiesta haber sido incorporada, error operativo que de ninguna manera podría obviar o dejar de aceptar."

Página 4. "Sí, en efecto. Como ya tuve ocasión de mencionar y aceptar desde un principio, el error endilgado por el denunciante fue cometido por parte de una de las auxiliares de nuestro equipo, quien en el afán de seguir las instrucciones de convocar a los miembros de nuestra comunidad a las capacitaciones que teníamos preparadas para ellos, tomó un archivo en formato Excel de circulación absolutamente restringida como lo pudo apreciar en el cuadro de privilegios en el manejo de la información que allegamos en la respuesta enviada el día 19 de marzo de 2019, al que más adelante haré nuevamente referencia, y lo remitió a los convocados, omitiendo eliminar dentro del mismo los datos correspondientes a su información de contacto."

Página 5. "En tal medida, y como una directriz que parte de sus directivas, nuestra entidad no podía haber hecho otra cosa que pedir disculpas a los posibles afectados por ese error humano, como en efecto se hizo a través del envío de un correo electrónico de fecha 19 de julio de 2018 en el que se les comunicó lo sucedido."

Página 11. "Una vez se nos informó del error cometido por la funcionaria en nuestra entidad procedimos a realizar acciones de mitigación de los efectos a los posibles afectados"

Página 11. "V. ACCIONES REPARADORAS (…)"

Página 12 "1. Se presentó un error humano por parte de una de nuestras funcionarias que, en su afán de informar a nuestros colaboradores de las capacitaciones desarrolladas con el único objetivo de contribuir en su propio beneficio, envió una base de datos sin contar con las adecuadas seguridades que son establecidas por nuestra entidad y resultan ser de su conocimiento, como el de todos los demás funcionarios."

- *Escrito de alegatos finales:*

Página 2. "Por otra parte, queremos ratificar que los hechos que se tratan en su requerimiento, en efecto sucedieron, somos totalmente conscientes de ello y por esto se adoptaron las diferentes medidas que fueron puestas en su conocimiento en nuestro escrito inicial y que esperamos sean tenidas en cuenta al momento de analizar esta situación."

Página 3. "Por otra parte, agradecemos que se tome en cuenta que en la situación presentada, nuestra Cámara de Comercio: a) no se buscaba, ni se obtuvo algún tipo de beneficio económico, ni de ninguna otra índole; b) Se ha aceptado plenamente la existencia del hecho implementando las medidas que puedan estar en nuestras manos para evitar una nueva ocurrencia; c) Hemos estado dispuestos a responder por las acusaciones efectuadas en contra de nuestra entidad y se ha colaborado con esa autoridad en lo que más ha podido de acuerdo con nuestro conocimiento de los hechos."

Así pues, el no haber mencionado la norma que se hubiere podido violar, como al parecer quiere indicarse dentro del documento sancionatorio, no puede resultar en el desconocimiento por parte de esa Superintendencia de la aceptación del hecho ocurrido por parte de LA CÁMARA. A esto se aúna la mención de todas las acciones de mitigación adelantadas por la entidad ¿Sino existiera un reconocimiento porque se mencionarían las acciones de mitigación para reducir los efectos adversos que con el hecho se hubieren podido causar?

Desconozco la razón de no haber tenido en cuenta el reconocimiento de la infracción cometida o ¿Acaso existe una fórmula sacramental para la aceptación de la comisión del hecho? ¿Omitió LA CÁMARA mencionar que aceptába la ocurrencia de la situación?. Sino es así, agradezco que se tome en cuenta lo hasta aquí manifestado, de manera que se haga efectiva la aplicación de está causal de atenuación de la pena impuesta."

Como consecuencia solicita lo siguiente:

"En vista de todo lo anterior, respetuosamente le solicito a la Dirección de Investigación de Protección de datos personales de la Superintendencia de Industria y Comercio que REPONGA la Resolución N° 81697 de 2020, y, en su lugar:

1.1. ANALICE las conductas de LA CÁMARA a la luz de los cargos imputados y las explicaciones brindadas, REVOCANDO los artículos primero y segundo del Resuelve de la Resolución N° 81697 de 2020.

1.2. En subsidio de lo anterior, que APLIQUE los criterios de graduación de la multa y disminuya la sanción en contra de LA CÁMARA atendiendo los argumentos puestos en su consideración y las disposiciones sobre dosificación de la sanción, MODIFICANDO el artículo primero de la Resolución N° 81697 de 2020.

En subsidio de lo anterior, solicito que se conceda el recurso de APELACIÓN en contra de la Resolución N° 81697 de 2020 y se remita el expediente al Despacho del Superintendente Delegado para la Protección de Datos Personales, con el fin de que sea el superior quien se pronuncie respecto de los argumentos aquí expuestos, que sustentan el recurso interpuesto.

