



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

RESOLUCIÓN NÚMERO 55943 DE 2021

(Agosto 31 de 2021)

Por la cual se resuelve un recurso de apelación

Radicación No. 18-64963

VERSIÓN PÚBLICA

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS
PERSONALES

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

CONSIDERANDO:

PRIMERO: Que mediante oficio radicado con el número 18-64963 de fecha 2 de febrero de 2018, el señor [REDACTED], presentó ante esta Superintendencia queja contra la sociedad COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A. identificada con NIT. 827.000.616-7, por presunta vulneración a las normas de protección de datos personales contenidas en la Ley 1581 de 2012.

SEGUNDO: Que una vez efectuado el análisis de los documentos que obran en el expediente, la Dirección de Investigación de Protección de Datos Personales mediante Resolución No. 53373 del 2 de septiembre de 2020, resolvió lo siguiente:

ARTÍCULO PRIMERO: Imponer una sanción pecuniaria a la sociedad **COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A.**, identificada con el Nit.827.000.616-7 de cien millones cincuenta y cinco mil seiscientos setenta pesos **M/CTE** (\$100.055.670) equivalente a dos mil ochocientos diez (2.810) UVT por la violación a lo dispuesto en la siguiente normatividad:

- i) Literal k) del artículo 17 de la ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la ley en cita y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015.
- ii) Literal n) del artículo 17 de la ley 1581 de 2012 en concordancia con el artículo 19 ejúsdem.

PARÁGRAFO: El valor de la sanción pecuniaria que por esta resolución se impone, deberá consignarse en efectivo o cheque de gerencia en el Banco Popular, Cuenta No. 050000249, a nombre de Dirección del Tesoro Nacional – Fondos Comunes, Código Rentístico No. 350300, Nit. 899999090-2. El pago deberá efectuarse dentro de los cinco (5) días hábiles siguientes a la ejecutoria de esta resolución y acreditarse en la ventanilla de Tesorería de esta Superintendencia con el original de la consignación, donde le expedirán el recibo de caja aplicado a la resolución sancionatoria. Vencido este plazo se cobrarán intereses por cada día de retraso, liquidados a la tasa del 12% efectivo anual.

ARTÍCULO SEGUNDO: Ordenar a la sociedad **COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A.**, identificada con el Nit.827.000.616-7 que:

“En cumplimiento de lo dispuesto en el literal k) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal g) del artículo 4 de la ley en cita y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015 deberá desarrollar y documentar un manual interno a través del cual se describan los procedimientos para garantizar la seguridad en la custodia de la información personal a cargo de la COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A., incluyendo archivos físicos, digitales y magnéticos”.

Por la cual se resuelve un recurso de apelación

PARÁGRAFO PRIMERO: La sociedad **COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A COAUTONOMA C.T.A.**, identificada con el Nit.827.000.616-7, deberá acreditar el cumplimiento de lo ordenado en el anterior artículo ante esta Superintendencia dentro de los noventa (90) días hábiles siguientes a la ejecutoria de la presente decisión, aportando el respectivo documento donde se acredite la orden aquí impartida.

PARÁGRAFO SEGUNDO: El incumplimiento de lo ordenado en el presente acto administrativo, hará a la sociedad **COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A COAUTONOMA C.T.A.**, acreedora de las sanciones previstas en la ley.

TERCERO: Que mediante escrito del 29 de septiembre de 2020 la sociedad COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A., a través de su representante legal, interpuso recurso de reposición y en subsidio el de apelación contra la Resolución No. 53373 del 2 de septiembre de 2020, solicitando se revoque la decisión basada en los siguientes argumentos:

“ I. Falta de congruencia entre los hechos investigados, los mencionados en la queja y los sancionados en la Resolución impugnada

Como se menciona en la Resolución sancionatoria y obra en el expediente, la actuación administrativa se inició por la queja presentada por el señor [REDACTED], en los siguientes términos:

(...)

Como se advierte, la queja tiene tres temas principales: I) Reparación por la pérdida de la carpeta; ii) Se investigue y sancione a la Cooperativa por haberse extraviado la carpeta y otros documentos y, iii) Se tome medidas con relación al ente certificador de la Cooperativa, por cuanto la certificación no se compadece con la realidad de la empresa.

La Resolución 10321, que formula pliego de cargos y la Resolución No. 53373 de 2020, que impone la sanción, se fundamentan en la presunta contravención de lo dispuesto en:

- i) el literal k) del artículo 17 de la ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la ley en cita y el artículo 2.2.2.25.6.1. del Decreto Único Reglamentario 1074 de 2015, por cuanto no se acreditó que la organización contara con el manual de políticas de seguridad.*
- ii) el literal n) del artículo 17 de la Ley 1581 de 2012 en concordancia con el artículo 19 ejúsdem, por no informar a la autoridad de protección de datos acerca del incidente consistente en el extravió de la carpeta que contenía la historia laboral del señor [REDACTED].*

Como se advierte, no obstante la claridad de la queja presentada los cargos y la sanción se impone por situaciones que no fueron objeto de queja, y a pesar que en el proceso se desvirtuaron los cargos al demostrar que la carpeta del señor [REDACTED] no esta perdida y que la Cooperativa cuenta con Manual Interno de Políticas y Procedimientos y para atender consultas y reclamos, de que trata el literal k) del artículo 17 de la ley 1581 de 2012, y que el "Manual de Políticas de Seguridad" es un documento diferente al exigido en la norma supuestamente vulnerada.

II. Vulneración de los derechos fundamentales de la investigada al debido proceso y a la defensa.

La Resolución No. 53373 de 2020, vulnera los principios del derecho administrativo sancionatorio, por incorporar una sanción por responsabilidad objetiva sin estar expresamente consagrada por la ley, y por desconocer los principios del debido proceso aplicable a estas actuaciones.

Para efectos de sustentar este punto, traemos a colación la Sentencia C-089 de dieciséis (16) de febrero de dos mil once (2011), expediente D-8206 Magistrado Ponente: Luis Ernesto Vargas Silva, donde la Corte Constitucional compila la jurisprudencia sobre responsabilidad objetiva en

Por la cual se resuelve un recurso de apelación el derecho administrativo sancionatorio y da los derroteros para el ejercicio de esta facultad sin vulnerar el artículo 29 de la Constitución Nacional. de la cual resaltamos los siguientes apartes:

(...)

El debido proceso se vulneró en la investigación y sanción impuesta a COAUTONOMA, por cuanto ésta se fundamenta en la responsabilidad objetiva, sin que se cumplan los requisitos jurisprudencialmente establecidos para su procedencia, toda vez con la misma se afectan derechos fundamentales, la sanción no solo es monetaria y el monto de la misma es de mayor entidad.

Inexistencia de las faltas alegadas por la Superintendencia

Con relación al primer cargo: *La Superintendencia cuestionó que en los documentos aportados por COAUTONOMA. No se acreditó que la organización contara con un Manual de Políticas de Seguridad, por lo que se estaría transgrediendo el literal k) del artículo 17 de la Ley 1581 de 2012, que dispone:*

(...)

Con los descargos, se puso en evidencia que la norma mencionada como infringida no tiene relación con la conducta investigada, toda vez que la primera establece la obligación de adoptar un Manual Interno de Políticas y Procedimientos y para atender consultas y reclamos, mientras que el cargo cuestiona no tener un "Manual de Políticas de Seguridad", documento que es diferente al exigido en el literal k) de la norma transcrita, motivo por el cual se solicitó la desestimación del cargo por inexistencia de norma que exija un Manual de Políticas de Tratamiento de Seguridad, y al estar acreditado que la Cooperativa cumple con el literal k) del artículo 17 de la Ley 1581 de 2012, por cuanto tiene un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos. como fue acreditado con la respuesta al requerimiento del ente de control.

Igualmente, se advirtió que no existe norma positiva que exija el mentado "Manual de Políticas de Seguridad", de tal manera que el ente de control no podía formular cargos y mucho menos sancionar, por un Manual que no es obligatorio para el responsable del tratamiento de los datos y/o que no esta incluido en la norma que se reputa como incumplida.

De otra parte, se resaltó que el Manual Interno de Políticas y Procedimientos y de Atención de Consultas y Reclamos, exigido por el literal k) del artículo 17 de la Ley 1581 de 2012, fue solicitado con el radicado 18-64963-4-1 del 20 de febrero de 2019, y aportado por COAUTONOMA con la respuesta al mismo radicado No. 18-064963-00005-0001 del 07 de marzo de 2019, identificado como ANEXO-SIG-05 en 12 páginas, el cual contiene todos los aspectos regulados por la Ley 1581 de 2012, y la política de tratamiento de seguridad implementado por la Cooperativa, el cual se adoptó conforme a los criterios fijados por la Superintendencia en la "Cartilla de formatos modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios", que en el punto 3, fija como criterios mínimos para el Manual los siguientes:

(...)

Como se indicó en el alegato de conclusión, la Corte Constitucional en sentencia C-748/11, expediente PE-03 2, en el control constitucional que avaló la expedición de la Ley 1581 de 2012, dispuso sobre la constitucionalidad del artículo 22, que la potestad sancionatoria es manifestación del jus punendi, razón por la que esta sometida a los principios de legalidad, tipicidad, debido proceso, proporcionalidad e independencia.

No se entiende entonces, como la Superintendencia sanciona por el incumplimiento de una norma (literal k) del artículo 17 de la Ley 1581 de 2012) que no exige el "Manual de Políticas de Seguridad" interpretando de manera subjetiva que el manual interno tiene que contener procedimientos idóneos que garanticen la implementación de políticas de seguridad, que estén en concordancia con el literal g) del artículo 4 de la ley referida y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015 (normas posteriores, que tampoco establecen ese

Por la cual se resuelve un recurso de apelación

Manual de manera expresa) so pretexto de determinar la infracción a las normas sobre protección de datos personales.

