REPUBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 28378 DE 2021

(11 MAYO 2021)

VERSIÓN PÚBLICA

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

Radicación 18-193960

EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por el artículo 21 de la Ley 1581 de 2012, el numeral 8 del artículo 17 del Decreto 4886 de 2011 y

CONSIDERANDO

PRIMERO: Que mediante Resolución 81697 del 21 de diciembre de 2020, la Dirección de Investigación de Protección de Datos Personales resolvió:

> *"**ARTÍCULO PRIMERO:** Imponer una sanción pecuniaria a la **CÁMARA DE COMERCIO DE BGOTÁ** (sic) 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.*
>
> *(…)*
>
> ***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".*

SEGUNDO: Que la Resolución 81697 del 21 de diciembre de 2020 se notificó electrónicamente, a la **CÁMARA DE COMERCIO DE BOGOTÁ**, el día mencionado, según consta en la certificación expedida por la Secretaría General de esta Superintendencia, radicada bajo el número 18-193960--27 del 20 de enero de 2021.

TERCERO: Que, dentro del término concedido para el efecto, mediante escrito radicado bajo el número 18-193960-26-1 del 05 de enero de 2021, la **CÁMARA DE COMERCIO DE BOGOTÁ**, a

través de apoderado especial, interpuso recurso de reposición y en subsidio de apelación en contra de la Resolución 81697 del 21 de diciembre de 2020, el cual fundamentó en los siguientes motivos:

3.1 En primer lugar, hace referencia a unos aspectos preliminares, los cuales se sintetizan a continuación:

El recurrente reafirma el compromiso de la Cámara de Comercio de Bogotá en el cumplimiento de las normas de protección de datos y el acatamiento de las decisiones de esta Superintendencia. Igualmente, manifiesta que, la Cámara de Comercio de Bogotá ha asumido un papel protagónico en materia de protección de la información e, incluso, ofrece capacitaciones para el desarrollo de programas de privacidad.

No obstante, señala que existe la posibilidad de ocurrencia de hechos que resultan absolutamente aislados y, que, de acuerdo con los parámetros de cuidado, se han realizado auditorías, las cuales permiten concluir que los aspectos tratados en la documentación pertinente se convierten en acciones verificables.

3.2 Posteriormente, señala que la actuación iniciada por esta Superintendencia en contra de la Cámara de Comercio de Bogotá tuvo origen en un hecho puntual y totalmente aislado a la dinámica de la entidad.

Sobre este punto, asevera que, el archivo en formato Excel era estrictamente para uso doméstico y estaba siendo utilizado por la funcionaria, con el propósito de realizar el seguimiento a una invitación a capacitaciones que se encontraban en curso para la época.

Asimismo, sostiene que el hecho que dio origen a la presente investigación se trata "*de un hecho puntual y totalmente aislado en la dinámica de la entidad*"[1] y que el mismo pudiese haber pasado desapercibido, dado que, los receptores del mensaje de correo electrónico, a través del cual se revelaron datos personales de cuatrocientas trece (413) personas, se conocen entre sí.

Considera la sociedad investigada que, el denunciante, pretermitiendo el conducto regular prescrito en el artículo 15 de la Ley 1581 de 2012, puso en conocimiento de esta Superintendencia el asunto consistente en la remisión de un correo electrónico en el que se adjuntaba una base de datos de conferencistas que incorporaba 413 registros con nombres completos, celulares, teléfonos, correos electrónicos y cursos con fechas.

3.3 A continuación, el recurrente realiza la sustentación de los motivos de inconformidad con la decisión adoptada por esta entidad, así:

Frente al deber de conservar la información bajo medidas de seguridad, expresa que, *"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"*[2].

Sin embargo, manifiesta su discrepancia frente a lo indicado en torno a la falta de verificación en la práctica de las medidas establecidas por la Cámara de Comercio de Bogotá para la custodia de la información, así como a la falta de adopción de medidas de seguridad para los archivos compartidos por la sociedad investigada. Sobre el particular, afirma que se omitió valorar *"el origen del archivo, su objetivo y su transitoria existencia"*[3]. Además, resalta que el archivo carecía de cualquier vocación circulatoria interna o externa y su utilización era absolutamente restringida.

Señala que, sin ninguna duda, el archivo, como el que hoy es objeto de cuestionamiento, no requiere las seguridades propuestas en el acto administrativo recurrido, debido a que, es un archivo temporal, de circulación restringida, cuya esencia consiste en que sea editable, modificable y sujeto a actualización por parte del funcionario que los trata. Por lo cual, declara que los argumentos en torno a las medidas de seguridad no resultan apropiados para la medición de la responsabilidad de la Cámara de Comercio de Bogotá.

---

[1] Radicado 18-193960-26-1, página 2
[2] Radicado 18-193960-26-1, página 4.
[3] Radicado 18-193960-26-1, página 5.

Luego, hace referencia a la presunta omisión probatoria por parte de esta Superintendencia, aseverando que, la Cámara cuenta con documentación en materia de protección de datos personales, la cual es conocida y expresamente aceptada por cada uno de los funcionarios que hacen parte de la entidad. En el mismo sentido, manifiesta que no es de su recibo el argumento de esta Superintendencia, en relación con la inexistencia de pautas para evitar el uso, acceso o consulta no autorizada, debido a que "*sí existían para el tiempo en que se presentaron los hechos materia de investigación y que eran de obligatoria aplicación por parte de toda la planta de personal de la Cámara*"[4].

Además, señala que desconoce que llevó a este Despacho a considerar que las acciones analizadas en el acto administrativo recurrido eran las únicas acciones en materia de capacitaciones y divulgación de la información que había adoptado y realizado la entidad, alegando que el contenido de la documentación aportada con la respuesta otorgada por la Cámara, con anterioridad a la formulación de cargos, se evidencia que estos no son las únicas medidas implementadas.

En línea con lo anterior, hace alusión a las múltiples capacitaciones que le permiten a la entidad 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, tal y como asegura lo prueba el informe de la auditoría externa realizada por la firma Ernst & Young del año 2017. De forma que, para demostrar sus afirmaciones, aporta copia de la documentación que contiene las acciones de formación realizadas en el segundo semestre de 2017 y el primer semestre de 2018.

3.4 Continúa, haciendo referencia al principio de responsabilidad demostrada, así:

Inicia este acápite, señalando que esta Superintendencia basa su conclusión de incumplimiento del principio de responsabilidad demostrada por parte de la Cámara en dos puntos principales: (i) la entidad no tomó las acciones pertinentes para que el personal de esta conociera el protocolo de violaciones e incidentes y actuara de conformidad y (ii) la Cámara no puso en práctica medidas para la mitigación de los riesgos que conlleva el tratamiento de datos personales.

Sobre el particular, el recurrente manifiesta su desacuerdo y afirma que es precisamente a partir del material probatorio allegado que se acredita que la Cámara, además de contar con toda una serie de políticas para el tratamiento de la información, las ponía en conocimiento de todos sus funcionarios.

Indica que, resulta apenas lógico que, a pesar de los protocolos y directrices existentes, la funcionaria que remitió el correo electrónico el día 17 de julio de 2018 comunicara lo sucedido a su superior jerárquica con el fin de pedir su direccionamiento. A su vez, señala que la forma en que procedió la funcionaria evitaría molestias derivadas de un actuar por cuenta propia, así fuera siguiendo los protocolos por todos conocidos. Sobre este punto, se apoya en su insistencia de que el documento de seguridad, cuya lectura, comprensión y suscripción se hizo obligatoria al momento de la contratación de la funcionaria y que, por ello, la misma sabía cómo proceder. Igualmente, hace referencia a las constantes tareas de capacitación en las diferentes materias que tienen que ver con privacidad y seguridad de la información.