QUINTO: Que mediante Resolución No. 28378 del 11 de mayo de 2021 la Dirección de Investigación para la Protección de Datos Personales, resolvió el recurso de reposición interpuesto por la CÁMARA DE COMERCIO DE BOGOTÁ**,** confirmando en todas sus partes la Resolución No. 81697 del 21 de diciembre de 2020, concediendo el recurso de apelación presentado de forma subsidiaria.

SEXTO: 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 por la CÁMARA DE COMERCIO DE BOGOTÁ (en adelante CCB), a través de su apoderado, contra la Resolución No. 81697 del 21 de diciembre de 2020 y con base en lo expuesto por la sociedad, se harán las siguientes:

CONSIDERACIONES DEL DESPACHO

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

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011[1] establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destacan las siguientes:
"(…)

[1] 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.

*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. (…)"* (Énfasis añadido)

2. DE LAS BASES DE DATOS O ARCHIVOS MANTENIDOS EN UN ÁMBITO EXCLUSIVAMENTE PERSONAL O DOMÉSTICO.

Plantea la CÁMARA DE COMERCIO DE BOGOTÁ (en adelante CCB) que la presente investigación "*parte de un hecho puntual y totalmente aislado en la dinámica de la entidad, consistente en el envío de un correo electrónico que a pesar de tratarse de una comunicación interna entre una funcionaria con su superior, resulto erróneamente dirigido a un grupo de "colaboradores-capacitadores expertos" como se han conocido al interior de la entidad, llevando lamentablemente como adjunto un archivo en formato Excel **de uso estrictamente doméstico**, el cual contenía los datos de contacto de los receptores y que **estaba siendo utilizado por parte de la funcionaria para hacer el seguimiento de la aceptación a la invitación a las capacitaciones** que pensando únicamente en el exclusivo beneficio de ellos, se les estaba cursando para la época*".(Énfasis añadido)

En el presente caso, se trata de una base de datos no excluida del ámbito de aplicación de la Ley Estatutaria 1581 de 2012 por pertenecer a una persona jurídica (CCB) que la utiliza para realizar sus actividades o funciones de capacitación.

En efecto, la Ley Estatutaria 1581 de 2012 establece:

ARTÍCULO 2o. ÁMBITO DE APLICACIÓN. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

ARTÍCULO 3o. DEFINICIONES. Para los efectos de la presente ley, se entiende por: (…)

b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;

c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

(…)

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Frente a los citados artículos, la Corte Constitucional en Sentencia C-748 de 2011 expuso:

*"El tratamiento de datos personales, en los términos que fueron definidos en el artículo 3, literal g) del proyecto en estudio, de conformidad con los recientes estándares internacionales sobre la materia **"es cualquier operación o conjunto de operaciones, sean o no automatizadas, que se apliquen a datos de carácter personal, en especial su recogida, conservación, utilización,***

> ***revelación o supresión".*** *Ese proceso de tratamiento de datos personales, que puede ser público o privado, requiere, en los términos de la jurisprudencia de esta Corporación, definiciones claras sobre "el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos." (Negrita fuera del texto)*

Como se observa, en las normas citadas anteriormente la Ley Estatutaria 1581 de 2012 no aplica a las "*bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico*". Para la Corte, la expresión "*mantenidos en un ámbito exclusivamente personal o doméstico*" no puede predicarse de las personas jurídicas ni comprende el tratamiento de datos cuando ellos circulan internamente en un una organización, gremio o grupo corporativo. Así esta Corporación manifestó:

> "*no puede entenderse que el primer contenido normativo del literal a) se extienda al tratamiento de cualquier dato cuando circule internamente, como pretende ASOBANCARIA. En primer lugar, (...) para que opere la excepción, por voluntad del legislador, se requiere además que los datos sean mantenidos por una persona natural en su esfera íntima. (...) En segundo lugar, (...)* ***El que los datos no circulen o circulen internamente, no asegura que su tratamiento no pueda tener consecuencias adversas para su titular. Piénsese por ejemplo en las hojas de vida de los empleados de una empresa mantenidas en el ámbito interno; si bien no van a ser divulgadas a terceros, su tratamiento y circulación interna sí puede traer consecuencias negativas para el titular del dato (por ejemplo, en términos sancionatorios o de ascensos), razón por la cual deben estar sujetas a las reglas generales que consagra el proyecto de ley***".[2] (Negrita fuera del texto)

Adicionalmente, el artículo 2 de decreto 1377 de 2013 (incorporado en el decreto 1074 de 2015) señala lo siguiente: "*Tratamiento de datos en el ámbito personal o doméstico. De conformidad con lo dispuesto en el literal a) del artículo 2° de la Ley 1581 de 2012, se exceptúan de la aplicación de dicha ley y del presente decreto, las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico. El ámbito personal o doméstico comprende aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales*".

En el artículo 2.2.2.25.1.2. del Decreto 1074 de 2015 se incorporó lo precisado por la Corte en el sentido de establecer que las bases de datos personales y domésticas son las de las personas naturales. No obstante, según el Decreto no basta que la base de datos sea de una persona natural, sino que ésta se utilice dentro del contexto de "la vida privada o familiar" de esa persona.