Tampoco podemos compartir la justificación del sancionador, cuando considera que por el hecho de haber mencionado en la formulación de cargos el manual de políticas de seguridad, que considera es el principio vulnerado al extraviarse la carpeta física con los soportes de la hoja de vida del denunciante, "reiterando que si bien en el literal k) del artículo 17 de la ley en comento no se nombra de manera expresa "Manual de Políticas de seguridad", este Despacho hizo alusión a las demás normas concordantes, en virtud del principio de legalidad" y que: "...es palmario que la Autoridad de Protección de Datos ha encontrado que el deber que le asiste a la investigada como responsable del tratamiento es de garantizar la seguridad de la información, deber que se materializa a través de la implementación de procedimientos documentados, como en el caso que nos ocupa." (Subrayados no son del texto original)

Al parecer el investigador confunde el manual con el principio, desconociendo que el primero se limita a documentar los procedimientos para garantizar el segundo y que las medidas adoptadas buscan disminuir el riesgo de la seguridad de la información, sin que sea dable afirmar que por presentarse una falla en la seguridad de la información, hay inexistencia del Manual, por cuanto el manual existe por sí mismo.

Lo que se evidenció en el proceso, es que Coautónoma cumplió con el literal k) del artículo 17 al expedir el Manual Interno de Políticas y Procedimientos y de Atención de Consultas y Reclamos, como se acreditó en su oportunidad y lo reconoce la Superintendencia, de manera independiente a que al investigador no le guste la presentación del Manual, situación que no es sancionable, por cuanto se incurre en una valoración subjetiva y en un error al considerar que la mentada norma sanciona las fallas en la seguridad de la información, cuando en la realidad exige es un documento con unos requisitos mínimos, que también fueron cumplidos por la Cooperativa.

Por lo anterior, la Resolución impugnada debe ser REVOCADA al quedar confirmada la deficiente adecuación típica del pliego de cargos, por cuanto se acude a una norma que exige un manual para sancionar por una falla de seguridad de la información, por la supuesta pérdida de una carpeta, que en el proceso se acreditó no esta perdida y al estar demostrado que COAUTONOMA desarrolló y cuenta con políticas internas efectivas para garantizar la adecuada protección de los datos personales que trata, con lo que se demuestra el cumplimiento de las obligaciones establecidas en la Ley 1581 de 2012 y en su Decreto Único Reglamentario

Con relación al segundo cargo: *La conducta investigada y sancionada, es la presunta violación del literal n) del artículo 17 de la Ley 1581 de 2012, que establece: "...n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares." por no haber informado a la autoridad de protección de datos acerca del incidente presentado con el extravió de la carpeta que contenía la historia laboral del señor [REDACTED].*

En los descargos y alegato se manifestó que esta norma no aplica para el caso materia de investigación, donde se cuestiona la supuesta pérdida de la carpeta física que contiene la hoja de vida del quejoso, por cuanto los Códigos de Seguridad son de común utilización en los sistemas de cómputo para proteger la información y su legitimidad, a fin de impedir el ingreso o utilización por personas no autorizadas, de tal manera que se entienden como una línea de defensa para garantizar la seguridad de información contenida en las bases de datos, y que el artículo 2° de la Ley 1581 de 2012 indica que los principios y disposiciones contenidas en esa ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada, excluyendo de aplicación a las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. (art. 2.2.2.25.1.2 Decreto 1074 de 2015).

Así las cosas, la Cooperativa no ha vulnerado la norma mencionada, por cuanto el deber de informar se genera únicamente por violaciones a los "Código(sic) de Seguridad" o riesgos en la administración de información contenida en bases de datos, mas no en carpetas físicas, por cuanto estas no tienen "Código de Seguridad" al no estar contenidas en bases de datos, menos aun, cuando la carpeta del Sr. [REDACTED], no contiene información sensible ya que esta

Por la cual se resuelve un recurso de apelación

conformada únicamente por la hoja de vida y los soportes de la misma, excluyendo la historia laboral, documentos que fueron suministrados como parte de la solicitud de trabajo presentada por el candidato para ser parte del equipo de trabajo para ejecutar el contrato que la Unión Temporal ICBF 2014 celebró con el ICBF, información laboral que no es susceptible de tratamiento por cuanto es de uso personal y domestico para la empresa, que por demás, tiene reserva legal conforme al Artículo 3, literal h) y artículo 4 literal g) de Ley 1266 de 2008 y lo dispuesto en la Sentencia No. T-768 de 2008, de la Honorable Corte Constitucional, expediente T-1865118, M. P. Dra. Clara Inés Vargas Hernández, de tal manera que el extravío es competencia de las autoridades jurisdiccionales, como fue el procedimiento realizado por la Cooperativa para dar respuesta al derecho de petición ante la imposibilidad de entregar la copia solicitada en el tiempo perentorio establecido en la Ley, como fue informado al Sr. [REDACTED] y a la Superintendencia. No obstante, que la carpeta fue localizada posteriormente y la documentación se encuentra en poder de la Cooperativa, como se demostró con la copia que se aportó con los descargos.

En conclusión, que conducta investigada no guarda relación con la norma presuntamente infringida, por cuanto la segunda es clara cuando establece que se debe informar cuando se presentes violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares y el cargo refiere a no haber informado de) extravío de una carpeta física que contenía la historia laboral del quejoso, incurriendo la Superintendencia nuevamente en inadecuada adecuación típica

En la Resolución impugnada la Superintendencia manifiesta que: "...la manera idónea para desvirtuar este cargo es demostrar que efectivamente si se informó a esta Superintendencia acerca de las violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los titulares, situación que no ocurrió. En consecuencia, este cargo será objeto de sanción."

No podemos compartir la conclusión anterior, por cuanto constituye una manifestación de aplicación de la responsabilidad objetiva que restringe el derecho a la defensa, al desconocer los argumentos planteados por la Cooperativa, que tienen un soporte legal que amerita ser considerados por el investigador.

Aunque compartimos la manifestación que el ámbito personal o domestico se refiere cuando la información se recopila para un uso eminentemente intimo y cuya finalidad no se ata a la circulación de la información, no estamos de acuerdo en la afirmación que en este caso concreto, "la información de la historia laboral se recopiló con el fin de alimentar una base de datos de la COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A COAUTONOMA C.T.A para el proceso de vinculación de su personal y el desarrollo de un objeto social, el cual se desborda ampliamente de la esfera personal", por cuanto de una parte, la Superintendencia no tiene prueba que ello sea así, y por la otra, en razón a que el peticionario como cooperado, se vinculó exclusivamente para ese contrato, una vez suscrito, y no para otros contratos ni para participar en el proceso de selección, de tal manera que su información no es publica ni ha sido divulgada.

La vinculación del peticionario a la cooperativa estar (sic) ligado al ámbito personal o domestico, que no cuenta con una naturaleza propia para la divulgación de datos personales, y en este sentido sus implicaciones son diferentes.

Tampoco compartimos la conclusión: "que las violaciones a los códigos de seguridad y los riesgos en la administración de la información de los Titulares, también se predicen de las carpetas físicas, pues tal como se dijo anteriormente, esta información es un dato personal y por tal razón debe tener un tratamiento con procedimientos con el fin de garantizar el cumplimiento de la Ley 1581 de 2012, especialmente lo concerniente al principio de seguridad" por cuanto el artículo 2° de la Ley 1581 de 2012 indica que los principios y disposiciones contenidas en esa ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza publica o privada, excluyendo de aplicación a las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o domestico, (art. 2.2.2.25.1.2 Decreto 1074 de 2015), de tal manera que la Superintendencia no puede aplicar la analogía para sancionar a la Cooperativa.

Finalmente, si bien el reproche que se hace es no haber reportado ante la Superintendencia la violación a los códigos de seguridad y la existencia de riesgos en la administración de la

Por la cual se resuelve un recurso de apelación

información de los Titulares, el investigador no puede desestimar los argumentos que desvirtúan la obligación de reporte como causal de exoneración de responsabilidad, o considerar como no relevante que la carpeta esté en poder de la Cooperativa, situación que desvirtúa el cargo por sustracción de materia, más aún cuando la Superintendencia no ha demostrado que hubo violación de los códigos de seguridad. Recordemos que la carga de la prueba es del investigador y no del investigado, en el que recae la presunción de inocencia, que tampoco ha sido respetado con la sanción impuesta.

Por lo anterior, consideramos que la Cooperativa no ha vulnerado la norma imputada, por cuanto la información suministrada con la hoja de vida se encuentra en poder de COAUTONOMA, no ha estado expuesta ni ha sido divulgada.

Falta de agotamiento del requisito de procedibilidad:

Se indico en los Descargos y en el alegato, que conforme al artículo 16 de la Ley 1581 de 2012, el Titular solo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el tramite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento y en el presente caso, no hay prueba que el Señor ██████ agotara este requisito previo de procedibilidad, resaltando que el derecho de petición presentado por el quejoso el 29 de marzo de 2017, no cumple los requisitos de reclamo para estos efectos, por cuanto la petición no tiene nada que ver con la queja que fue el soporte de la investigación y el requerimiento realizado por la Superintendencia el 22 de diciembre de 2017 tampoco puede tornarse como tal, por cuanto este se hizo después de presentada la queja y cuando la investigación estaba en curso.

En la Resolución impugnada, el Despacho manifiesta que es argumento no es de recibo, entre otros, porque el artículo 16 de la Ley no exige ninguna formalidad para el agotamiento del requisito de procedibilidad y porque en este caso si hubo un requerimiento previo por parte del denunciante ante la investigada (29 de marzo de 2017), aclarando que el acto de formulación de cargos no solo halla su sustento en los hechos denunciados, sino que la Dirección, adicionalmente, tuvo en cuenta el resultado de las averiguaciones preliminares adelantadas por la Coordinación del Grupo de Trabajo de Investigaciones Administrativas, de acuerdo con lo previsto en el artículo 47 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, con el fin de contar con las pruebas idóneas con merito para el inicio de una investigación administrativa de carácter sancionatorio.

Continua manifestando la Superintendencia que la petición del denunciante siempre estuvo encaminada a solicitar la carpeta que contiene sus datos personales, y que fue la investigada quien le informó que: “no es posible (...) allegar la documentación solicitada en consecuencia (sic) que la carpeta donde reposaba esta documentación se extravió de la sede principal a Bogotá”, motivo por el cual, la petición presentada si guarda relación con el requerimiento efectuado ante este Despacho, pues el denunciante tras evidenciar el extravío de su documentación puso en conocimiento dicha situación ante esta Superintendencia.