Finalmente, sobre este punto, solicita un análisis del acervo probatorio que da muestra de las acciones que se han tomado por parte de la Cámara, en aras de impedir que por parte de los 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 paras adelantar las acciones institucionales más pertinentes.

3.5 Posteriormente, plantea una presunta inobservancia de los requisitos de procedibilidad para el inicio de actuaciones ante la Superintendencia de Industria y Comercio. Al respecto, advierte que la desatención de estos requisitos 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 un desgaste en materia operativa y económica.

---

[4] Radicado 18-193960-26-1, página 7.

La segunda, para la propia autoridad administrativa, en cuanto genera un movimiento del recurso institucional que, podría dedicarse a resolver cuestiones relevantes, en lugar de concentrar su capacidad operacional en casos que pueden ser atendidos y resueltos por las partes involucradas[5].

3.6 En cuanto al presunto desconocimiento de la existencia de una causal disminución de la pena, sostiene que la sociedad investigada no solo aceptó la existencia del hecho, sino que, en repetidas ocasiones hizo alusión al error operativo e involuntario, presentando, además, las acciones de mitigación efectuadas a partir de su reconocimiento. Con el propósito de soportar su argumento, trae a colación algunos apartes del escrito de descargos y de alegaciones de conclusión.

3.7 Finaliza su escrito, solicitando que, se analicen las conductas y se revoquen los artículos primero y segundo de la parte resolutiva del acto administrativo en cita.

Subsidiariamente, solicita la aplicación de los criterios de graduación de la sanción, disminuyendo el monto de la multa impuesta a la Cámara de Comercio y, en consecuencia, se modifique el artículo primero de la Resolución 81697 del 21 de diciembre de 2020.

Por último, solicita que se conceda el recurso de apelación 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 que sustentan el recurso interpuesto.

CUARTO: Competencia de la Superintendencia de Industria y Comercio

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

QUINTO: Que una vez revisado el cumplimiento de los requisitos establecidos en el artículo 77 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo y con base en lo expuesto por el recurrente, este Despacho procede a realizar las siguientes consideraciones, teniendo en cuenta que los argumentos del recurrente se enmarcan en los siguientes puntos (i) 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; (ii) Frente a la aplicación del principio de responsabilidad demostrada; (iii) Frente a la inobservancia de los requisitos de procedibilidad; (iv) Frente a las causales de graduación de la sanción y (v) frente a las pretensiones:

5.1 Sobre el deber de conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

Para efectos de procedimiento, este acápite se dividirá en dos partes, el primero tendiente a analizar el error alegado por el recurrente y otro para analizar las características del archivo remitido.

5.1.1. Frente al error operativo alegado por la recurrente

El recurrente inicia el recurso manifestando que el hecho que dio origen a la presente investigación versa "*de un hecho puntual y totalmente aislado en la dinámica de la entidad*"[6] y que el mismo pudiese haber pasado desapercibido, dado que, los receptores del mensaje de correo electrónico, a través del cual se revelaron datos personales de cuatrocientas trece (413) personas, se conocen entre sí

Igualmente, sostiene que, "*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*"[7].

Al respecto, para esta Dirección, el hecho de que lo sucedido sea catalogado por el recurrente como una situación "*puntual, aislada y que incluso hubiese pasado desapercibida*", no desvirtúa la

[5] Radicado 18-193960-26-1, página 13.
[6] Radicado 18-193960-26-1, página 2
[7] Radicado 18-193960-26-1, página 4.

violación al Régimen de Protección de Datos Personales, que en este caso se materializó el día 17 de julio de 2018, cuando una funcionaria de la **CÁMARA DE COMERCIO DE BOGOTÁ**, estando en ejercicio de sus funciones, remitió vía correo electrónico, una base de datos en formato editable realizaba mediante el programa Excel que contenía información referente a nombres y apellidos, número celular, número de teléfono fijo y correo electrónico de cuatrocientas trece (413) personas.

Además de lo anterior, para este Despacho, este tipo de situaciones no pueden ser normalizadas, ni aceptadas, como se deduce de las argumentaciones del recurrente cuando afirma que este *"(…) 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 (…)*"[8], ya que de forma indistinta a la entidad en la que se generen estas situaciones las mismas suponen una clara violación de la Ley que esta entidad está encargada de proteger.

La anterior cita, propia del recurso y de la actitud de la Cámara de Comercio, que aunque afirme que es respetuosa del Régimen General de Protección de Datos Personales, solo denota con su conducta, al pretender que la misma pueda pasar desapercibida, que se produzca una violación al régimen mencionado y que la misma, supone que, por más de que hayan implementado y documentado manuales y procedimientos tendientes a la protección de los datos personales, evidencia que los mismos resultan deficientes en su aplicación.

Adicionalmente, contrario a lo afirmado por el recurrente, es frecuente que el error humano se constituya como causa primigenia de incidentes de seguridad asociados a datos personales; razón por la cual, resulta imperioso ir más allá de la deficiente justificación otorgada por la sociedad investigada y, en su lugar, propender por la real demostración de las múltiples herramientas documentales con la que cuenta la Cámara en el ejercicio práctico, de forma que si es posible que la Cámara pueda prever este tipo de situaciones y se mitiguen los riesgos de un incidente, estableciendo controles de acceso y de circulación estricta de la documentación interna en la entidad.

En este punto, se cuestiona este Despacho si más allá de la aceptación de la documentación, que se entiende con la suscripción del contrato de trabajo, los funcionarios de la Cámara aplican lo que se entiende aceptado tanto en la documentación que les es entregada, como en los protocolos que alega existen al interior de la entidad, ya que es claro que la actuación de la funcionaria no está acorde con los propios procedimientos que ha dispuesto e implementado la Cámara de Comercio.

En este punto, resulta necesario traer a colación apartes de la sentencia C-748 de 2011 de la Corte Constitucional, sobre el principio y deber de seguridad[9]:

> "*(…)*
>
> ***Principio de seguridad:*** *Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
>
> *De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto "diluvio de datos", a través del cual día a día la masa de datos personales existente, objeto de tratamiento y de ulterior transferencias, no cesa de aumentar. Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riegos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre.*

---

[8] Radicado 18-193960-26-1, página 2.

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

En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales" o "SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de "parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos".

Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria.

(…)"

En línea con lo expuesto, conviene resaltar que, no es del recibo de esta Dirección la afirmación del recurrente en referencia a que el hecho objeto de investigación pudo incluso haber pasado desapercibido; máxime si se tiene en cuenta que:

1. La Ley Estatutaria 1581 de 2012 contempla el deber de los Responsables de informar a la autoridad de protección de datos situaciones como la acontecida en el caso objeto de estudio (incidentes de seguridad).

2. La Cámara afirma contar con un protocolo para la gestión de incidentes de protección de datos personales que, en teoría, facilitaría la detección y respuesta por parte de sus funcionarios ante cualquier incidente que afecte la confidencialidad, disponibilidad e integridad de los datos personales bajo su protección; protocolo que, por lo evidenciado a partir del material probatorio obrante en el expediente, no es de aplicación absoluta por parte del personal de la recurrente.

   Igualmente, no se avizora una respuesta rápida, coordinada y eficaz en el caso que nos ocupa. De hecho, las acciones desplegadas tanto por la funcionaria que, en términos del recurrente, cometió el error operativo, como por parte de su superior jerárquica en nada corresponden al protocolo documentado por la entidad para el efecto, lo que sustenta aún más la idea de que el personal de la recurrente no tiene claridad sobre cómo actuar en este tipo de situaciones.

3. Así las cosas, llama la atención que sea la misma entidad quien pretende restarle importancia al suceso que tuvo lugar el 17 de julio de 2018 al considerar que, en tanto este no llegara a ser de conocimiento de la autoridad de protección de datos personales, podría ser superado casi de manera inmediata y sin consecuencia alguna, conducta que es desde todo punto de vista violatoria del Régimen General de Protección de Datos Personales. Sin embargo, olvida el recurrente que sin seguridad no hay debido tratamiento de datos personales.