No sobra recordar que las Cámaras de Comercio no son personas naturales sino personas jurídicas, tal y como lo establece el artículo 78 del Código de Comercio.

El presente caso no se encuentra enmarcado dentro de tal escenario pues quien realiza el tratamiento no es una persona natural, ni se trata de un contexto de vida privada o familiar, se enmarca en las actividades que hacen parte del desarrollo del objeto social de la entidad. El hecho de que el documento de Excel no estuviera destinado al público, no significa que se trate de una base de datos mantenida en un ámbito exclusivamente personal o doméstico. Así, el argumento de la recurrente en este sentido no está llamado a prosperar.

En suma, la base de datos de la CCB no es de aquellas a que se refiere el literal a) del artículo 2 de la Ley Estatutaria 1581 de 2012, ni está excluida de su ámbito de aplicación, porque no es un conjunto organizado de datos personales mantenido por una persona natural en su esfera íntima, sino que se trata información que utiliza la CCB (persona jurídica) para el cumplimiento de sus funciones de capacitación.

---

[2] Corte Constitucional, sentencia C-748 de 2011, numeral 2.4.5.3.1

3. DEL PRINCIPIO Y DEL DEBER DE SEGURIDAD EN EL DEBIDO TRATAMIENTO DE DATOS PERSONALES

Sin seguridad no existe debido tratamiento de datos personales. Es por eso que la Ley Estatutaria 1581 de 2012 señala, entre otras, lo siguiente:

Literal g) del artículo 4:

> ***ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.*** *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*
> *(...)*
> *g)* ***Principio de seguridad:*** *La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

Literal d) del artículo 17:

> *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:*
> *(…)*
> *d) Conservar la información bajo las condiciones de seguridad necesarias para impedir 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 a adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información sobre las personas.

Como es sabido, la Corte Constitucional ha establecido que:

> *"Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
> *(...)*
>
> *En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. (...)*
>
> ***Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria.***"[3] *(Destacamos).*

En el caso concreto, la Cámara manifiesta que cuenta con las medidas de seguridad adecuadas para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Al respecto, manifiesta que la Dirección omitió que se cuenta con un "Manual de Lineamientos y Prácticas Gestión de seguridad de la Información". Allí se expone que la información de los archivos que requieran ser enviados

[3] Corte Constitucional. Sentencia C – 748 del 2011.

fuera de la entidad, y que por sus características de integridad deban ser protegidos, deben estar en formatos no editables o debidamente protegidos para modificaciones (contraseñas o cifrado), resaltan además que este manual es conocido y expresamente aceptado por cada uno de los funcionarios que hacen parte de la Cámara.

Argumenta además que ha realizado capacitaciones a estos colaboradores desde antes de ocurrido el incidente. Aporta el Informe de Auditoría externa realizado en 2017 en donde se observa que entre las medidas llevadas a cabo por la entidad para cumplir con el principio de responsabilidad demostrada se encuentran las capacitaciones y reuniones periódicas para este fin.

Dado lo anterior, es necesario precisar lo siguiente:

a) La seguridad de los datos personales no se logra con la mera expedición de manuales y políticas de seguridad. Es necesario pasar de la seguridad en el papel (documentos, políticas, etc) a la seguridad en la práctica.
b) La CCB efectivamente cuenta con manuales y políticas de seguridad, razón por la cual no se le sancionó por el incumplimiento del deber de "*adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley (…)*" a que se refiere el literal k) del artículo 17 de la Ley Estatutaria 1581 de 2012.
c) Proteger la información es una condición crucial para garantizar el debido tratamiento de datos personales. 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.
d) La CCB violó los deberes establecidos en el literal d) del artículo 17 de la Ley 1581 de 2012 en concordancia con lo indicado en el literal g) del artículo 4 de la misma Ley y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015, pues por medio de las acciones de uno de sus colaboradores, fueron expuestos o dados a conocer los datos personales de 413 Titulares a terceros no autorizados. Esto quedó demostrado y la Cámara no logró desvirtuar este cargo a lo largo de la presente actuación administrativa.

Es importante mencionar que la CCB manifestó lo que sigue a continuación:

- *Documento de descargos:*

Página 3. "Estimado doctor Salazar, sea lo primero indicar que, en efecto, como bien lo anuncia el denunciante, en la fecha por él indicada le fue remitido un correo electrónico con la información que manifiesta haber sido incorporada, error operativo que de ninguna manera podría obviar o dejar de aceptar."