Las manifestaciones anteriores, son igualmente objeto de inconformidad de nuestra parte, por cuanto el pliego de cargo es claro al indicar que el acto administrativo de iniciación de la investigación administrativa y formulación de cargos, se genera con ocasión de la solicitud presentada por el señor ██████ de investigar a la Cooperativa por presunto incumplimiento de la Ley 1581 de 2012, por la pérdida de la carpeta que contiene sus datos personales, conducta que es diferente a las indicadas en la apertura y en la sanción, referidas a que no se acreditó que la organización contara con el manual de políticas de seguridad y por no informar a la autoridad de protección de datos acerca del incidente consistente en el extravío de la carpeta que contenía la historia laboral del señor ██████; igualmente, el pliego de cargos no indica cuales fueron las averiguaciones preliminares adelantadas por la Coordinación del Grupo de Trabajo de Investigaciones Administrativas, ni las pruebas idóneas recaudadas con merito para el inicio de la investigación administrativa de carácter sancionatorio, que sustentaran os (sic) cargos formulados.

De otra parte, la petición presentada no guarda relación con la solicitud ante ese Despacho ni con los cargos formulados, toda vez que como se ha insistido en todas las instancias, la petición incorporaba la entrega de copia de información, mientras que la solicitud a la Superintendencia tiene tres temas principales: i) Reparación por la perdida de la carpeta; ii) Se investigue y

Por la cual se resuelve un recurso de apelación

sancione a la Cooperativa por haberse extraviado la carpeta y otros documentos y, iii) Se tome medidas con relación al ente certificador de la Cooperativa, por cuanto la certificación no se compadece con la realidad de la empresa, temas que no tienen ninguna relación con la petición y mucho menos, con los cargos formulados por presuntamente no acreditar que la organización contara con el manual de políticas de seguridad y por no informar a la autoridad de protección de datos acerca del incidente consistente en el extravió de la carpeta que contenía la historia laboral del señor [REDACTED].

En consecuencia, respetuosamente insistimos que en este caso no se agotó en debida forma el requisito de procedibilidad.

111. Falsa motivación de la Resolución No. 53373 de 2020 y violación directa de las normas en que se debe fundamentar

La Resolución No. 53373 de 2020, incurre igualmente en causal de nulidad por falsa motivación y desconocimiento de las normas administrativas sobre los procesos sancionatorios, especialmente los establecidos en el Código Procesal Administrativo y de lo Contencioso Administrativo, como son:

Indebida interpretación del literal k) del artículo 17 de la Ley 1581 de 2012

Como se ha manifestado durante todo este proceso, el literal k) del artículo 17 de la Ley 1581 de 2012 no exige un "Manual de Políticas de Seguridad" sino: "Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos; ..."

Las manifestaciones del Despacho, en el sentido que esa norma debe ser analizada de manera armónica e integral, con el fin de entender la finalidad de la misma y así determinar con claridad cuál es el incumplimiento a las disposiciones legales para la protección de datos personales y que precisamente en la formulación de cargos se hizo mención al manual de políticas de seguridad, pues este principio fue el que se vulneró al extraviarse la carpeta física, desconoce las reglas fundamentales para la interpretación de la ley, que enseña que: cuando el sentido de la ley sea claro, no se desatenderá su tenor literal a pretexto de consultar su espíritu (Art. 27 Código Civil) para exigir un manual que no se exige en la ley y muchos (sic) menos para concluir que el manual adoptado es inexistente por haber ocurrido el extravió de una carpeta, que como se demostró no se ha perdido.

Atenta adicionalmente, la interpretación anterior, con la tipicidad que debe operar en materia sancionatoria, por cuanto se acude a una "interpretación armónica" para sancionar por la ausencia de un Manual que no exige esa norma, ni ninguna otra, y para desconocer un procedimiento adoptado que cumple con los requisitos mínimos fijados por la misma autoridad.

En estas condiciones, la Resolución sancionatoria incurre en abuso de poder y falsa motivación, toda vez que adopta una decisión subjetiva y discrecional, que no esta adecuada a la queja formulada ni a la norma invocada, adicional a que la sanción no es proporcional a los hechos que le sirven de causa, como se vera mas adelante.

Sobre este particular, se desconoció la Sentencia del Consejo de Estado de Agosto 30 de 1977, Sección Tercera que advierte que la motivación se impone por el principio de la legalidad de la administración, la cual debe ser seria adecuada y suficiente e íntimamente relacionada con la decisión que se pretende.

IV- Ausencia de valoración de la prueba aportada e inexistencia de prueba que soporte los hechos materia de sanción.

Cualquier sanción debe estar sustentada en pruebas legalmente practicadas y aportadas al proceso, las cuales deben tener la suficiente credibilidad y entidad para demostrar el incumplimiento de las norma(sic) por parte del sancionado.

Igualmente, la carga de la prueba esta a cargo del investigador, en este caso la Superintendencia, que cuenta con todas las herramientas legales para practicar las que considere necesarias para establecer los hechos e irregularidades, al igual que debe considerar

Por la cual se resuelve un recurso de apelación

las que aporta el investigado haciéndoles un estudio bajo las normas de la sana crítica. Es tan drástica la norma en el caso de las pruebas, que ante la ausencia de las mismas o duda, estas se deben resolver a favor del investigado.

En el caso concreto, es evidente que el Despacho invirtió la carga de la prueba, al sancionar a la empresa bajo las consideraciones generales que el investigado no logró desvirtuar los cargos formulados, cuando la realidad procesal y las normas sancionatorias, imponían la carga a la Superintendencia de demostrar que el investigado incurrió efectivamente en las conductas incluidas en los cargos y que lo manifestado por los quejosos esta debidamente soportado, hechos que no fueron probados, adicional a que no podían serlo por cuanto se exige un manual inexistente legalmente y se investiga por unas conductas diferentes a las de la queja.

En la otra conducta objeto de sanción, no se demostró las violaciones a los códigos de seguridad, requisito necesario para el reporte.

Pero lo más grave en este caso, es que el investigador desconoció la prueba aportada por la investigada, desconociendo la libertad probatoria y el principio de favorabilidad que legalmente tiene. No podía desconocer la Superintendencia los argumentos de COAUTONOMA CTA, mencionados en los descargos y en el alegato de conclusión, donde acredita el cumplimiento el literal k) del artículo 17 al expedir el Manual Interno de Políticas y Procedimientos y de Atención de Consultas y Reclamos, como lo reconoce la Superintendencia, incurriendo en una valoración subjetiva al considerar que la norma sanciona las fallas en la seguridad de la información, cuando en la realidad exige es un documento con unos requisitos mínimos, que también fueron cumplidos por la Cooperativa.

Igualmente, la Superintendencia no probó que la información formaba parte de una base de datos, ni desvirtuó que la misma hubiera sido publica para desvirtuar que estaba dentro del ámbito exclusivamente personal o domestico como lo ha manifestado la investigada.

En razón a lo anterior, es de precisar que la Superintendencia no logró probar lo manifestado por el quejoso ni las conductas endilgadas, razón por la cual muy respetuosamente solicitamos se revoque la Resolución, y en consecuencia, se absuelva de cualquier cargo a mi representada.

V Desproporción de la sanción

Con relación a la sanción impuesta, consideramos que la Resolución no es clara en la dosificación conforme al soporte legal de la misma, y en todo caso es desproporcionada, improcedente, indebida e injustificada, puesto que como se manifestó en los descargos y se demostró en el proceso, COAUTONOMA cumplió el literal k) del artículo 17 de la Ley 1581 de 2012, al adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y para la atención de consultas y reclamos, y de otra parte, la información es privada y la carpeta no se perdió, de tal manera que no era necesario hacer el reporte.

Para sancionar, la Superintendencia hace uso del artículo 23 de la ley 1581 de 2012, que con relación a la multa señala: "a) multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción..." y aplica el artículo 49 de la Ley 1955 de 2019, para calcular la sanción no en SMMLV sino con base en su equivalencia en términos de la unidad de valor tributario UVT

Igualmente, menciona el artículo 24 de la Ley 1581 de 2012, que señala los criterios de graduación de las sanciones, indicando que entrara a determinar cuales se deben tener en cuenta en caso concreto que permita garantizar el respeto de las garantías del artículo 29 Constitucional y que ejercerá su potestad sancionatoria de forma razonable y proporcionada, de modo que logre el equilibrio entre la sanción y la finalidad que la norma vulnerada, así como la proporcionalidad entre la gravedad de la infracción y la sanción aplicada

Después de hacer un extenso recuento normativo y jurisprudencial, entra al caso concreto afirmando que quedó demostrada la infracción a las normas incluidas en los cargos y así las cosas, impondrá una sanción por el monto de cien millones cincuenta y cinco mil seiscientos setenta pesos M/CTE (\$100.055.670), aclarando que los criterios de graduación de la sanción

Por la cual se resuelve un recurso de apelación

señalados en los literales b), c), d) y e) del artículo 24 de la Ley 1581 de 2008 no serán tenidos en cuenta debido a que (i) dentro de la investigación realizada no se encontró que la investigada hubiera obtenido beneficio económico alguno por la comisión de la infracción, (ii) no hubo reincidencia en la comisión de la infracción, (iii) no hubo resistencia u obstrucción a la acción investigativa de la Superintendencia y, (iv) no hubo renuencia o desacato a cumplir las órdenes e instrucciones del Despacho, suma que en la parte resolutive manifiesta equivale a dos mil ochocientos diez (2.810) UVT.