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

Posteriormente, la recurrente hace referencia a la presunta omisión probatoria por parte de esta Superintendencia, aseverando que, la Cámara cuenta con documentación en materia de protección de datos personales, la cual es conocida y expresamente aceptada por cada uno de los funcionarios que hacen parte de la entidad. En el mismo sentido, manifiesta que no es de su recibo el argumento de esta Superintendencia, en relación con la inexistencia de pautas para evitar el uso, acceso o consulta no autorizada, debido a que "*sí existían para el tiempo en que se presentaron los hechos materia de investigación y que eran de obligatoria aplicación por parte de toda la planta de personal de la Cámara*"[10].

Además, señala que desconoce que llevó a este Despacho a considerar que las acciones analizadas en el acto administrativo recurrido eran las únicas acciones en materia de capacitaciones y divulgación de la información que había adoptado y realizado la entidad, alegando que el

[10] Radicado 18-193960-26-1, página 7.

contenido de la documentación aportada con la respuesta otorgada por la Cámara, con anterioridad a la formulación de cargos, se evidencia que estos no son las únicas medidas implementadas.

En línea con lo anterior, hace alusión a las múltiples capacitaciones que le permiten a la entidad 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, tal y como asegura lo prueba el informe de la auditoría externa realizada por la firma Ernst & Young del año 2017. De forma que, para demostrar sus afirmaciones, aporta copia de la documentación que contiene las acciones de formación realizadas en el segundo semestre de 2017 y el primer semestre de 2018.

Frente a lo anterior, relativo a que este Despacho omitió pronunciarse y valorar todo el material probatorio aportado tendiente a demostrar las acciones implementadas para evitar una violación al deber de seguridad de la información, esta Dirección debe indicarle a la recurrente que los mismos fueron valoradas conforme a las reglas de la sana crítica, de manera que todo el material aportado por la recurrente fue tenido en cuenta para efectos de tomar la decisión plasmada en la Resolución recurrida.

Por lo expuesto, no son del recibo de este Despacho las afirmaciones del recurrente, según las cuales, en el caso que nos ocupa nos encontramos ante un hecho puntual y totalmente aislado a la dinámica de la entidad que, incluso hubiese pasado desapercibido.

5.1.2. De las características del archivo remitido el día 17 de julio de 2018

Adicionalmente, la recurrente manifiesta su discrepancia frente a lo indicado en torno a la falta de verificación en la práctica de las medidas establecidas por la Cámara de Comercio de Bogotá para la custodia de la información, así como a la falta de adopción de medidas de seguridad para los archivos compartidos por la sociedad investigada. Sobre el particular, afirma que se omitió valorar "*el origen del archivo, su objetivo y su transitoria existencia*"[11]. Además, resalta que el archivo carecía de cualquier vocación circulatoria interna o externa y su utilización era absolutamente restringida.

Señala que, sin ninguna duda, el archivo, como el que hoy es objeto de cuestionamiento, no requiere las seguridades propuestas en el acto administrativo recurrido, debido a que, es un archivo temporal, de circulación restringida, cuya esencia consiste en que sea editable, modificable y sujeto a actualización por parte del funcionario que los trata. Por lo cual, declara que los argumentos en torno a las medidas de seguridad no resultan apropiados para la medición de la responsabilidad de la Cámara de Comercio de Bogotá.

De estos argumentos se desprende que el recurrente realiza una caracterización de la base de datos en formato Excel que contenía información referente a nombres y apellidos, número celular, número de teléfono fijo y correo electrónico de cuatrocientas trece (413) personas, en los siguientes términos:

> *"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."*[12]

Frente a los argumentos esgrimidos por el recurrente en referencia a las características del archivo en formato Excel remitido vía correo electrónico, conviene realizar las siguientes precisiones:

La Ley Estatutaria 1581 de 2012 en su artículo 3 precisa las definiciones de los vocablos técnicos indispensables para la protección de datos personales, en tanto permiten una correcta

[11] Radicado 18-193960-26-1, página 5.
[12] Ibidem.

interpretación de la ley y contribuyen a determinar las responsabilidades de los Responsables en el tratamiento de datos personales.

Adicionalmente y para efectos del análisis de los argumentos expuestos por el recurrente, es menester traer a colación el contenido del artículo en cita, particularmente la definición de base de datos, así:

> *"**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;*
>
> *(…)."*

En referencia al contenido de este artículo, la Corte Constitucional al efectuar el análisis de constitucionalidad de la Ley Estatutaria 1581 de 2012, mediante sentencia C-748 de 2011, realizó un estudio sobre el concepto de base de datos, entendiendo que este cobija los archivos, como depósitos ordenados de datos y, en consecuencia, estos se encuentran sujetos a las garantías previstas en la ley. Para una mayor ilustración, se presentan a continuación extractos del referido análisis:

> *"**2.5.5. Constitucionalidad del literal b): definición de "base de datos"***
>
> *El literal b) define las bases de datos como un "(…) conjunto organizado de datos personales que sea objeto de tratamiento". Pese a que esta definición es bastante amplia y parece coincidir más con la de un banco de datos empleada en la Ley 1266, en tanto el legislador goza de libertad de configuración en la materia, puede adoptar definiciones diferentes dependiendo de la regulación.*
>
> *Ahora bien, la definición se ajusta a la Carta, pues cobija todo espacio donde se haga alguna forma de tratamiento del dato, desde su simple recolección, lo que permite extender la protección del hábeas data a todo tipo de hipótesis. En concordancia, la Sala recuerda, como se indicó en la consideración 2.4.3.2, que el concepto de base de datos, cobija los archivos, entendidos como depósitos ordenados de datos, lo que significa que los archivos están sujetos a las garantías previstas en el proyecto de ley.*
>
> ***2.4.3.2.** (…)*
>
> *El artículo 3 del proyecto define las base (sic) de datos de una manera muy amplia como el "[c] conjunto organizado de datos personales que sea objeto de Tratamiento". El tratamiento, por su parte, es definido como "[c] cualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso circulación o supresión".*
>
> *El proyecto no contiene una definición de archivo; sin embargo, éste es definido por la Real Academia de la Lengua como el "[c]onjunto ordenado de documentos que una persona, una sociedad, una institución, etc., producen en el ejercicio de sus funciones o actividades" o como el "[l]ugar donde se custodian uno o varios archivos." Los archivos también son definidos por la Ley 594 de 2000 "por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones", como el "[c]onjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de historia (…)" (artículo3). Finalmente, los archivos también han sido conceptualizados por esta Corporación, así: "(…) un conjunto orgánico de documentos, unidos por un vínculo originario o de procedencia, que sirven para recuperar con agilidad y en tiempo oportuno toda la información almacenada por una oficina o institución en el curso de su actividad."*
>
> *De acuerdo con estas definiciones, los archivos -para efectos exclusivamente del proyecto-, en tanto son **(i)** depósitos ordenados de datos personales, y **(ii)** suponen, como mínimo, que los datos han sido recolectados, almacenados y, eventualmente usados- modalidades de tratamiento, son una especie de base de datos que contiene datos personales*

susceptibles de ser tratados y, en consecuencia, serán cobijados por la ley una vez entre en vigencia.