Página 4. "Sí, en efecto. Como ya tuve ocasión de mencionar y aceptar desde un principio, el error endilgado por el denunciante fue cometido por parte de una de las auxiliares de nuestro equipo, quien en el afán de seguir las instrucciones de convocar a los miembros de nuestra comunidad a las capacitaciones que teníamos preparadas para ellos, tomó un archivo en formato Excel de circulación absolutamente restringida como lo pudo apreciar en el cuadro de privilegios en el manejo de la información que allegamos en la respuesta enviada el día 19 de marzo de 2019, al que más adelante haré nuevamente referencia, y lo remitió a los convocados, omitiendo eliminar dentro del mismo los datos correspondientes a su información de contacto."

Página 12 "1. Se presentó un error humano por parte de una de nuestras funcionarias que, en su afán de informar a nuestros colaboradores de las capacitaciones desarrolladas con el único objetivo de contribuir en su propio beneficio, envió una base de datos sin contar con las

adecuadas seguridades que son establecidas por nuestra entidad y resultan ser de su conocimiento, como el de todos los demás funcionarios."

- *Escrito de alegatos finales:*

Página 2. "Por otra parte, queremos ratificar que los hechos que se tratan en su requerimiento, en efecto sucedieron, somos totalmente conscientes de ello y por esto se adoptaron las diferentes medidas que fueron puestas en su conocimiento en nuestro escrito inicial y que esperamos sean tenidas en cuenta al momento de analizar esta situación."

En el presente caso, la falla de seguridad no solo se originó por error o negligencia humana sino porque el archivo que contenía la información de 413 personas no tenía ningún tipo de seguridad técnica para que, en caso que el mismo llegará a destinatarios no deseados, ellos no pudiesen ver el contenido. Por ejemplo, la CCB no utilizó un documento cifrado con clave de acceso (cifrado de archivos) para que, en casos como el presente, un destinatario que recibe el documento por equivocación no pueda ver el contenido del mismo.

Esto último (cifrado de archivos) también es relevante para los documentos de circulación interna en la entidad porque no todas las personas de la misma deben tener acceso a los datos personales de terceros y porque en caso de que, por error, se envíe esa base de datos a terceros pues ello ayudará a impedir que tengan acceso no autorizado a los datos personales de 413 personas.

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

Nuestra la regulación 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*"[4] y a "*conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*[5]. 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"*[6]*.*

Nótese que la norma impone una carga probatoria en cabeza de los Responsables de probar que adoptado las medidas citadas para cumplir los ordenado por dicha ley. En este caso, como se mencionó, el principio y el deber de seguridad tiene un criterio eminentemente preventivo, lo cual obliga a las organizaciones a poner en marcha medidas técnicas, humanas, administrativas y de cualquier otra índole para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a los datos personales[7]. Pero, adicionalmente, es imprescindible que se esté efectuando un monitoreo o seguimiento permanente para asegurar que dichas medidas se aplican en la práctica y son útiles.

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

---

[4] Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012
[5] Cfr. Literal d) del artículo 17 de la Ley Estatutaria 1581 de 2012
[6] Cfr. Artículo 26 del decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015)
[7] Cfr. Literal g) del artículo 4 de la Ley 1581 de 2012

"*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*."[8] (Destacamos)

Así las cosas, la recurrente tiene el deber de demostrar que adoptó medidas de seguridad apropiadas, útiles y eficientes. En este caso, como se expuso, la CCB no sólo cuenta con un Manual de Lineamientos y Prácticas Gestión de seguridad de la Información, sino que ha realizado capacitaciones sobre dicho tema. No obstante, en la presente actuación se puso de presente que ello fue insuficiente para impedir que terceros conocieran o accedieran sin autorización a los datos personales de 413 personas.

De esta manera, según los documentos que obran en el expediente, el procedimiento para el incidente de seguridad presentado era el siguiente:[9]

[8] 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
[9] Expediente digital 18-193960, hoja 25, página 16 folio 10.

?

cámara

Inicio Para mi trabajo Lo que nos mueve Cultura productiva Noticias CCB

lcámara > Noticias > Gestión de Riesgos

+like +comentado

7 días 30 días Siempre

Gestión de Riesgos

Publicado el, 10/05/2018

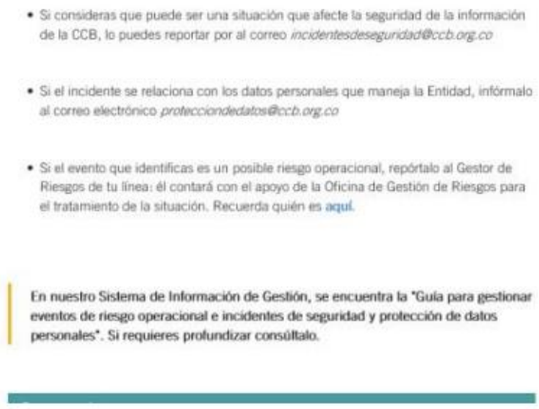
¿Sábes qué es un evento o incidente cuando hablamos de gestión de riesgos? Aquí te contamos cómo identificarlos y reportarlos.

En Nuestra Casa de manera permanente trabajamos para identificar riesgos operacionales, de seguridad de la información y protección de datos que puedan materializarse en eventos o incidentes.