No obstante el antecedente y principios transcritos en la Resolución, el Despacho no indica que procedimiento utilizó para (sic) cuantificar la sanción de 2.810 UVT, de la cual ni siquiera menciona el valor actual, convirtiéndose esa suma en un valor subjetivo y caprichoso, que contradice aun el mismo acto que en apartes anteriores el Despacho considera procedente imponer la sanción correspondiente a cincuenta millones veintisiete mil ochocientos treinta y cinco pesos M/CTE (\$ 50.027.835) equivalente a mil cuatrocientos cinco (1.405) UVT

Por lo anterior, es imposible para el investigado ejercer su derecho a la defensa en este aspecto, y sólo nos queda mencionar que el monto de la sanción no cumple los criterios de la ley antes mencionados, para su graduación y cuantificación, mas aun cuando la norma habla no de una sanción fija sino variable, que puede ser desde (una) 1 UVT a 2.810 UVT.

Si la UVT para el año 2020 esta en \$35.607, según la Resolución DIAN 000084 del 28 de Noviembre de 2019, la sanción máxima solo podría ser de \$71' 214.000, de tal manera que no se entiende se aplique una sanción superior a 2.000 UVT, cuando la misma administración admite que en este caso no hay situaciones de agravación en los criterios de graduación de la sanción, de los señalados en los literales b), c), d) y e) del artículo 24 de la Ley 1581 de 2008.

Por lo anterior se objeta la sanción impuesta y la cuantificación.

VI Aclaración de la orden de desarrollar y documentar un manual interno a través del cual se describan los procedimientos para garantizar la seguridad en la custodia de la información

En el artículo SEGUNDO de la Resolución No. 53373 de 2020, se ordena a COAUTONOMA desarrollar y documentar un manual interno a través del cual se describan los procedimientos para garantizar la seguridad en la custodia de la información personal a cargo de la COOPERATIVA, incluyendo archivos físicos, digitales y magnéticos, concediendo un termino de noventa (90) días hábiles siguientes a la ejecutoria de la decisión, para aportar el respectivo documento donde se acredite la orden impartida.

Entendemos que esta orden guarda relación con lo dispuesto en la parte considerativa, donde se exhorta a la Cooperativa, para que adopte las medidas pertinentes, útiles, efectivas y verificables con el propósito de:

(...)

Con los descargos se adjuntó el "Manual Interno de Políticas y Procedimientos y de atención de consultas y reclamos" el cual contiene todos los aspectos regulados por la Ley 1581 de 2012, y se adoptó conforme a los criterios fijados por la Superintendencia en la "Cartilla de formatos modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios", que en el punto 3, fija como criterios mínimos para el Manual de Políticas y Procedimientos Internos y Política de tratamiento de datos personales, los siguientes: Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable del tratamiento de los datos, tratamiento al cual serán sometidos los datos y finalidad del mismo cuando no se haya informado mediante aviso de privacidad, derechos que tiene el titular de la información y persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y/o revocar la autorización y se solicitó.

Por lo anterior, solicitamos se ACLARE y precise la orden impartida, en el sentido de indicar cuales son las deficiencias del manual frente a la política de tratamiento de seguridad implementado por la Cooperativa, y que debemos cambiar o mejorar del mismo, toda vez que

Por la cual se resuelve un recurso de apelación estimamos el mismo cumple con la ley e incorpora las medidas y procedimientos necesarios para la operación de la Cooperativa conforme a las disposiciones previstas en la Ley.

Como consecuencia solicita lo siguiente:

Se reitera al Despacho la solicitud de REVOCATORIA de la Resolución No. 53373 de 2020, con fundamento en las causales establecidas en el artículo 93 del Código de Procedimiento Administrativo (Ley 1437 de 2011), por haber sido expedida con desconocimiento de las normas constitucionales y legales para este tipo de actuaciones respeto del debido proceso, carga de la prueba y proporcionalidad de la sanción.”

CUARTO: Que mediante Resolución No. 9275 del 26 de febrero de 2021 la Dirección de Investigación para la Protección de Datos Personales, resolvió el recurso de reposición interpuesto por la COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A, modificando la Resolución No. 53373 del 2 de septiembre de 2020 y concediendo el recurso de apelación interpuesto de manera subsidiaria, así:

ARTÍCULO PRIMERO: MODIFICAR el artículo primero del resuelve de la Resolución No. 53373 del 2 de septiembre de 2020 por las razones expuestas en la parte motiva de este acto administrativo, el cual quedará así:

“ARTÍCULO PRIMERO: IMPONER una sanción pecuniaria a la sociedad **COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A COAUTONOMA C.T.A.**, identificada con el NIT 827.000.616- 7, de CUARENTA MILLONES TRESCIENTOS UN MIL OCHOCIENTOS OCHENTA PESOS M/CTE (\$ 40.301.880) equivalente a MIL CIENTO DIEZ (1.110) UVT por la violación a lo dispuesto en la siguiente normatividad:

- i) *Literal k) del artículo 17 de la ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la ley en cita y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015.*
- ii) *Literal n) del artículo 17 de la ley 1581 de 2012 en concordancia con el artículo 19 ejúsdem.*

PARÁGRAFO: *El valor de la sanción pecuniaria que por esta resolución se impone, deberá consignarse en efectivo o cheque de gerencia en el Banco Popular, Cuenta No. 050000249, a nombre de Dirección del Tesoro Nacional +- Fondos Comunes, Código Rentístico No. 350300, Nit. 899999090-2. El pago deberá efectuarse dentro de los cinco (5) días hábiles siguientes a la ejecutoria de esta resolución y acreditarse en la ventanilla de Tesorería de esta Superintendencia con el original de la consignación, donde le expedirán el recibo de caja aplicado a la resolución sancionatoria. Vencido este plazo se cobrarán intereses por cada día de retraso, liquidados a la tasa del 12% efectivo anual”.*

ARTÍCULO SEGUNDO: ACLARAR la orden impartida en el artículo segundo del resuelve de la Resolución No. 53373 del 2 de septiembre de 2020 por las razones expuestas en la parte motiva de este acto administrativo, la cual quedará así:

“ARTÍCULO SEGUNDO: ORDENAR a la sociedad **COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A COAUTONOMA C.T.A.**, identificada con el NIT 827.000.616-7, que:

En cumplimiento de lo dispuesto en el literal k) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal g) del artículo 4 de la ley en cita y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015 deberá desarrollar y documentar un manual interno a través del cual se describan los procedimientos y políticas de seguridad (medidas técnicas, humanas y administrativas) que considere pertinentes, útiles y necesarias para garantizar la integridad, disponibilidad y confidencialidad de los datos personales contenidos en bases de datos físicas o automatizadas con el fin de evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulenta.

PARÁGRAFO PRIMERO: *La sociedad COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A COAUTONOMA C.T.A., identificada con el Nit.827.000.616-7, deberá acreditar el cumplimiento de lo ordenado en el anterior artículo ante esta Superintendencia dentro de los noventa (90) días hábiles siguientes a la ejecutoria de la presente decisión, aportando el respectivo documento donde se acredite la orden aquí impartida.*

PARÁGRAFO SEGUNDO: *El incumplimiento de lo ordenado en el presente acto administrativo, hará a la sociedad COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A COAUTONOMA C.T.A., acreedora de las sanciones previstas en la ley.”*

Por la cual se resuelve un recurso de apelación

ARTÍCULO TERCERO: CORREGIR la omisión del resuelve de la Resolución No. 53373 del 2 de septiembre de 2020, de acuerdo con lo expuesto en la parte motiva de este acto administrativo, por lo cual se **EXHORTA** al señor [REDACTED], identificado con [REDACTED], en su calidad de representante legal de la sociedad **COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A COAUTONOMA C.T.A.**, para que se adopten las medidas pertinentes, útiles, efectivas y verificables con el propósito de:

- 1) Evitar que se repitan hechos como los que dieron origen a la presente investigación.
- 2) Respetar y garantizar los derechos de los Titulares de los datos.
- 3) Dar estricto cumplimiento a las disposiciones legales y estatutarias sobre el tratamiento de datos personales.
- 4) Aplicar el principio de responsabilidad demostrada, observando las orientaciones de la Superintendencia de Industria y Comercio incorporadas en la "Guía para implementación del principio de responsabilidad demostrada (accountability)", con especial énfasis en utilizar mecanismos de monitoreo y control que permitan comprobar la efectividad de las medidas adoptadas para garantizar en la práctica los derechos de los Titulares de los datos personales respecto de los principios que rigen el tratamiento de datos personales, especialmente el principio de seguridad.
- 5) Hacer efectivo el pleno respeto del derecho fundamental de Habeas Data.

ARTÍCULO CUARTO: ACLARAR que las demás disposiciones de la Resolución No. 53373 del 2 de septiembre de 2020, no sufren modificación alguna.

QUINTO: Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho procede a resolver el recurso de apelación interpuesto por la sociedad COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A, a través de su apoderado, contra la Resolución No. 53373 del 2 de septiembre de 2020 y con base en lo expuesto por la sociedad, se harán las siguientes:

CONSIDERACIONES DEL DESPACHO

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

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011¹ establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destacan las siguientes:

"(...)

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

2. DE LA CONGRUENCIA ENTRE LA DENUNCIA PRESENTADA Y LA SANCIÓN EMITIDA POR ESTA SUPERINTENDENCIA.

A lo largo del recurso, la sociedad argumenta que las situaciones que dieron lugar a los cargos formulados y sancionados difieren del objeto de la denuncia, a pesar de que esta es clara.

¹ Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones.