(…)

Vale la pena mencionar que si bien la definición de base de datos que trae el proyecto puede diferir del uso común del término, no por ello es inconstitucional, pues el legislador goza de discrecionalidad para hacer clasificaciones y fijar definiciones, como ocurrió en este caso."[13]

En virtud de lo expuesto, no son del del recibo de esta Dirección los argumentos presentados por el recurrente frente a la caracterización del archivo Excel remitido el 17 de julio de 2018, particularmente cuando el mismo asevera que la base de datos era "*de uso estrictamente doméstico*" por las siguientes razones:

1. En el caso que nos ocupa, la **CÁMARA DE COMERCIO DE BOGOTÁ** realiza el tratamiento de datos personales a través de la recolección, uso, almacenamiento y circulación del número celular, número de teléfono fijo y correo electrónico de cuatrocientas trece (413) personas, de los cuales alrededor de:

(i) 18 cuentas están vinculadas a personas jurídicas;

(ii) 125 cuentas están relacionadas a personas naturales con dominio de persona jurídica (direcciones de correo electrónico corporativas); y,

(iii) 253 cuentas están relacionadas a personas naturales con dominios "*Google*", "*Yahoo*", "*Hotmail*", "*Etb*", "*Une*", independiente si las mismas estaban relacionadas con la profesión u oficio de los individuos afectados o, por el contrario, pertenecen a su ámbito personal.

(iv) 358 números de líneas de telefonía móvil o celular; y,

(v) 220 números de líneas de telefonía fija.

Para dar claridad sobre este punto, es necesario referirse al tipo de dato que es considerado un número de teléfono, así como el correo electrónico, en la medida en que el tratamiento de estos datos debe darse de acuerdo con los estándares legales pertinentes.

Por ello, dicho tratamiento no resulta menor, ya que como lo expuso la Corte Constitucional, al referirse a la clasificación de los datos personales, definió el dato semiprivado como aquel cuyo conocimiento o divulgación se encuentra sujeto al cumplimiento de los preceptos expuestos en la Ley Estatutaria.

A continuación, se transcribe un extracto de la sentencia C-748 de 2011:

"En primer lugar, la clasificación de los datos personales en públicos, semiprivados y privados o sensibles, es solamente una posible forma de categorizar los datos, pero no la única; otras clasificaciones podrían ser producto de criterios diferentes al grado de aceptabilidad de la divulgación del dato. El legislador, por tanto, tiene libertad para elegir o no elegir una categorización.

Ahora bien, es cierto que el propio legislador estatutario adoptó algunas de estas clasificaciones, como la de datos sensibles, cuyo tratamiento se prohíbe con algunas excepciones en el artículo 6 del proyecto. Para poder dar sentido a este precepto, a juicio de la Sala, basta con acudir a las definiciones elaboradas por la jurisprudencia constitucional o a las definiciones de otros preceptos legales, como la Ley 1266, cuyo artículo 3 dispone:

(…)

g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.

---

[13] Ibid. 9

(…)."

En línea con dicha definición, el Decreto Único Reglamentario 1074 de 2015 aclaró por medio del numeral segundo del artículo 2.2.2.25.1.3 que los datos públicos son aquellos que, entre otros están relacionados con *"[e]l estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público*".

Así pues, en la medida en que el número de teléfono y el correo electrónico relacionadas a personas naturales no hace referencia a la profesión, oficio, calidad de comerciante o de servidor público de los Titulares, el mismo no puede ser entendido como un dato de naturaleza publica, sino semiprivada, en la medida en que estos datos solo interesan al Titular y a cierto grupo de personas que este considere. Ello implica que su uso está permitido única y exclusivamente por las partes que los Titulares hayan autorizado.

Por esto, no es dable que la Cámara de Comercio, alegando la ocurrencia de un error humano, pretenda restarle importancia al hecho de que los datos de los cuatrocientos trece (413) Titulares circularon y fueron conocidos por personas no tenían por qué conocerlos, aun cuando sean de la "familia" de la recurrente.

2. Las características expuestas por el recurrente en torno a la transitoriedad, vida útil y uso doméstico del archivo no desnaturalizan la esencia del mismo. Contrario a lo manifestado por la Cámara, la transitoriedad del archivo no implica que no haya datos personales registrados en este; razón por la cual, su circulación sin medidas de protección y seguridad representan un riesgo inminente para la protección de los datos de los Titulares de la información.

   En el examen de constitucionalidad de la Ley Estatutaria 1581 de 2012, la Corte Constitucional realizó el análisis del principio de acceso y circulación restringida en los siguientes términos[14]:

   "(…)

   Principio de acceso y circulación restringida: *En razón de esta directriz, el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, éste sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Además, se prohíbe que los datos personales, salvo información pública, se encuentren disponibles en Internet, a menos que se ofrezca un control técnico para asegurar el conocimiento restringido.*

   En relación con ***el primer inciso****, deben hacerse las siguientes precisiones. Como se explicó anteriormente, esta Ley Estatutaria, al establecer las condiciones mínimas en el manejo de la información, no agota la regulación en materia de habeas data, y por tanto, el Tratamiento estará también sujeto a la normatividad que se expida posteriormente.*

   En cuanto ***al segundo inciso****, la norma debe entenderse que también se encuentra prohibida toda conducta tendiente al cruce de datos entre las diferentes bases de información, excepto cuando exista una autorización legal expresa, es decir, lo que la jurisprudencia ha denominado el* ***principio de individualidad*** *del dato. Como consecuencia de lo anterior, queda prohibido generar efectos jurídicos adversos frente a los Titulares, con base****, únicamente*** *en la información contenida en una base de datos.*

   De otra parte, y en relación con ese segundo inciso, uno de los interviniente solicita a esta Corporación, declarar su constitucionalidad bajo los siguientes condicionamientos: (i) se debe evitar que los datos privados, semiprivados, reservados o secretos puedan estar junto con los datos públicos, y por tanto, los primeros no pueden ser objeto de publicación en línea, a menos que se ofrezcan todos los requerimientos técnicos y (ii) se debe eliminar cualquier posibilidad de acceso indiscriminado, mediante la digitación del número de identificación a los datos personales del ciudadano.

   Considera la Sala que tales condicionamientos no son necesarios, por cuanto la misma norma elimina estas posibilidades. En efecto: (i) prohíbe que los datos no públicos sean publicados en Internet y (ii) sólo podrían ser publicados si se ofrecen todas las garantías. De lo anterior se infiere que si el sistema permite el acceso con la simple digitación de la

[14] Cfr. Corte Constitucional, sentencia C 748 del 2011 de fecha 6 de octubre de 2011, M.P.: Jorge Ignacio Pretelt Chaljub Considerando 2.6.5.2.6 Análisis de la constitucionalidad del Principio de acceso y circulación restringida**.**

cédula, no es un sistema que cumpla con los requerimientos del inciso segundo del literal f) del artículo 4.

Sin embargo, debe reiterarse que el manejo de información no pública debe hacerse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el Responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular.

De otra parte, cabe señalar que aún cuando se trate de información pública, su divulgación y circulación está sometida a los límites específicos determinados por el objeto y finalidad de la base de datos.

(…)"

De acuerdo con lo anterior, es claro que la jurisprudencia denota la necesidad de que la información que se encuentre contenida en una base de datos y que no se trate de información pública, deba gozar de todas las medidas de seguridad necesarias, útiles y pertinentes para evitar que terceros no autorizados accedan a ella.

Por ello, no es dable aceptar el argumento de la recurrente en el sentido de que el archivo en formato editable Excel al ser conocido por terceros puso en evidente riesgo los datos personales de los Titulares cuya información estaba contenido en dicho archivo, puesto que los terceros no solamente no se encontraban autorizados para conocerlo, siendo este un requisito para poder circular la información.

Frente al uso doméstico del archivo, ciertamente, el ámbito doméstico se encuentra ligado al derecho a la intimidad y la posibilidad de autodeterminación como un elemento de la dignidad humana, el cual no puede predicarse de las personas jurídicas.