Te contamos a que se refiere cada uno:

- **Eventos de riesgo operacional:** Se refiere a las posibles fallas o deficiencias en un proceso que pueda impedir el logro de su objetivo, con posibles consecuencias económicas, reputacionales, humanas o reprocesos. Ejemplo: registro de información errada o incompleta en formularios o sistemas o incumplimiento de proveedores u operadores.
- **Incidentes de seguridad de la información**: Son situaciones que afectan la disponibilidad, confidencialidad e integridad de la información de la Entidad. Ejemplo: pérdida o robo de un computador, modificación de un archivo de trabajo por un tercero no autorizado, recepción de un correo sospechoso, presencia de virus informático en equipos de trabajo, entre otras.
- **Incidentes de protección de datos personales:** Son situaciones que afectan el manejo y el tratamiento de los datos personales de colaboradores, empresarios y terceros, a los que tiene acceso la Entidad. Ejemplo: enviar comunicaciones institucionales a clientes que hayan pedido no enviarles y sin usar los canales establecidos, uso de datos para finalidades distintas a las autorizadas por el usuario o solicitud de datos no necesarios para un evento o sin autorización previa, entre otros.

Es responsabilidad de todos los colaboradores de Nuestra Casa identificar eventos o incidentes de riesgos y saber cómo reportarlos. Para esto tenemos varios canales:



- Si consideras que puede ser una situación que afecte la seguridad de la información de la CCB, lo puedes reportar por al correo *incidentesdeseguridad@ccb.org.co*
- Si el incidente se relaciona con los datos personales que maneja la Entidad, infórmalo al correo electrónico *protecciondedatos@ccb.org.co*
- Si el evento que identificas es un posible riesgo operacional, repórtalo al Gestor de Riesgos de tu línea: él contará con el apoyo de la Oficina de Gestión de Riesgos para el tratamiento de la situación. Recuerda quién es aquí.

En nuestro Sistema de Información de Gestión, se encuentra la "Guía para gestionar eventos de riesgo operacional e incidentes de seguridad y protección de datos personales". Si requieres profundizar consúltalo.

Efectivamente, como afirma la recurrente, puede suceder que el colaborador intercambie comunicaciones con su superior jerárquico sobre el incidente. Si bien es importante estar preparados para un incidente de seguridad, en este caso la falla fue no haber adoptado las medidas necesarias la impedir el acceso indebido a autorización a los datos personales de 413 personas.

Se reitera que el cumplimiento del principio de responsabilidad demostrada no debe limitarse a que los procesos o documentos estén elaborados y disponibles para consulta de los colaboradores de la CÁMARA DE COMERCIO DE BOGOTÁ, o que sean aceptados por ellos. Es perentorio que las medidas de seguridad se apliquen e implementen de manera efectiva por todos los miembros de la entidad.

Ahora, este Despacho considera necesario hacer las siguientes precisiones adicionales sobre el principio de responsabilidad demostrada:

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*"[10].

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

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

[11] 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.

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

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)"[12]. 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[13] para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los Responsables 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

---

3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas"

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

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

políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones.

El principio de responsabilidad demostrada busca que los mandatos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las organizaciones sean proactivos respecto del tratamiento de la información de manera que por iniciativa propia adopten medidas estratégicas 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, ponemos de presente que el principio de responsabilidad demostrada se articula con el concepto de "compliance" en la medida que éste 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"*[14].

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)"*[15]. 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"[16].

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"*[17] 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"*[18].

5. DEBIDO PROCESO Y DEL REQUISITO DE PROCEDIBILIDAD DEL ARTÍCULO 16 DE LA LEY ESTATUTARIA 1581 DE 2012.

La CCB manifiesta que conforme al articulo16 de la Ley 1581 de 2012, el Titular solo podrá

---

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

[15] 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/

[16] Idem

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

[18] Ibid. P 16

elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento.

Dicha norma establece lo siguiente: "*ARTÍCULO 16. REQUISITO DE PROCEDIBILIDAD. El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento*."

Como se observa, dicha norma no impide que esta entidad inicie procesos sancionatorios porque lo señalado en el artículo 16 de la Ley 1581 de 2012 está relacionado con el ejercicio de las consultas y reclamos de los titulares de los datos que tienen por objeto consultar la información personal o solicitar su corrección, actualización o supresión, tal y como lo indican los artículos 14 y 15 de la precitada ley.