Por la cual se resuelve un recurso de apelación

Efectivamente fue a partir de la denuncia presentada por el Titular que se dio inicio a la presente actuación administrativa, por lo cual se procedió dentro del marco del artículo 47 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo a realizar las averiguaciones preliminares correspondientes. Así, mediante oficio 18064963--00003² se solicitó a la Cooperativa dar respuesta a unos requerimientos particulares que estaban relacionados, mas no se limitaban, a los hechos de la denuncia así:

1. Sírvase remitir copia de la denuncia presentada ante la Fiscalía General de la Nación por la pérdida o extravió de la carpeta que contenía toda la historia laboral y/o el "convenio de trabajo asociado" del señor ██████████, quien estuvo vinculado en la **COOPERATIVA AUTÓNOMA DE SERGURIDAD** desde el 23 de diciembre de 2015 hasta el 15 de marzo de 2016.
2. Sírvase remitir copia del Manual de Política de tratamiento de datos personales implementado al interior de su organización.
3. Remita copia del procedimiento del ciclo del dato realizado por su organización.
4. Remita copia del manual de atención de consultas y reclamos utilizado por su organización para dar trámite a las solicitudes de los Titulares.
5. Remita copia del manual de políticas de tratamiento de seguridad implementado por su organización.
6. Informen si tienen implementado procedimientos y protocolos de gestión de incidentes. Sírvase remitir copia de esto.
7. Informe cuál fue el procedimiento adelantado una vez el denunciante puso en conocimiento la situación.
8. Informe si para la fecha de ocurrencia de los hechos (pérdida o extravió de la historia laboral y/o "convenio de trabajo asociado"), el Titular fue informado sobre esa situación.
9. Informe si se extraviaron las carpetas de otros Titulares en el incidente que tuvo lugar en sus instalaciones.
10. Indique cuáles fueron las medidas preventivas y correctivas tomadas por la sociedad luego de haberse presentado el incidente para que tales hechos no se vuelvan a presentar.

La respuesta al presente requerimiento deberá ser suscrita por el representante legal de sociedad o por apoderado debidamente constituido en un plazo que vence dentro de los ocho (8) días hábiles siguientes a la fecha de recibo de la presente comunicación.

Se le recuerda que el incumplimiento de las disposiciones de la Ley o de las órdenes o instrucciones de esta Superintendencia, puede dar lugar a responsabilidad administrativa y a la imposición de las sanciones contempladas por el artículo 21 de la Ley 1581 de 2012.

La Cooperativa respondió el oficio el 7 de marzo de 2021.³

Este tipo de requerimientos se realizan con el objetivo de verificar el cumplimiento de la Ley 1581 de 2012 por parte de la investigada, pues a través de estas averiguaciones preliminares puede esta Superintendencia concluir si posiblemente se vulneraron las normas del Régimen de Protección de Datos Personales. La decisión de iniciar una investigación administrativa y formular cargos no se realiza basándose únicamente en la denuncia presentada.

Tras realizarse las averiguaciones preliminares si se determina que el Responsable y/o Encargado del Tratamiento pudo incurrir en una violación a la norma, la cual como se mencionó puede no estar relacionada directamente a los hechos relatados por el

² Expediente digital, consecutivo 3, hoja 1 páginas 1-2.

³ Expediente digital, consecutivo 5, hoja 1 página 2.

Por la cual se resuelve un recurso de apelación

denunciante, es posible para la Dirección de Investigación de Protección de Datos Personales formular cargos en este sentido. Esto se encuentra fundamentado en las disposiciones de la Ley 1581 de 2021 la cual establece:

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.

ARTÍCULO 21. FUNCIONES. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;

(...)

e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;

f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

Como allí se evidencia corresponde a esta Delegatura garantizar el pleno cumplimiento del Régimen de Protección de Datos Personales, y se encuentra además facultada para adelantar las investigaciones del caso, incluso de oficio. Contrario a lo que considera la recurrente, la regulación colombiana no limita el campo de acción de las investigaciones a los aspectos que denuncien los ciudadanos, pues sus competencias legales van mucho más allá para cumplir los mandatos constitucionales previstos en el artículo 15 de la Constitución de la República de Colombia.

Por consiguiente, la Resolución No. 10321 de 2019 formuló cargos a la Cooperativa basándose en la denuncia presentada por el Titular el 2 de febrero de 2018 y en las averiguaciones preliminares realizadas de acuerdo con lo establecido al artículo 47 de la Ley 1437 de 2011. Cabe señalar que ni la formulación de cargos, ni la sanción y orden impuesta por medio de la Resolución No. 53373 de 2020, se alejan de los hechos objeto de la denuncia y que, en virtud de las normas señaladas, esta Superintendencia está facultada para requerir a los responsables del Tratamiento y a realizar las averiguaciones pertinentes para garantizar el cumplimiento del Régimen de Protección de Datos Personales. Así, no es de recibo el argumento de la recurrente donde manifiesta que los cargos y la sanción se impone por situaciones que no fueron objeto de queja.

3. DE LA RESPONSABILIDAD OBJETIVA EN EL DERECHO ADMINISTRATIVO SANCIONATORIO

La sociedad manifiesta que la Resolución No. 53373 de 2020, vulnera los principios del derecho administrativo sancionatorio, por incorporar una sanción por responsabilidad objetiva sin estar expresamente consagrada por la ley, y por consiguiente desconoce los principios del debido proceso aplicables a estas actuaciones.

Frente a este argumento, debe considerarse que la responsabilidad objetiva en el derecho administrativo sancionatorio, la Corte Constitucional ha manifestado:

Por la cual se resuelve un recurso de apelación

(...) El objeto del derecho administrativo sancionatorio es la prevención de las conductas que ponen en riesgo o lesionan bienes protegidos por el ordenamiento jurídico, a través de procedimientos que deben garantizar el debido proceso. En reiteradas ocasiones⁴ la Corte se ha pronunciado en el sentido de que la determinación de la responsabilidad administrativa, requiere que la infracción se haya realizado con dolo, o con culpa, como elemento que debe concurrir para la imposición de la sanción. En efecto, en la Sentencia C-597 de 1996, esta Corporación precisó que en materia sancionatoria administrativa está proscrita toda forma de responsabilidad objetiva y las faltas sólo son sancionables a título de dolo o culpa (...)

La culpabilidad constituye un elemento subjetivo esencial sobre el cual se edifica la responsabilidad administrativa (...)⁵ (énfasis añadido).

Igualmente, en este mismo sentido el Consejo de Estado frente al proceso administrativo sancionatorio y la responsabilidad objetiva ha manifestado:

“No se trata de un régimen de responsabilidad objetiva sino de una reasignación de la carga probatoria, la responsabilidad sigue siendo subjetiva porque como se desprende de lo afirmado existe la posibilidad de exoneración comprobando un comportamiento ajustado al deber objetivo de cuidado”⁶

Adicionalmente, olvida la recurrente que en materia de tratamiento de datos personales existe la responsabilidad demostrada, la cual exige que los Responsables del Tratamiento implementen medidas apropiadas, efectivas y verificables que le permitan probar el correcto cumplimiento de las normas sobre el citado tema.

Este principio guarda directa relación con la necesidad de implementar medidas internas efectivas en cada organización porque si sus decisiones y estrategias son correctas pues al mismo tiempo pasarán la prueba de corroborar que están realizando un Tratamiento debido de la información citada. Estos requisitos fueron incluidos en los artículos 26 y 27 del Decreto 1377 de 2013.

Sobre este punto, en la Sentencia C-32 del 18 de febrero de 2021 la Corte Constitucional reiteró lo anterior en los siguientes términos:

*“219. El principio de responsabilidad demostrada, conocido en el derecho comparado como *accountability* en la protección de datos personales, es incorporado por la legislación interna por el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2013. **El artículo 26 de esa normativa determina que los responsables del tratamiento de datos personales deberán demostrar, a petición de la Superintendencia de Industria y Comercio, entidad que obra como autoridad colombiana de protección de datos, que han implementado medidas apropiadas y efectivas para cumplir con las citadas normas jurídicas.***

(...)

“El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de demostrar ante la autoridad de datos que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal.”

(...)

⁴ Como se cita en las Sentencias de la Corte Constitucional C-226 de 1996 y C-720 de 2006.

⁵ Corte Constitucional, Sentencia C-699 de 2015.

⁶ Consejo de Estado Sala de lo Contencioso Administrativo, Sección Tercera, Subsección C, Consejero ponente: Enrique Gil Botero, 22 de octubre de 2012, Radicación número: 05001-23-24-000-1996-00680-01(20738)

Por la cual se resuelve un recurso de apelación

“el principio de responsabilidad demostrada no se opone a la Constitución sino que, antes bien, es desarrollo propio de la eficacia del derecho al habeas data. (...)”.
(Destacamos).

Por consiguiente, esta Superintendencia a través de la Delegatura de Protección de Datos Personales ejerce su facultad sancionatoria establecida en el artículo 21 de la Ley 1581 de 2012, dentro del marco de la responsabilidad subjetiva al demostrarse dentro de una actuación administrativa que la investigada cometió o está cometiendo una infracción contra el Régimen de Protección de Datos Personales. Para esto se debe configurar un actuar negligente por parte de la sociedad investigada para que la conducta sea sancionable, es decir, que se evidencie una responsabilidad subjetiva y no objetiva.

En el presente caso, los cargos formulados y por los cuales fue sancionada COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A. son por el incumplimiento a:

- i) El literal k) del artículo 17 de la ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la ley en cita y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015, al probarse dentro de la actuación administrativa que la sociedad no cuenta con un manual de políticas y procedimientos que garantice la seguridad de la información frente a la administración de los datos de los titulares.
- ii) El literal n) del artículo 17 de la ley 1581 de 2012 en concordancia con el artículo 19 ejúsdem, al evidenciarse en la actuación administrativa que la investigada no informó a esta Superintendencia sobre las violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los titulares.

Cada uno de los deberes que fueron incumplidos por la sociedad se encuentran debidamente establecidos en el Régimen de Protección de Datos personales, y en la Resolución recurrida se expuso de qué manera el actuar de la sociedad vulneró las normas citadas, en ningún momento la Dirección de Investigación de Protección de Datos Personales sancionó dentro del marco de la responsabilidad objetiva, por lo que no se vulneró el derecho al debido proceso de la investigada y el argumento de la recurrente no esta llamado a prosperar.

4. DE LAS CONDUCTAS SANCIONADAS

4.1. Del deber de adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley 1581 de 2012 - literal k) del artículo 17.

Frente al primero de los cargos la sociedad manifiesta que la norma mencionada como infringida no tiene relación con la conducta investigada, pues la primera establece la obligación de adoptar un Manual Interno de Políticas y Procedimientos y para atender consultas y reclamos, mientras que el cargo cuestiona no tener un “Manual de Políticas de Seguridad”. Expone que el documento es diferente al exigido en el literal k) del artículo 17 de la Ley 1581 de 2012, el cual fue aportado por la Cooperativa.