Frente al uso de bases de datos de uso doméstico, la Corte Constitucional en sentencia C 748 del 2011, dispuso lo siguiente:

"(…)

2.4.5.3. Constitucionalidad del literal a): la excepción "las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico".

(…)

2.4.5.3.1. En relación con el primer contenido normativo, uno de los intervinientes asegura que la excepción debe cobijar todo dato que circula internamente, es decir, no solamente a nivel personal y doméstico, sino también, por ejemplo, a nivel de una empresa, y entiende que lo que delimita la circulación interna es el tratamiento del dato sin la intención de suministrarlo a terceros. La Sala, por el contrario, encuentra que la regla, tal cual está redactada en el proyecto, es compatible con la Constitución y que la Corte no puede extender el ámbito de la excepción a hipótesis que no fueron previstas por el legislador, por las razones que a continuación se exponen:

El primer contenido normativo del literal a) tiene tres elementos: (i) hace referencia a datos personales, (ii) contenidos en bases de datos (iii) "mantenidos en un ámbito exclusivamente personal o doméstico". El último elemento, que es el cuestionado por el interviniente, se refiere al ámbito de la intimidad de las personas naturales; ciertamente, los ámbitos personal y doméstico son las esferas con las que tradicionalmente ha estado ligado el derecho a la intimidad, el cual, en tanto se relaciona con la posibilidad de autodeterminación como un elemento de la dignidad humana, no puede predicarse de las personas jurídicas. Por tanto, esta excepción busca resolver la tensión entre el derecho a la intimidad y el derecho al habeas data.

Así, en tanto los datos mantenidos en estas esferas (i) no están destinados a la circulación ni a la divulgación, y (ii) su tratamiento tampoco puede dar lugar a consecuencias adversas para el titular, tiene sentido que su tratamiento esté exceptuado de algunas disposiciones del proyecto. Por ejemplo, no sería razonable que la protección de los datos personales mantenidos en estos ámbitos (por ejemplo, un directorio telefónico doméstico) estuviera a cargo de la Superintendencia de Industria y Comercio o que quien trata los datos estuviera sometido al régimen sancionatorio que prevé el proyecto.

Ahora bien, no puede entenderse que el primer contenido normativo del literal a) se extienda al tratamiento de cualquier dato cuando circule internamente, (…). En primer lugar, si bien es cierto una de las razones por las cuales la excepción del literal a) es razonable es porque los datos "mantenidos en un ámbito exclusivamente personal o doméstico" no están destinados a circular, ***de ahí no se sigue que todo dato que no circula o circula internamente deba ser exceptuado, pues 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****. Ciertamente, se trata de dos hipótesis diferentes, razón por la cual, por ejemplo, en el texto de la Ley 1266, si bien fueron tratadas conjuntamente, fueron unidas por la conjunción "y", lo que significa que son dos ideas distintas.[164]*

En segundo lugar, no hay razones para concluir que, en el contexto de una regulación general y mínima del habeas data[165], el tratamiento de datos que circulan internamente merezca las mismas consecuencias jurídicas del tratamiento de datos "mantenidos en un ámbito exclusivamente personal o doméstico"; en otras palabras, no hay argumentos constitucionales que lleven a concluir que las dos hipótesis deben recibir el mismo trato legal. 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.

En este orden de ideas, siempre y cuando se cumplan las condiciones mencionadas previamente y se entienda que, en todo caso, esta hipótesis sí se encuentra sujeta a los principios del artículo 4, para la Sala la excepción prevista en la primera regla del literal a) se ajusta a la Carta."

De lo anterior, se encuentra entonces que en el caso objeto de estudio: (i) la protección de los datos personales de los Titulares de la información esté a cargo de esta Superintendencia, (ii) la **CÁMARA DE COMERCIO DE BOGOTÁ** se encuentre sometida al Régimen General de Protección de Datos Personales y (iii) la base de datos que fue puesta en conocimiento de terceros, sin la autorización de los titulares, no goza del carácter de ser de uso personal o doméstico en la medida en que la recurrente no es una persona natural y que la información no estaba resguardada en su esfera íntima, ya que precisamente la información circulaba internamente dentro de la institución de la **CÁMARA DE COMERCIO DE BOGOTÁ**.

3. Se encuentra acreditado que la base de datos, que contenía datos personales de cuatrocientas trece (413) personas, circuló vía correo electrónico, pese a que el recurrente sostiene de manera reiterada que la misma no tenía vocación de circular; llegando a un destinatario que no tenía por qué conocer el contenido de dicha base de datos.

4. Es claro que el archivo de Excel es un conjunto de datos personales objeto de tratamiento por parte de la **CÁMARA DE COMERCIO DE BOGOTÁ**.

5. La sociedad investigada administra un archivo de Excel, el cual se constituye como una base de base de datos, en términos del Alto Tribunal Constitucional, que contienen información personal susceptible de ser tratada y, en consecuencia, se encuentran cobijados por la Ley Estatutaria 1581 de 2012.

Consecuencia de lo anterior, no se avizora yerro alguno en el contenido del acto administrativo objeto de recurso; lo cual fractura los cimientos de la sustentación propuesta por el recurrente y conlleva a que los argumentos referidos en este motivo de inconformidad no estén llamados a prosperar.

5.2 Frente a la aplicación del principio de responsabilidad demostrada

La recurrente inicia este acápite, señalando que esta Superintendencia basa su conclusión de incumplimiento del principio de responsabilidad demostrada por parte de la Cámara en dos puntos principales: (i) la entidad no tomó las acciones pertinentes para que el personal de esta conociera

el protocolo de violaciones e incidentes y actuara de conformidad y (ii) la Cámara no puso en práctica medidas para la mitigación de los riesgos que conlleva el tratamiento de datos personales.

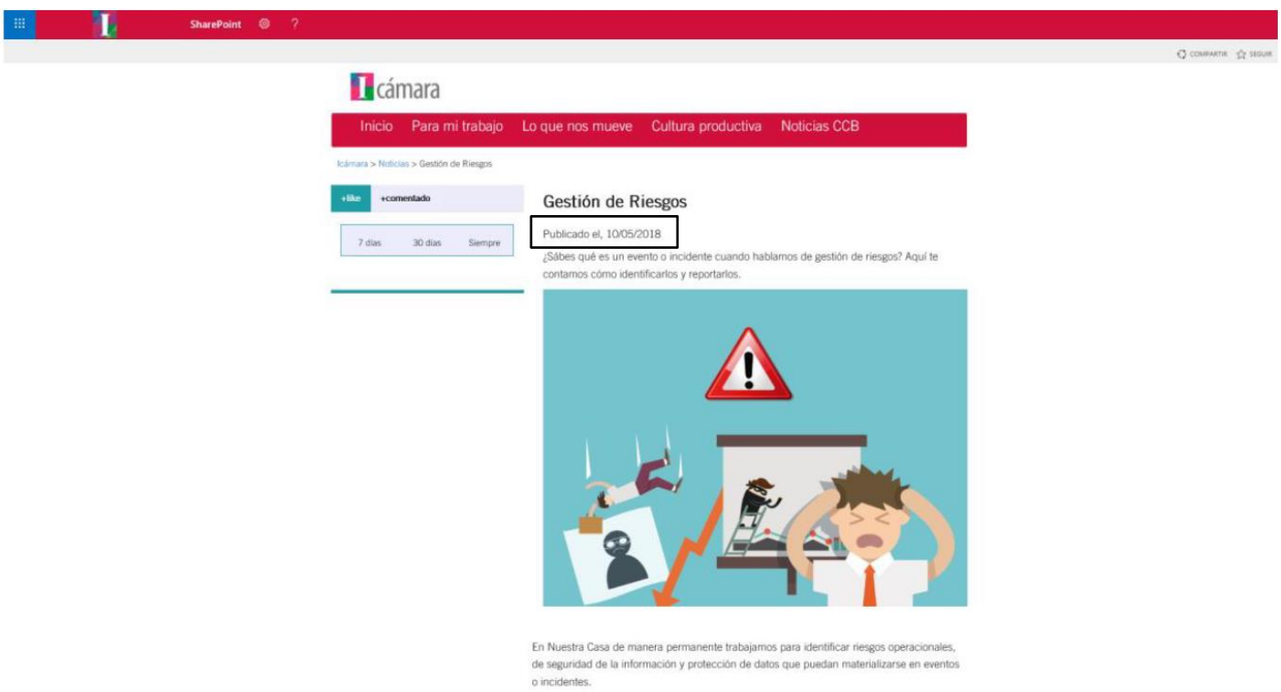
Sobre el particular, el recurrente afirma que es precisamente a partir del material probatorio allegado que se acredita que la Cámara, además de contar con toda una serie de políticas para el tratamiento de la información, las ponía en conocimiento de todos sus funcionarios.