La presente actuación está asociada con la potestad sancionatoria de esta Delegatura que le permite de manera oficiosa adelantar las investigaciones correspondientes para verificar el cumplimiento de la Ley Estatutaria 1581 de 2012. En efecto, tanto el literal b) del artículo 21 de dicha ley, como el artículo 47 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Ley 1437 de 2011) ordenan lo siguiente:

> **"*ARTÍCULO 21. FUNCIONES.*** *La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:*
>
> *(…)*
>
> *"b) Adelantar las investigaciones del caso,* ***de oficio*** *o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos*; (…)" (Énfasis añadido)
>
> *ARTÍCULO 47. PROCEDIMIENTO ADMINISTRATIVO SANCIONATORIO. (…).*
>
> *Las actuaciones administrativas de naturaleza sancionatoria* ***podrán iniciarse de oficio o por solicitud de cualquier persona****. Cuando como resultado de averiguaciones preliminares, la autoridad establezca que existen méritos para adelantar un procedimiento sancionatorio, así lo comunicará al interesado. (…)".* (Énfasis añadido)

Adicionalmente, el artículo 22 dispone lo que sigue a continuación:

> *"ARTÍCULO 22. TRÁMITE. 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."* (Énfasis añadido)

El artículo 16 hace parte del Título V de la citada Ley Estatutaria 1581 de 2012, el cual hace referencia a los procedimientos para las consultas o reclamos ante los Responsables y Encargados del Tratamiento. Se trata entonces del procedimiento a seguir cuando los Titulares o sus causahabientes deseen consultar la información personal del Titular que repose en cualquier base de datos,[19] o que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan

[19] Ley 1581 de 2012 artículo14.

el presunto incumplimiento de cualquiera de los deberes contenidos en la ley.[20]

Así las cosas, el precitado artículo no impide que esta entidad pueda iniciar de oficio o a petición de parte, investigaciones administrativas para establecer eventuales irregularidades en el tratamiento de datos personales. En otras palabras, esta Delegatura puede iniciar investigaciones sin que sea necesario que el Titular del dato agote el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

Respecto de la "potestad sancionatoria", la Corte Constitucional ha señalado, entre otras, lo que sigue a continuación:

> *"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 medios 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 otros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (iv) El principio de proporcionalidad que se traduce en que la sanción debe ser proporcional 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".*[21]

Así, la Superintendencia de Industria y Comercio, en ejercicio de sus facultades legales, puede iniciar investigaciones administrativas, a petición de parte, tendientes a establecer si hay lugar o no a la imposición de una sanción en aras de preservar el orden jurídico y proteger los derechos de las personas.

El debido proceso se respetó toda vez que existe un procedimiento establecido que garantiza el derecho de defensa e incluye la designación expresa de una autoridad competente para imponer la sanción. En este caso, la Dirección de Investigación de Protección de Datos Personales.

La Superintendencia de Industria y Comercio obró dentro del marco de sus facultades legales para, de una parte, garantizar a las personas el derecho fundamental de la protección de datos personales y, de otra, respetar el debido proceso en cabeza de CCB. En línea con lo anterior, tanto la investigación administrativa como la sanción impuesta se hicieron observando lo que ordena la regulación colombiana.

Al respecto, este Despacho advierte que en ningún momento los actos o actuaciones de esta Delegatura han estado en contravía del Derecho. Esta entidad aplicó y respetó las garantías procesales necesarias, y en todas las etapas respectivas se emitieron las resoluciones y actos administrativos a que hubo lugar. Los que en ninguna circunstancia fueron arbitrarios. Por lo expuesto previamente, no tiene razón la recurrente cuando afirma que se configuró una violación al debido proceso: primero, por cuanto la Superintendencia de Industria y Comercio sí puede realizar una investigación de oficio tendiente a establecer la infracción de una disposición legal. Segundo, no se desvirtuó por el recurrente el respeto de los postulados

---

[20] Ley 1581 de 2012 artículo15.
[21] Corte Constitucional. Sentencia C-748 de 2011.

que el debido proceso enmarca. Y, tercero, confunde la recurrente el ejercicio del derecho de *protección de datos personales* que le asiste al quejoso con la facultad de investigación, control y vigilancia en cabeza de la Superintendencia de Industria y Comercio.

Visto lo anterior, la Dirección de Investigación de Protección de Datos Personales siguió los procedimientos establecidos para, posteriormente, en virtud de las funciones otorgadas a esta Superintendencia por el artículo 21 de la Ley 1581 de 2012, adelantar la investigación correspondiente. Por lo que no se acogerá el argumento presentado por la recurrente.

En síntesis, lo señalado en el artículo 16 de la Ley Estatutaria 1581 de 2012 no es un requisito de procedibilidad para que esta entidad inicie un proceso administrativo sancionatorio. Por ende, no se ajustan a derecho los argumentos de la recurrente.

6. DE LA GRADUACIÓN Y PROPORCIONALIDAD DE LA SANCIÓN.

Según la Corte Constitucional, "*es innegable que a través del derecho administrativo sancionador se pretende garantizar la preservación y restauración del ordenamiento jurídico, mediante la imposición de una sanción que no sólo repruebe sino que también prevenga la realización de todas aquellas conductas contrarias al mismo. Se trata, en esencia, de un poder de sanción ejercido por las autoridades administrativas que opera ante el incumplimiento de los distintos mandatos que las normas jurídicas imponen a los administrados y aún a las mismas autoridades públicas*"[22].