Adicionalmente advierte que no existe norma positiva que exija el "Manual de Políticas de Seguridad", por lo cual no sería posible para esta Superintendencia sancionar por un Manual que no es obligatorio para el Responsable del Tratamiento.

Por la cual se resuelve un recurso de apelación

Resalta que la Cooperativa en el escrito del 7 de marzo de 2019 aportó el Manual requerido por la Ley 1581 de 2012, el cual contiene todos los elementos requeridos en ella y que la "política de tratamiento de seguridad" fue implementada por la sociedad de acuerdo con los criterios establecidos en la "Cartilla de formatos modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios".

En vista de los argumentos expuestos, esta Delegatura considera necesario hacer las siguientes precisiones:

En primer lugar, es necesario resaltar que sin seguridad no existe debido tratamiento de datos personales. Es por eso que la regulación señala, entre otras, lo siguiente:

Literal g) del artículo 4 de la Ley 1581 de 2012:

ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES. *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*

(...)

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Literal d) del artículo 17 de la Ley 1581 de 2012:

ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. *Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*

(...)

g) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

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

La relevancia y alcance del deber de seguridad ha sido puesto de presente en los siguientes términos:

"La seguridad es un proceso dinámico en constante evolución y prueba. Se quiere que exista un nivel de seguridad apropiado en las diferentes etapas del tratamiento de datos personales en donde las medidas de seguridad sean objeto de evaluación y revisión.

Dichas medidas deben estar enfocadas para mitigar los siguientes riesgos: acceso no autorizado a los datos personales, pérdida, destrucción (accidental o no autorizada), contaminación (por virus informático) uso fraudulento, consulta, copia, modificación, adulteración, revelación, comunicación, o difusión no autorizados.

Para establecer las medidas se deben tener en cuenta, entre otras, las técnicas de seguridad existentes en general y para sectores específicos, los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse, la probabilidad y severidad del daño obtenido, la sensibilidad de la información y el contexto en el que es realizado el tratamiento y las eventuales consecuencias negativas para los titulares de los datos. (...)

Proteger la información es una condición crucial del tratamiento de datos personales. Una vez recolectada debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que

Por la cual se resuelve un recurso de apelación

pueden afectar los derechos de los titulares y de los mismos Responsables y Encargados del tratamiento de los datos. El acceso, la consulta y el uso no autorizado o fraudulento así como la manipulación y pérdida de la información son los principales riesgos naturales y humanos que se quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa o técnica.”⁷

Por su parte, la Corte Constitucional ha establecido que:

“Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

(...)

En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. (...)

Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria.”⁸ (Destacamos).

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

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

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

El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de demostrar ante la autoridad de datos que cuenta

⁷ Cfr. REMOLINA ANGARITA, Nelson. 2013. Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012. 1 ed. Bogotá: Legis Editores. Págs. 216-217

⁸ Corte Constitucional. Sentencia C – 748 del 2011.

⁹ Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012

¹⁰ Cfr. Literal d) del artículo 17 de la Ley Estatutaria 1581 de 2012

¹¹ Cfr. Artículo 26 del decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015)

Por la cual se resuelve un recurso de apelación con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal.”¹² (Destacamos)

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

Ahora, en el caso concreto, el literal k) del artículo 17 de la Ley 1581 de 2012 establece:

ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

(...)

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos; (subrayado fuera de texto)

Como allí se expone, la COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A. en su condición de Responsable del Tratamiento debe adoptar un manual interno de políticas y procedimientos que garantice el adecuado cumplimiento de la Ley 1581 de 2012, para garantizar, entre otras, el adecuado cumplimiento del principio y del deber de seguridad.

Así, la lectura que hace la recurrente de la norma no es de recibo pues como allí mismo se expone el manual interno de políticas y procedimientos debe garantizar el cumplimiento de la citada Ley, la cual incluye el principio y el deber de seguridad.

En línea con lo anterior, y lo expuesto por el Titular en la denuncia, mediante oficio 18064963-00003¹³ se requirió a la sociedad para que entre otros documentos aportara, “copia del manual de políticas de tratamiento de seguridad implementado por su organización” frente a lo que la sociedad manifestó:¹⁴

5. Remita copia del manual de políticas de tratamiento de seguridad implementando por su organización.

Dando alcance al requerimiento adjunto copia de:

- POLÍTICA DE TRATAMIENTO PROTECCIÓN DE DATOS PERSONALES DE LA COOPERATIVA AUTONOMA DE SEGURIDAD Codificada con Anexo-SIG-05,
- AVISO DE PRIVACIDAD Y AUTORIZACION PARA EL TRATAMIENTO DE DATOS PERSONALES Codificado con F-TH-29
- ACTUALIZACION DE DATOS PARA TRABAJADOR ASOCIADO Codificado con F-TH-24

Esta Delegatura procedió a revisar los documentos a los que allí se hace referencia y encuentra que por medio de estos no se acreditó que la Cooperativa contara con un Manual de Políticas de Seguridad de la Información, o que dentro de la “Política de tratamiento protección de datos personales de la Cooperativa Autónoma de Seguridad” se establecieran los lineamientos y/o políticas administrativas, humanas y técnicas que se deben adoptar por todas las áreas de la organización y cada uno de sus integrantes en el cuidado de los datos personales, con el objeto de cumplir el principio de seguridad a que se refiere la Ley 1581 de 2012.

Ahora, en términos generales, el Manual de Políticas de Seguridad, es un conjunto de lineamientos, y/o políticas administrativas, humanas y técnicas de administración de la información. Por medio del cual, la organización realiza el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar de manera eficiente el acceso y

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

¹³ Expediente digital, consecutivo 3, hoja 1 páginas 1-2.

¹⁴ Expediente digital, consecutivo 5, hoja 1 página 2.

Por la cual se resuelve un recurso de apelación

uso de la información, con base en los principios de la seguridad de la misma, que son la confidencialidad, integridad y disponibilidad, para de esta manera minimizar los riesgos asociados a la información, de acuerdo con su clasificación.

Se reitera a la sociedad que esta Superintendencia es consciente de que la pérdida de una carpeta no es, per se, evidencia de que la sociedad no cuenta con un Manual o Política de Seguridad, es por esto que en la etapa de averiguaciones preliminares se requirió a la Cooperativa para que aportara, entre otras cosas el mencionado manual. Ahora, los documentos a los cuales hace referencia la Cooperativa en el oficio y posteriormente en los descargos, alegatos de conclusión y nuevamente en el recurso, no se evidencian los mencionados procedimientos que garanticen el cumplimiento del principio de seguridad, el cual es esencial dentro del tratamiento de los datos personales. Así, la sociedad no demostró ante el requerimiento de la autoridad que cuenta con que cuenta con la institucionalidad y los procedimientos para garantizar la seguridad en el tratamiento de datos personales. Por lo tanto, el argumento de la sociedad en este sentido no está llamado a prosperar.

4.2. Del deber de informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares - literal n) del artículo 17 de la ley 1581 de 2012.

Frente al segundo cargo la recurrente manifiesta que así como expuso en los descargos y en los alegatos de conclusión esta norma no debe ser aplicada para el caso de estudio pues considera que los Códigos de Seguridad son aplicables a los sistemas de cómputo para proteger la información y su legitimidad, y que de acuerdo a lo establecido en la norma serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento, excluyendo de aplicación a las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Así, expone que las carpetas físicas no contienen códigos de seguridad pues las mismas no están contenidas en bases de datos, más aún cuando la carpeta del señor [REDACTED] no contiene información sensible. Afirma que al tratarse de una hoja de vida y sus respectivos soportes no es susceptible de tratamiento por cuanto es de uso personal y doméstico para la empresa.

Además, argumenta que el extravío de la carpeta, al tratarse de documentos de reserva legal en virtud de la Ley 1266 de 2008, es competencia de las autoridades jurisdiccionales. Manifiesta también que la carpeta fue localizada posteriormente y la documentación se encuentra en poder de la Cooperativa, como se demostró con la copia que se aportó con los descargos. Finalmente, afirma que esta Superintendencia incurrió en una inadecuada adecuación típica y que no tuvo en cuenta los argumentos planteados por la recurrente.

Al analizar los argumentos que expone la recurrente este Despacho encuentra que son reiterativos frente a lo expuesto en el escrito de descargos y los alegatos de conclusión presentados por la cooperativa. En este sentido encuentra que en la Resolución 53373 del 2 de septiembre de 2020 la Dirección de Investigación de Protección de Datos Personales expuso de manera completa y detallada por qué el literal n) del artículo 17 le es aplicable a las bases de datos físicas, porque la sociedad si realiza tratamiento sobre los datos del señor [REDACTED] y porque no estamos frente al caso de un tratamiento dentro del ámbito personal y doméstico. Así que en ningún momento se han desestimado los argumentos de la sociedad por parte de esta Superintendencia.

Por la cual se resuelve un recurso de apelación

No obstante, en vista de que la cooperativa reitera los argumentos, este Despacho se pronunciará sobre los mismos.

En primer lugar, la ley 1581 de 2012 establece:

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

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

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

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

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

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

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

(...)

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

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

*“El tratamiento de datos personales, en los términos que fueron definidos en el artículo 3, literal g) del proyecto en estudio, de conformidad con los recientes estándares internacionales sobre la materia **“es cualquier operación o conjunto de operaciones, sean o no automatizadas, que se apliquen a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión”**. Ese proceso de tratamiento de datos personales, que puede ser público o privado, requiere, en los términos de la jurisprudencia de esta Corporación, definiciones claras sobre “el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos.” (Negrita fuera del texto)*

En concordancia con lo anterior, el Decreto Único 1074 de 2015 dispone:

"Artículo 2.2.2.26.2.6. Formas de Tratamiento. Los datos personales contenidos en bases de datos podrán ser tratados de manera automatizada o manual. Son bases de datos manuales los archivos cuya información se encuentra organizada y almacenada de manera física y bases de datos automatizadas aquellas que se almacenan y administran con la ayuda de herramientas informáticas." (Subrayado fuera del texto)

Así, la ley 1581 de 2012 y las disposiciones que la reglamentan son claras al establecer que una base de datos puede ser manual o automatizada y los datos almacenados en ella encontrarse de manera física o digital. En cualquiera de estos escenarios, se aplicarán las disposiciones contenidas en la citada Ley.