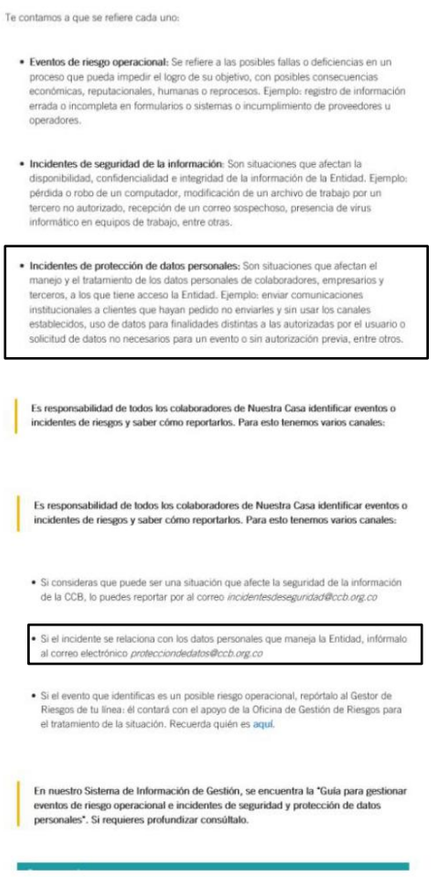
Indica que, resulta apenas lógico que, a pesar de los protocolos y directrices existentes, la funcionaria que remitió el correo electrónico el día 17 de julio de 2018 comunicara lo sucedido a su superior jerárquica con el fin de pedir su direccionamiento. A su vez, señala que la forma en que procedió la funcionaria evitaría molestias derivadas de un actuar por cuenta propia, así fuera siguiendo los protocolos por todos conocidos. Sobre este punto, se apoya en su insistencia de que el documento de seguridad, cuya lectura, comprensión y suscripción se hizo obligatoria al momento de la contratación de la funcionaria y que, por ello, la misma sabia como proceder. Igualmente, hace referencia a las constantes tareas de capacitación en las diferentes materias que tienen que ver con privacidad y seguridad de la información.

Solicita un análisis del acervo probatorio que da muestra de las acciones que se han tomado por parte de la Cámara, en aras de impedir que por parte de los 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 paras adelantar las acciones institucionales más pertinentes.

En relación con las manifestaciones efectuadas por el recurrente, este Despacho debe señalar que, en la parte motiva de la Resolución 81697 del 21 de diciembre de 2020 se detalló suficientemente el análisis y valoración de las piezas probatorias obrantes en el expediente, las cuales, analizadas en su conjunto y de conformidad con las reglas de la sana crítica, permitieron determinar el incumplimiento al deber 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.

Sin embargo, advierte esta Dirección que, la sociedad investigada aportó una nueva pieza probatoria, mediante complemento de información radicado el día 05 de enero de 2021, bajo el número 18-193960-25-1, cuya imagen se muestra a continuación:





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:

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.

A partir de las anteriores imágenes, es pertinente transcribir unos apartes de estas, con el propósito de velar por la trazabilidad de la información:

> *"(…)*
>
> *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:*
>
> *(…)*
>
> - ***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.*
>
> *(…)*
>
> - *Si el incidente se relaciona con los datos personales que maneja la Entidad, infórmalo al correo electrónico protecciondedatos@ccb.org.co*
>
> *(…)".*

A partir del contenido de la pieza documental en cita se tiene que, si bien la sociedad investigada tenía documentado un procedimiento para el trámite de incidentes de seguridad en materia de protección de datos personales con anterioridad a la ocurrencia de los hechos objeto de investigación; lo cierto es que, dicho procedimiento era totalmente desconocido, tanto por la funcionaria que remitió el correo el día 13 de julio de 2018 como por su superior jerárquica. Lo anterior, por cuanto se tiene que de haber conocido dicho protocolo, la funcionaria o, en su defecto, su superior jerárquica hubiese remitido un correo electrónico a la dirección dispuesta por la Cámara de Comercio para el reporte de incidentes de seguridad asociados a datos personales, es decir, al

correo electrónico "protecciondedatos@ccb.org.co" situación que no ocurrió, tal y como lo acredita el material probatorio obrante en el expediente.

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

El principio de responsabilidad demostrada se articula con el concepto de "compliance" en la medida que este hace referencia *"al conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos"*[15].

Así las cosas, la identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del "compliance" y de la efectiva aplicación del principio de responsabilidad demostrada (accountability). De ahí que, se considere fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un sistema de administración de riesgos asociados al tratamiento de datos personales, que les permita identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales.

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

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

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

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

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

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

Precisado lo anterior, y retomando el caso que nos ocupa, este Despacho encuentra que, el recurrente no aportó material probatorio que desvirtúe lo expuesto en la parte motiva de la Resolución N°.81697 proferido el 21 de diciembre de 2020. Por el contrario, la pieza documental en

---

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

cita confirma la desconexión que existe entre el andamiaje documental que se encuentra al interior de la institución y el accionar del talento humano de la Cámara en materia de seguridad y confidencialidad de datos personales.

Frente a los argumentos de la recurrente sobre la carga probatoria, este Despacho se sirve hacer claridad sobre la actuación de la recurrente como Responsable del Tratamiento:

La Ley 1581 de 2012 se expidió para desarrollar el derecho constitucional de *habeas data* consagrado en el artículo 15 de la Carta Política de 1991; es decir, esta Ley desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales.

Igualmente, importante resulta el concepto de "*ley estatutaria*", la cual, según la sentencia C-687 de 2002, está dispuesta para regular ciertas materias que el Constituyente consideró de especial importancia en nuestra sociedad. Esta figura legislativa tiene una especial jerarquía, ya que una ley se entenderá pertenecer a tal jerarquía cuando se cumplen los siguientes requisitos: (i) el asunto trata de un derecho fundamental y no de un derecho constitucional de otra naturaleza, (ii) cuando por medio de la norma está regulándose y complementándose un derecho fundamental, (iii) cuando dicha regulación toca los elementos conceptuales y estructurales mínimos de los derechos fundamentales, y (iv) cuando la normatividad tiene una pretensión de regular integralmente el derecho fundamental.

Así las cosas, entendiendo que estamos ante una legislación de especial jerarquía sobre el resto de las leyes nacionales en la medida en que regula el derecho fundamental a la protección de datos personales, todo Responsable del Tratamiento de dichos datos debe obligatoriamente ajustarse a los requisitos y deberes que les impone la ley por tratase de un derecho fundamental.

Así las cosas, la Ley 1581 de 2012 y sus decretos reglamentarios están dispuestos para proteger el derecho fundamental de *habeas data* con el que cuenta todo Titular y garantizar que los Responsables del Tratamiento cumplan a cabalidad los deberes que recaen sobre ellos sin tener que recurrir a razonamientos complejos, ya que debería ser de fácil entendimiento que los deberes de ley son de obligatoria observancia para garantizar la protección de este derecho fundamental.