A lo largo de la presente actuación administrativa se logró demostrar que la sociedad vulneró los deberes establecidos en el literal d) del artículo 17 de la Ley 1581 de 2012 en concordancia con lo establecido en el literal g) del artículo 4 de la misma Ley y el artículo 2.2.2.25.6.1 del Decreto único Reglamentario 1074 de 2015, al probarse dentro de la actuación administrativa que por medio de la conducta investigada la CÁMARA DE COMERCIO DE BOGOTÁ vulneró el principio y el deber de seguridad de la información.

Ahora, el artículo 23[23] de la Ley Estatutaria 1581 de 2012 determina las sanciones que puede imponer esta Superintendencia a los Responsables y Encargados del Tratamiento. Revisado el expediente y el contenido de la resolución recurrida, se encuentra entonces que de los criterios de graduación contenidos en el artículo 24 de la Ley Estatutaria 1581 de 2012, **únicamente** se tuvo en cuenta aquél que habla de la dimensión del daño o peligro a los intereses jurídicamente tutelados, pues efectivamente se encontró probado que la CÁMARA DE COMERCIO DE BOGOTÁ, incumplió los deberes mencionados.

Así las cosas, se encuentra que el monto de la sanción en el citado acto administrativo es proporcional, en consideración a los hechos que le sirvieron de causa y la motivación del acto administrativo recurrido. No sobra señalar que la sanción aquí impuesta, tiene como

---

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

[23] "**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;
Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva".

objetivo que la investigada en el futuro no incurra en violaciones al derecho de hábeas data de los Titulares de la información y, en su defecto, cumpla a cabalidad con las disposiciones de la Ley Estatutaria 1581 de 2012 y demás normas que rigen el sistema de protección de datos personales en Colombia.

Finalmente, resulta pertinente resaltar lo siguiente:

I. La multa de $80.008.929 equivale al 4,55% 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 Estatutaria 1581 de 2012 a los Responsables 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, también fue el resultado de la valoración fáctica y probatoria de la primera instancia que llevó a concluir y comprobar la vulneración al derecho de *habeas data* del Titular y en particular los mandatos legales señalados.

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

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"*[24]. 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[25]. 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.

---

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

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

7. DEL RECONOCIMIENTO O ACEPTACIÓN EXPRESOS SOBRE LA COMISIÓN DE LA INFRACCIÓN.

Según la CCB, esta entidad no aplicó el criterio de atenuación previsto en el literal f) del artículo 24 de Ley Estatutaria 1581 de 2012. Manifiesta lo siguiente luego de traer a colación algunos apartes del documento de descargos y de los alegatos finales transcritos en este acto administrativo:

> *Así pues, el no haber mencionado la norma que se hubiere podido violar, como al parecer quiere indicarse dentro del documento sancionatorio, no puede resultar en el desconocimiento por parte de esa Superintendencia de* ***la aceptación del hecho ocurrido por parte de LA CÁMARA****. A esto se aúna la mención de todas las acciones de mitigación adelantadas por la entidad ¿Sino existiera un reconocimiento porque se mencionarían las acciones de mitigación para reducir los efectos adversos que con el hecho se hubieren podido causar?*
>
> *Desconozco la razón de no haber tenido en cuenta el reconocimiento de la infracción cometida o* ***¿Acaso existe una fórmula sacramental para la aceptación de la comisión del hecho?*** *¿Omitió LA CÁMARA mencionar que aceptába la ocurrencia de la situación?. Sino es así, agradezco que se tome en cuenta lo hasta aquí manifestado, de manera que se haga efectiva la aplicación de está causal de atenuación de la pena impuesta."*

Sobre el particular, ordena la norma en comento lo siguiente:

> *ARTÍCULO 24. CRITERIOS PARA GRADUAR LAS SANCIONES. Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:*
> *(…)*
> *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, dicha norma no exige ninguna fórmula sacramental -*como lo pregunta la CCB*- para que se tenga en cuenta el atenuante previsto es el literal f). Sólo pide que de manera expresa se reconozca o acepte la comisión de la infracción. En el presente caso, la CCB reconoció la veracidad de los hechos que dieron origen a la actuación administrativa, pero **no aceptó expresamente la comisión de la infracción** antes de la imposición de la sanción.

No es lo mismo reconocer o admitir la veracidad de los hechos, que aceptar expresamente la comisión de la infracción señalada en el pliego de cargos.

Así las cosas, no son de recibo los argumentos de la CCB para que se le aplique el atenuante mencionado.

Con apoyo en estos argumentos, se confirmará en todas sus partes la Resolución No. 81697 del 21 de diciembre de 2020.

8. CONCLUSIONES:

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

1. La base de datos de la CCB no es de aquellas a que se refiere el literal a) del artículo 2 de la Ley Estatutaria 1581 de 2012, ni está excluida de su ámbito de aplicación, porque no es un conjunto organizado de datos personales mantenido por una persona

natural en su esfera íntima, sino que se trata información que utiliza la CCB (persona jurídica) para el cumplimiento de sus funciones de capacitación.