Las carpetas físicas que son almacenadas o conservadas por la Cooperativa hacen parte de las bases de datos sobre las cuales realiza tratamiento la sociedad, la clasificación interna que se realice según el objeto o la finalidad del tratamiento será determinada por la empresa

Por la cual se resuelve un recurso de apelación

de acuerdo con sus actividades. Sin embargo, en ningún momento el medio en el cual se recolecte y almacene la información es un motivo para no aplicarle a estas bases de datos las disposiciones del Régimen de Protección de Datos Personales. Así las cosas, no se ajusta a derecho el argumento de la recurrente según el cual el literal n) del artículo 17 no le es aplicable al incidente en cuestión pues se trata de una base de datos física.

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

*“no puede entenderse que el primer contenido normativo del literal a) se extienda al tratamiento de cualquier dato cuando circule internamente, como pretende ASOBANCARIA. En primer lugar, (...) para que opere la excepción, por voluntad del legislador, se requiere además que los datos sean mantenidos por una persona natural en su esfera íntima. (...) En segundo lugar, (...) **El que los datos no circulen o circulen internamente, no asegura que su tratamiento no pueda tener consecuencias adversas para su titular. Piénsese por ejemplo en las hojas de vida de los empleados de una empresa mantenidas en el ámbito interno; si bien no van a ser divulgadas a terceros, su tratamiento y circulación interna sí puede traer consecuencias negativas para el titular del dato (por ejemplo, en términos sancionatorios o de ascensos), razón por la cual deben estar sujetas a las reglas generales que consagra el proyecto de ley**”.*¹⁵ (Negrita fuera del texto)

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

El presente caso no se encuentra enmarcado dentro de tal escenario pues quien realiza el tratamiento no es una persona natural, ni se trata de un contexto de vida privada o familiar. La misma Corte Constitucional hace referencia al caso de las hojas de vida de los empleados de una empresa, las cuales a pesar de que se mantienen en un ámbito interno, el mismo no se considera como “personal o doméstico” y como consecuencia no puede considerarse que están fuera del ámbito de aplicación de la Ley 1581 de 2012. Así, el argumento de la recurrente en este sentido tampoco está llamado a prosperar.

Ahora, la sociedad hace referencia a que entre los datos tratados no hay datos sensibles, motivo por el cual no están contenidos en una base de datos y no le son aplicables los códigos de seguridad. En cuanto a este argumento se señala que el tratamiento de datos sensibles puede “generar altos riesgos en términos de vulneración del habeas data, la intimidad e incluso la dignidad de los titulares de los datos”¹⁶, razón por la cual, los Responsables y Encargados que realizan tratamiento de este tipo de datos “tienen una responsabilidad reforzada que se traduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y los deberes del título VI”¹⁷ de la ley 1581 de 2012. Sin embargo, en ningún momento significa que si no se tratan datos sensibles no le son aplicables a las bases de datos las disposiciones de la citada ley.

En cuanto a la afirmación de que se tratan de datos reservados en virtud de las disposiciones de la Ley 1266 de 2008, se resalta el ámbito de aplicación de esta ley, el cual dispone:

¹⁵ Corte Constitucional, sentencia C-748 de 2011, numeral 2.4.5.3.1

¹⁶ Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.8.4

¹⁷ Loc. cit.

Por la cual se resuelve un recurso de apelación

ARTÍCULO 1o. OBJETO. La presente ley tiene por objeto desarrollar 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 a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países. (Subrayado fuera del texto)

Así, las disposiciones citadas por la recurrente no son aplicables al presente caso ya que este no se enmarca en el ámbito de aplicación de la Ley 1266 de 2008, pues no se trata de información financiera y crediticia, comercial, de servicios. Así, la regulación aplicable es el Régimen General de Protección de Datos personales establecido en la Ley Estatutaria 1581 de 2012 y las normas que la reglamentan.

En vista de lo expuesto, a la Cooperativa le es aplicable el deber contenido en el literal n) del artículo 17 de la Ley 1581 y debió informar a esta Superintendencia acerca del incidente ocurrido pues se trata de una violación a los códigos de seguridad y existió un riesgo en la administración de la información de los Titulares o del Titular en este caso. Por ende, el argumento según el cual se incurrió en una indebida adecuación típica tampoco está llamado a prosperar. Adicionalmente, se resalta que el hecho de que la carpeta apareciera con posterioridad no exime a la sociedad de haber cumplido con este deber porque puso en riesgo la seguridad de la información del Titular.

5. DEL AGOTAMIENTO DEL REQUISITO DE PROCEDIBILIDAD

La recurrente manifiesta que conforme al artículo 16 de la Ley 1581 de 2012, el Titular solo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento. Argumenta que en el presente caso el señor [REDACTED] no agotó el requisito previo de procedibilidad pues la petición presentada el 29 de marzo de 2017 no cumple los requisitos de reclamo para tal efecto.

El artículo 16 de la Ley 1581 de 2012 citado por la recurrente expone:

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

Este artículo hace parte del Título V de la citada Ley el cual hace referencia a los procedimientos para las consultas o reclamos ante los Responsables y Encargados del Tratamiento. Se trata entonces del procedimiento a seguir cuando los Titulares o sus causahabientes deseen consultar la información personal del Titular que repose en cualquier base de datos,¹⁸ o que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley.¹⁹

Junto con la denuncia presentada por el señor [REDACTED] en febrero de 2018, donde narra los hechos objeto de la denuncia, el Titular aporta copia del oficio con radicado 17-366445-2 de esta Superintendencia en donde se manifiesta lo expuesto por la recurrente frente al requisito de procedibilidad. No obstante, en el mismo oficio se establece que se remitirá su queja al responsable del Tratamiento con el fin de que fuera atendido dentro del término que

¹⁸ Ley 1581 de 2012 artículo 14.

¹⁹ Ley 1581 de 2012 artículo 15.

dispone la ley así:²⁰

Por la cual se resuelve un recurso de apelación

Bogotá D.C.
7110

RAD: 17-366445--00002-000
DEP: 7110 HABEASDATA
TRA: 384 HABEAS DATA
ACT: 330 COMUNICACI

FECHA: 2017-12-20 11:04:09
EVE: 328 DENUNCIAS
FOLIOS: 1

CORREO CERTIFICADO

Señor (a) (es)

Asunto: Radicación: 17-366445--00002-000
Trámite: 384 HABEAS DATA
Evento: 328 DENUNCIAS
Actuación: 330 COMUNICACI
Folios: 1

Respetado (a) (s) señor (a) (es)

De acuerdo con lo establecido por el literal b del artículo 21 de la Ley 1581 de 2012, la Superintendencia de Industria y Comercio tiene competencia para "(a)delantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos". Igualmente el artículo 16 de la ley citada dispone que "(e) Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento".

Del mismo modo, en cuanto a la reclamación dirigida ante el Responsable del Tratamiento o al Encargado del Tratamiento, el numeral 3 del artículo 15 de la ley en mención establece que "(e)l término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término".

Revisando la documentación anexa a su queja, se encuentra que no aparece prueba que acredite que presentó reclamo ante el Responsable o al Encargado del Tratamiento, relacionado con su derecho de hábeas data.

Por lo anterior este Despacho procederá a dar traslado del reclamo presentado a COOPERATIVA AUTONOMA DE SEGURIDAD C.T.A., con el fin de que sea atendido dentro del término previsto por la ley.

estar favor indique el número de radicación que se indica
nuación: Radicación: 17-366445--00002-000 - 2017-12-20 11:04:09
SUPERINTENDENCIA



Si COOPERATIVA AUTONOMA DE SEGURIDAD C.T.A., no da respuesta favorable o dentro del término previsto por la ley, usted podrá presentar una nueva reclamación, adjuntando copia de la respuesta desfavorable suministrada.

Atentamente,

Claudia B. García
CLAUDIA BIBIANA GARCIA VARGAS
Coordinadora Grupo de trabajo de Habeas Data

Elaboró: GERMAN CERON
Revisó: CLAUDIA GARCIA
Aprobó: CLAUDIA GARCIA

En vista de lo expuesto en este oficio, el Titular también presenta con su nueva denuncia copia de la respuesta negativa otorgada por parte de la Cooperativa:²¹

²⁰ Expediente Digital 18-64963 consecutivo 1 hoja 1 páginas 19-20.

²¹ Expediente Digital 18-64963 consecutivo 1 hoja 1 página 21.

VERSIÓN PÚBLICA

Por la cual se resuelve un recurso de apelación



1b
COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A.
NIT. 827.000.616 - 7

Bogotá D.C., 25 de enero de 2018



Ref. Contestación radicado No. 17-366445-00003-000.

Cordial saludo,

En atención a su solicitud me permito manifestar lo siguiente, a saber:

En Cuanto a las peticiones.

Primero: Me permito manifestarle que no se accede a lo solicitado pues como bien se le ha informado la carpeta donde reposaba su documentación se encuentra traspapelada, razón por la cual se presentó denuncia por la misma y del cual se le allegó copia del mismo, sin que usted haya sufrido daño o perjuicio alguno, por lo que no es viable la reparación solicitada por usted.

De esta manera se da contestación de fondo, conforme lo ordenado por la Superintendencia de Industria y Comercio, en oficio de la referencia.

Atentamente,



VIGILADO SUPERINTENDENCIA N.º 6817 del 22 de Septiembre de 2016

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

6. DE LA CARGA DE LA PRUEBA.

La recurrente también manifiesta que la carga de la prueba esta a cargo del investigador, y que este Despacho invirtió la carga de la prueba “al sancionar a la empresa bajo las consideraciones generales que el investigado no logró desvirtuar los cargos formulados”. Afirma además que se desconoció la prueba allegada por la recurrente por medio de la cual acredita el cumplimiento el literal k) del artículo 17 al expedir el Manual Interno de Políticas y Procedimientos y de Atención de Consultas y Reclamos.