Finalmente, al aplicar el principio de la carga dinámica de la prueba, este Despacho entiende que era la apoderada de la recurrente quien debía probar el cumplimiento de los deberes de ley y en ese sentido aportar las pruebas que fueren pertinentes para desvirtuar las presunciones del Despacho, ya que en los procesos administrativos sancionatorios se está ante una investigación amparada en la facultad sancionatoria del Estado[16], consagrada en el artículo 209 de la Constitución Política de 1991, en el cual busca garantizar el orden público, más específicamente, garantizar el adecuado cumplimiento del Régimen General de Protección de Datos Personales dispuesto en la Ley 1581 de 2012.

La facultad sancionatoria de vigilancia y control que ejerce esta entidad fue explicada por la Corte Constitucional en sentencia C 703 del 2010[17], en la cual determinó que:

> "*(…)*
>
> *En cuanto hace a la administración, la filiación de su potestad sancionadora se suele situar en la función de policía que pretende asegurar el orden público y en el poder de policía que, con la finalidad de garantizar el orden público, permite regular el ejercicio de las libertades individuales e imponer sanciones orientadas al cumplimiento de las medidas de policía[18].*
>
> *En cualquier caso, el fundamento de la potestad sancionadora de la administración actualmente se encuentra en una pluralidad de disposiciones constitucionales que van desde el señalamiento de los fines del Estado, contemplados en el artículo 2º, hasta el establecimiento, en el artículo 209, de los principios que guían la función administrativa y,*

[16] **Artículo 209**. La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.

[17] Cfr. Sentencia C 703 del 2010, M.P.: Gabriel Eduardo Mendoza Martelo

[18] Cfr. Sentencia C-506 de 2002, M.P.: Marco Gerardo Monroy Cabra

señaladamente, el de eficacia, pasando por el artículo 29 superior que, al estatuir la aplicación del debido proceso "a toda clase de actuaciones judiciales y administrativas", reconoce, de modo implícito, que la administración está facultada para imponer sanciones.

(…)"

A partir de la facultad sancionatoria que otorga el artículo 19[19] de la Ley 1581 de 2012 y según el anterior apartado jurisprudencial de dicho Tribunal, este Despacho se encarga de verificar si la conducta desplegada por la recurrente fue o no violatoria de la Ley 1581 de 2012 a efectos de garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

De esta manera, este Despacho no puede aceptar las afirmaciones de la apoderada por cuanto este Despacho no tiene que desvirtuar las pruebas allegadas al proceso, sino que en virtud de su potestad sancionatoria, esta Dirección se encarga de verificar si la conducta desplegada por la recurrente fue o no violatoria de la Ley 1581 de 2012 a efectos de garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

5.3 Frente a la inobservancia de los requisitos de procedibilidad

En este acápite del escrito, sostiene el recurrente que:

"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."

En atención al argumento en cita, es pertinente mencionar que el artículo 19 de la Ley 1581 de 2012 establece las facultades otorgadas a esta Superintendencia, para el ejercicio de la función de vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en dicha norma.

Igualmente, el literal b) del artículo 21 de la citada norma, señala que esta Superintendencia puede *"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 habeas 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; (…)".*

[19] **Artículo 19. Autoridad de Protección de Datos**. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.
Parágrafo 1°. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.
Parágrafo 2°. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

La disposición citada anteriormente, significa que la reclamación previa presentada por el quejoso ante la sociedad investigada, es un requisito indispensable para que esta Superintendencia pueda ordenar la corrección, actualización o retiro de datos personales a petición del interesado, pero no para iniciar investigaciones administrativas tendientes a establecer si hay lugar o no a la imposición de una sanción, facultad que le asiste a esta entidad, sin necesidad de agotar requisito de procedibilidad alguno. Por tal razón, no era necesario que el Titular de la información agotara el mencionado requisito de procedibilidad.

De esta manera, entendiendo que en los procesos administrativos sancionatorios se está ante una investigación amparada en la facultad sancionatoria del Estado[20], consagrada en el artículo 209 de la Constitución Política de 1991, en el cual busca garantizar el orden público, más específicamente, garantizar el adecuado cumplimiento del Régimen General de Protección de Datos Personales dispuesto en la Ley 1581 de 2012.

La facultad sancionatoria de vigilancia y control que ejerce esta entidad fue explicada por la Corte Constitucional en sentencia C 703 del 2010[21], en la cual determinó que:

> "*(…)*
>
> *En cuanto hace a la administración, la filiación de su potestad sancionadora se suele situar en la función de policía que pretende asegurar el orden público y en el poder de policía que, con la finalidad de garantizar el orden público, permite regular el ejercicio de las libertades individuales e imponer sanciones orientadas al cumplimiento de las medidas de policía[22].*
>
> *En cualquier caso, el fundamento de la potestad sancionadora de la administración actualmente se encuentra en una pluralidad de disposiciones constitucionales que van desde el señalamiento de los fines del Estado, contemplados en el artículo 2º, hasta el establecimiento, en el artículo 209, de los principios que guían la función administrativa y, señaladamente, el de eficacia, pasando por el artículo 29 superior que, al estatuir la aplicación del debido proceso "a toda clase de actuaciones judiciales y administrativas", reconoce, de modo implícito, que la administración está facultada para imponer sanciones.*
>
> *(…)*"

A partir de la facultad sancionatoria que otorga el artículo 19[23] de la Ley 1581 de 2012 y según el anterior apartado jurisprudencial de dicho Tribunal, este Despacho se encarga de verificar si la conducta desplegada por la recurrente fue o no violatoria de la Ley 1581 de 2012 a efectos de garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Ahora bien, como puede observarse, en el presente caso no existió desatención normativa alguna, ni mucho menos se permitieron actuaciones con desafortunadas consecuencias como lo señala el recurrente; máxime si se tiene en cuenta que los procesos de carácter administrativo sancionatorios adelantados por esta Superintendencia se surten con total apego a las normas que rigen la materia y de cara a proteger los derechos de los Titulares de la información.

Por ello, esta Dirección de Investigación de Protección de Datos Personales, de acuerdo con sus facultades legales, realiza las siguientes funciones:

1. Velar por el cumplimiento de la Constitución y la Ley en materia de protección de datos personales.

---

[20] **Artículo 209**. La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.

[21] Cfr. Sentencia C 703 del 2010, M.P.: Gabriel Eduardo Mendoza Martelo

[22] Cfr. Sentencia C-506 de 2002, M.P.: Marco Gerardo Monroy Cabra

[23] **Artículo 19. Autoridad de Protección de Datos**. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Parágrafo 1°. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.

Parágrafo 2°. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

2. Adelantar investigaciones sobre presuntas vulneraciones de la regulación de tratamiento de datos personales.

3. Ordenar las medidas que sean necesarias para hacer efectivos los derechos fundamentales al "habeas data" y al "debido tratamiento de datos personales".

Por lo expuesto, es pertinente recordarle a la recurrente que esta autoridad se dedica a exigir el respeto del derecho al *habeas data* previsto en el artículo 15 de la Constitución Política y a garantizar que, en la recolección, el almacenamiento, el uso, la circulación y eventual supresión de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la Constitución y en la Ley Estatutaria 1581 de 2012, por lo que no es del resorte de la **CÁMARA DE COMERCIO DE BOGOTÁ** determinar qué casos son relevantes y cuáles no para efectos de que esta entidad realice sus funciones constitucionales y legales. Por esta razón, siempre que se avizore una presunta vulneración en materia de datos personales, esta autoridad conocerá el caso y tomará las decisiones que correspondan en derecho, conforme a las pruebas obrantes en cada expediente.

Por las razones esgrimidas en líneas precedentes, esta Dirección manifiesta enfáticamente su rechazo a la afirmación expuesta por la recurrente, al considerar que *"(…) 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"* y desestima los motivos de inconformidad presentados en este parte del recurso.

5.4 Frente a las causales de graduación de la sanción

Sustenta el recurrente este motivo de inconformidad de la siguiente manera:

> *"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.*[24]
>
> *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*

[24] Radicado 18-193960-26-1, página 13.