2. La CCB 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 lo establecido en el literal g) del artículo 4 de la misma Ley y el artículo 2.2.2.25.6.1 del Decreto único Reglamentario 1074 de 2015.

3. La seguridad de los datos personales no se logra con la mera expedición de manuales y políticas de seguridad. Es necesario pasar de la seguridad en el papel (documentos, políticas, etc) a la seguridad en la práctica.

4. En el presente caso, la falla de seguridad no solo se originó por error o negligencia humana sino porque el archivo que contenía la información de 413 personas no tenía ningún tipo de seguridad técnica para que, en caso que el mismo llegará a destinatarios no deseados, ellos no pudiesen ver el contenido. Por ejemplo, la CCB no utilizó un documento cifrado con clave de acceso (cifrado de archivos) para que, en casos como el presente, un destinatario que recibe el documento por equivocación no pueda ver el contenido del mismo.

   Esto último (cifrado de archivos) también es relevante para los documentos de circulación interna en la entidad porque no todas las personas de la misma deben tener acceso a los datos personales de terceros y porque en caso de que, por error, se envíe esa base de datos a terceros pues ello ayudará a impedir que tengan acceso no autorizado a los datos personales de 413 personas.

5. Lo señalado en el artículo 16 de la Ley Estatutaria 1581 de 2012 no es un requisito de procedibilidad para que esta entidad inicie un proceso administrativo sancionatorio. Las actuaciones administrativas de naturaleza sancionatoria pueden iniciarse de oficio o por solicitud de cualquier persona. La presente actuación está asociada con la potestad sancionatoria de esta Delegatura que le permite de manera oficiosa adelantar las investigaciones correspondientes para verificar el cumplimiento de la Ley Estatutaria 1581 de 2012.

6. La Ley Estatutaria 1581 de 2012 no exige ninguna fórmula sacramental *-como lo pregunta la CCB-* para que en la graduación de la sanción se tenga en cuenta el atenuante previsto en el literal f) del artículo 24. Sólo pide que de manera expresa se reconozca o acepte la comisión de la infracción. En el presente caso, la CCB reconoció la veracidad de los hechos que dieron origen a la actuación administrativa, pero no aceptó expresamente la comisión de la infracción antes de la imposición de la sanción.

7. No es lo mismo reconocer o admitir la veracidad de los hechos, que aceptar expresamente la comisión de la infracción señalada en el pliego de cargos.

8. La multa de $80.008.929 equivale al 4,55% del máximo legal permitido (2000 salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012).

9. La regulación colombiana sobre tratamiento de datos impone al Responsable del Tratamiento el deber demostrar que ha adoptado medidas efectivas para cumplir la ley (Deber de Responsabilidad demostrada). Según la Corte Constitucional, *“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. 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. (…)" (C-32 de 2021)

En razón de lo expuesto, este Despacho procederá a confirmar la Resolución No. 81697 del 21 de diciembre de 2020.

SEPTIMO: Que, analizada la cuestión planteada, y teniendo en cuenta lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirmará la decisión contenida en la Resolución No. 81697 del 21 de diciembre de 2020.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO: Confirmar la Resolución No. 81697 del 21 de diciembre de 2020 de conformidad con lo expuesto en la parte motiva de la presente resolución.

ARTÍCULO SEGUNDO: Notificar personalmente el contenido de la presente resolución a CÁMARA DE COMERCIO DE BOGOTÁ, identificada con el NIT. 860.007.322-9, 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.

ARTÍCULO TERCERO: Comunicar la presente decisión al señor [redacted], identificado con la cédula de ciudadanía No. [redacted]

ARTÍCULO CUARTO: 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., noviembre 26 de 2021

El Superintendente Delegado para la Protección de Datos Personales

NELSON REMOLINA ANGARITA

Firmado digitalmente por NELSON REMOLINA ANGARITA
Fecha: 2021.11.26 14:23:46 -05'00'

NELSON REMOLINA ANGARITA

MPM/MEG

NOTIFICACIÓN:

Sociedad: CÁMARA DE COMERCIO DE BOGOTÁ
Identificación: Nit. 860.007.322-9
Representante legal: Nicolás Uribe Rueda
Identificación: CC. 79.944.552
Dirección: Avenida El Dorado No. 68 D – 35 piso 8°
Ciudad: Bogotá D.C.
Correo electrónico: notificacionesjudiciales@ccb.org.co

Apoderado: José Ignacio Pedro Elías Novoa Serrano
Identificación: C.C. 79.592.192 T.P. 100.709 del CSJ

COMUNICACIÓN:

Nombre: [redacted]
Identificación: C.C. No. [redacted]
Correo electrónico: [redacted]
Dirección: [redacted]
Ciudad: [redacted]