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 (sic) 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 (sic) 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 (sic) causal de atenuación de la pena impuesta.

Al respecto, resulta imperioso traer a colación el artículo 24 de la Ley 1581 de 2012, que, a su tenor literal señala 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:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

c) La reincidencia en la comisión de la infracción;

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;

> *e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;*
>
> ***f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.****"*
> (subraya y negrilla fuera del texto original)

Sobre este punto, la Corte Constitucional en la sentencia C-748 de 2011, precisó, que:

> *"Este precepto se ajusta a la Constitución, en la medida en que corresponde al legislador establecer parámetros para que las autoridades, al momento de aplicar determinada sanción, puedan hacer graduaciones dependiendo de factores o circunstancias del investigado o de su actuación. En ese sentido, el precepto analizado consagra en los primeros 5 literales, circunstancias de agravación de la sanción, mientras el último, el literal f) consagra una causal de disminución."*[25]

Nótese que como único criterio de atenuación de la responsabilidad se contempla 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.

Por lo anterior, no es del recibo de este Despacho, el argumento del recurrente en referencia al presunto desconocimiento del reconocimiento de la comisión de la infracción realizado por la sociedad investigada, en los términos expuestos en líneas precedentes; toda vez que como lo señaló esta Dirección en la parte motiva de la Resolución 81697 del 21 de diciembre de 2020, la sociedad investigada ejerció los derechos de contradicción y defensa dentro de la actuación administrativa de la referencia y, restringió su ejercicio a la confirmación de la ocurrencia del hecho denunciado, tal y como se puede observar en los extractos citados en el escrito de recurso.

De los argumentos propuestos por el recurrente y las consideraciones expuestas por este Despacho, mediante la Resolución 81697 del 21 de diciembre de 2020, en referencia a la aplicación del criterio de atenuación señalado en el literal f) del artículo 24 de la Ley 1581 de 2012, esta Dirección reitera la postura esgrimida en el acto administrativo en cita, toda vez que:

1. La **CÁMARA DE COMERCIO DE BOGOTÁ** ejerció el derecho de contradicción dentro de la presente actuación administrativa.

2. La sociedad investigada, tal y como lo manifestó en el escrito de descargos, alegatos de conclusión y lo reiteró el recurso objeto de análisis, 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, como lo exige la norma en cuestión.

3. En suma, a criterio de este Despacho, las consideraciones planteadas en los numerales 1 y 2 antes referido fracturan el espíritu de la norma en lo concerniente a los supuestos que deben cumplirse para la aplicación del criterio de atenuación, los cuales pueden sintetizarse de la siguiente manera: (i) el reconocimiento o aceptación que haga la sociedad investigada sobre la comisión de la infracción y (ii) que dicho reconocimiento o aceptación se realicé con anterioridad a la imposición de la sanción a la que haya lugar, es decir, el reconocimiento se debe realizar antes de la expedición del acto administrativo que represente la decisión final de la administración en cuanto a este asunto.

Así, encuentra esta Dirección que, la situación descrita resulta rotundamente contraria al espíritu de la norma en cita y al estudio de constitucionalidad que al respecto realizó la Corte Constitucional, por cuanto la aplicación del criterio de atenuación contemplado en el literal f) del artículo 24 de la Ley 1581 de 2012, implica el reconocimiento o aceptación expresos; es decir, la manifestación escrita e inequívoca de la comisión de la infracción, sin que dicha manifestación se limite a la

[25] Cfr. Corte Constitucional, sentencia C 748 del 2011 de fecha 6 de octubre de 2011, M.P.: Jorge Ignacio Pretelt Chaljub Considerando 2.23.3. La constitucionalidad del artículo 24.

narración de un hecho suficientemente acreditado dentro de la actuación administrativa de la referencia.

Ahora bien, frente al interrogante del recurrente en torno a la existencia de una "fórmula sacramental para la aceptación de la comisión de un hecho", basta con señalar que, con lectura sencilla del literal f) 24 de la Ley 1581 de 2012 podrá absolver suficientemente su cuestionamiento.

En virtud de lo expuesto, este Despacho no encuentra que los motivos de inconformidad presentados por el Recurrente, en este acápite del recurso, estén llamados a prosperar y mantendrá los criterios de graduación de la sanción, según lo expuesto en el acto administrativo proferido el 21 de diciembre de 2020.

5.5 Frente a las solicitudes realizadas por el recurrente

En su escrito de recurso, la **CÁMARA DE COMERCIO DE BOGOTÁ** señala:

> *"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."*

Teniendo en cuenta que fueron desvirtuados todos y cada uno de los motivos de inconformidad esgrimidos por la **CÁMARA DE COMERCIO DE BOGOTÁ** en su escrito de recurso, esta Dirección no encuentra procedente conceder lo solicitado; razón por la cual, la Resolución 81697 del 21 de diciembre de 2020 se confirmará la decisión adoptada.

En consecuencia, esta Dirección concederá el recurso de apelación interpuesto subsidiariamente por la sociedad investigada y procederá a trasladar las presentes diligencias al Despacho del Superintendente Delegado para la Protección de Datos Personales.

SEXTO: CONCLUSIONES

1. Con fundamento en lo expuesto, se encuentra suficientemente acreditado que la **CÁMARA DE COMERCIO DE BOGOTÁ** vulneró el precepto normativo contenido 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 no haber adoptado las medidas de seguridad efectivas tendientes a la conservación de la información, omisión que llevó a que fueran expuestos datos personales a terceros no autorizados por sus Titulares.

2. Las piezas probatorias obrantes en el expediente fueron debidamente valoradas.

3. La actividad investigativa de esta Superintendencia no se encuentra condicionada al agotamiento del requisito de procedibilidad previsto en el artículo 16 de la Ley Estatutaria 1581 de 2012.

4. La graduación de la sanción no obedeció a una decisión caprichosa de esta Dirección, sino que se realizó con base a los parámetros legales y a los criterios desarrollados por vía jurisprudencial, para el efecto.

SÉPTIMO: Que analizadas todas las cuestiones planteadas con ocasión del recurso y al tenor de lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirmará en todas sus partes la Resolución 81697 del 21 de diciembre de 2020.

En mérito de lo expuesto, este Despacho

RESUELVE

ARTÍCULO PRIMERO: **CONFIRMAR** en todas sus partes la Resolución 81697 del 21 de diciembre de 2020, de conformidad con la parte motiva del presente acto administrativo.

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

ARTÍCULO TERCERO: NOTIFICAR a la **CÁMARA DE COMERCIO DE BOGOTÁ** identificada con el NIT. **860.007.322-9**, a través de su representante legal y de su apoderado especial, entregándoles copia de la misma.

ARTÍCULO CUARTO: COMUNICAR al señor [redacted] identificado con la cédula de ciudadanía número [redacted], el contenido de la presente resolución.

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá D.C., 11 MAYO 2021

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

Proyectó: MRFA
Revisó: SRB
Aprobó: CESM

NOTIFICACIÓN:

Investigada:
Entidad: **CÁMARA DE COMERCIO DE BOGOTÁ**
Identificación: Nit.: 860.007.322-9
Representante Legal: **NICOLÁS URIBE RUEDA**
Identificación: C.C. No. 79.944.552
Apoderado: **JOSÉ IGNACIO PEDRO ELÍAS NOVOA SERRANO**
Identificación: C.C. 79.592.192
T.P. 100.709 del CSJ
Dirección: Avenida El Dorado No. 68 D – 35 piso 8°
Ciudad: Bogotá D.C.
Correo electrónico: notificacionesjudiciales@ccb.org.co

COMUNICACIÓN:

Señor: [redacted]
Identificación: [redacted]
Dirección: [redacted]
Ciudad: [redacted]
Correo electrónico: [redacted]