En cuanto a estos argumentos esta Delegatura señala que la jurisprudencia colombiana en general, ha reasignado la responsabilidad de la prueba a quien esté en mejores condiciones para probar dentro del proceso. Por lo que, la carga probatoria no actúa en función de la parte que se limita a alegar el hecho que se pretende probar. Al respecto, la Corte Constitucional ha señalado:

“Esta institución pretende que quien concurre a un proceso en calidad de parte asuma un rol activo y no se limite a refugiarse en la diligencia del juez ni se beneficie de las dificultades probatorias o mala fortuna de su contraparte. En otras palabras, ‘las partes en el proceso deben cumplir con el deber de diligencia en lo que pretenden probar. Ninguna debe obrar con inercia porque ello causa que las consecuencias adversas de la decisión sean deducidas en su contra. El proceso no premia la estrategia sino la solución del conflicto con la participación de las partes’²²

En correspondencia con lo anterior, este Despacho considera importante resaltar que la recurrente en ningún momento, aportó las pruebas esperadas y suficientes en este tipo de actuaciones. Lo anterior, a pesar de haber contado con las oportunidades legales para tal fin.

²² Corte Constitucional, Sentencia T-733 de 2013.

Por la cual se resuelve un recurso de apelación

En orden a desatar el recurso, vale la pena puntualizar algunas disposiciones normativas al respecto.

La Ley 1437 de 2011 en su artículo 40 se refiere a las pruebas así:

“Durante la actuación administrativa y hasta antes de que se profiera la decisión de fondo se podrán aportar, pedir y practicar pruebas de oficio o a petición del interesado sin requisitos especiales. Contra el acto que decida la solicitud de pruebas no proceden recursos. El interesado contará con la oportunidad de controvertir las pruebas aportadas o practicadas dentro de la actuación, antes de que se dicte una decisión de fondo.

(...)

Serán admisibles todos los medios de prueba señalados en el Código de Procedimiento Civil.”

De esta manera, la misma norma hace una remisión expresa a los medios de prueba del hoy Código General del Proceso.

Ahora, la jurisprudencia se ha pronunciado frente a la carga probatoria así:

“Desde luego, al juez no le basta la mera enunciación de las partes para sentenciar la controversia, porque ello sería tanto como permitirles sacar beneficio del discurso persuasivo que presentan; por ende, la ley impone a cada extremo del litigio la tarea de traer al juicio de manera oportuna y conforme a las ritualidades del caso, los elementos probatorios destinados a verificar que los hechos alegados efectivamente sucedieron, o que son del modo como se presentaron, todo con miras a que se surta la consecuencia jurídica de las normas sustanciales que se invocan”²³

Finalmente, y no menos importante, la regulación colombiana sobre tratamiento de datos impone al Responsable del Tratamiento el deber demostrar que ha adoptado medidas efectivas para cumplir la ley (Deber de Responsabilidad demostrada). Esto se deriva de lo expresamente señalado en el Decreto 1377 de 2013²⁴ que ordena lo siguiente: **“Artículo 26. Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto (...)**” (Destacamos y subrayamos).

Sobre este punto, recalamos que en la sentencia C-32 del 18 de febrero de 2021 la Corte Constitucional señaló que:

*“219. El principio de responsabilidad demostrada, conocido en el derecho comparado como *accountability* en la protección de datos personales, es incorporado por la legislación interna por el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2013. El artículo 26 de esa normativa determina que **los responsables del tratamiento de datos personales deberán demostrar**, a petición de la Superintendencia de Industria y Comercio, entidad que obra como autoridad colombiana de protección de datos, que han implementado medidas apropiadas y efectivas para cumplir con las citadas normas jurídicas. (...)*

“El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de demostrar ante la autoridad de datos que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal.”

(...)

²³ Corte Suprema de Justicia, Sala de Casación Civil, Sentencia de 28 de mayo de 2010. Exp. 23001-31-10-002-1998-00467-01.M.P. Edgardo Villamil Portilla.

²⁴ Incorporado en el Decreto 1074 de 2015

Por la cual se resuelve un recurso de apelación

“el principio de responsabilidad demostrada no se opone a la Constitución sino que, antes bien, es desarrollo propio de la eficacia del derecho al habeas data. (...)” (Destacamos)

De manera que la Superintendencia de Industria y Comercio obró dentro del marco de sus facultades legales para, de una parte, garantizar a las personas el Derecho Fundamental de la Protección de Datos Personales junto con el correcto Tratamiento de esa información y, de otra, respetar el debido proceso en cabeza de la Cooperativa.

En línea con lo anterior, tanto la investigación administrativa como la sanción impuesta se hicieron observando lo que ordena la regulación colombiana.

Al respecto, este Despacho advierte que en ningún momento los actos o actuaciones de esta Delegatura, en el curso del proceso han estado en contravía del derecho, como erróneamente lo da a entender la recurrente. Esto, bajo el entendido de que en estas materias se tratan temas de magnitud constitucional y legal.

Esta entidad aplicó y respetó las garantías procesales necesarias, y en todas las etapas respectivas se emitieron las resoluciones y actos administrativos a que hubo lugar. Los que, en ninguna circunstancia fueron arbitrarios. Por el contrario, lo que sí hizo esta Superintendencia, fue propender por la correcta aplicación de las normas y los principios que las fundamentan.

Adicionalmente, este proceso administrativo sancionatorio está compuesto de una serie de actos o actuaciones con un orden de continuidad establecido. En el que los tiempos y etapas que en él se fijan, son disposiciones de orden público y de obligatorio cumplimiento.

Tal como está el expediente, es posible verificar que en todo el camino de la actuación administrativa, la Superintendencia de Industria y Comercio ofreció las garantías que le permitieran a la recurrente evaluar las condiciones de transparencia y seguridad jurídica que caracterizan estos procesos.

Así no se accederá a la solicitud de la recurrente de revocar la Resolución No. 53373 del 2 de septiembre de 2020.

7. DE LA GRADUACIÓN Y PROPORCIONALIDAD DE LA SANCIÓN.

En primer lugar, se resalta que el monto de la multa impuesta a la investigada, es el resultado del análisis del daño y/o puesta en peligro de los intereses jurídicos tutelados en el trámite de la primera instancia de esta actuación administrativa.

A lo largo de la presente actuación administrativa se logró demostrar que la sociedad vulneró los deberes establecidos en el literal k) del artículo 17 de la ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la ley en cita y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015, al probarse dentro de la actuación administrativa que la sociedad no cuenta con un manual de políticas y procedimientos que garantice la seguridad de la información frente a la administración de los datos de los titulares y el literal n) del artículo 17 de la ley 1581 de 2012 en concordancia con el artículo 19 ejúsdem, al evidenciarse en la actuación administrativa que la investigada no informó a esta Superintendencia sobre las violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los titulares.

Por la cual se resuelve un recurso de apelación

Ahora, el artículo 23²⁵ de la Ley Estatutaria 1581 de 2012 determina las sanciones que puede imponer esta Superintendencia a los Responsables y Encargados del Tratamiento. Revisado el expediente y el contenido de la resolución recurrida, se encuentra entonces que de los criterios de graduación contenidos en el artículo 24 de la Ley Estatutaria 1581 de 2012, **únicamente** se tuvo en cuenta aquél que habla de la dimensión del daño o peligro a los intereses jurídicamente tutelados, pues efectivamente se encontró probado que la Cooperativa, incumplió los deberes mencionados.

Respecto del criterio de atenuación establecido en el literal f) del artículo 24²⁶ su aplicación fue descartada en la medida que la investigada a lo largo de la actuación no reconoció o aceptó expresamente la comisión de la infracción antes de la imposición de la sanción.

Sin embargo, en vista del análisis realizado y las modificaciones introducidas por la Resolución No. 9275 del 26 de febrero de 2021, este Despacho coincide con la decisión de disminuir la sanción impuesta y procederá a confirmar la Resolución 53373 del 2 de septiembre de 2020 con las modificaciones realizadas por medio de la Resolución No. 9275 del 26 de febrero de 2021 y no se pronunciará de manera adicional al respecto.

Así las cosas, se encuentra que el monto de la sanción en el citado acto administrativo, es proporcional, en consideración a los hechos que le sirvieron de causa y la motivación del acto administrativo recurrido. No sobra señalar que la sanción aquí impuesta, tiene como objetivo que la sociedad en el futuro no incurra en violaciones al derecho de hábeas data de los Titulares de la información y, en su defecto, cumpla a cabalidad con las disposiciones de la Ley Estatutaria 1581 de 2012 y demás normas que rigen el sistema de protección de datos personales en Colombia.

Finalmente, resulta pertinente resaltar lo siguiente:

- I. La multa inicial de \$100,055,670 impuesta mediante la resolución 53373 de 2020 fue reducida a \$40,301,880 por la resolución 9275 de 2021 mediante la cual se resolvió el recurso de reposición. En otras palabras, la multa se disminuyó en un 59%.
- II. La multa de (\$40.301.880 equivale al 2,05% del máximo legal permitido (2000 salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012).
- III. El monto de dicha sanción es el resultado del análisis del daño y/o puesta en peligro de los intereses jurídicos tutelados en el trámite de la primera instancia de esta actuación administrativa. Así como del incumplimiento de los deberes impuestos por la Ley 1581 de 2012 a los Responsables del Tratamiento de los Datos personales.

²⁵ **Artículo 23. Sanciones.** La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

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

²⁶ "f) El reconocimiento o aceptación expresas que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar."

Por la cual se resuelve un recurso de apelación

- IV. La Resolución recurrida fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Asimismo, también fue el resultado de la valoración fáctica y probatoria de la primera instancia que llevó a concluir y comprobar la vulneración al derecho de *habeas data* del Titular y en particular los mandatos legales señalados.
- V. Las sanciones que se imponen dentro de esta clase de procesos, no derivan de los daños o perjuicios causados a los Titulares por incumplir la regulación sobre tratamiento de datos personales. Es decir, las normas que protegen el derecho de *habeas data o protección de datos personales* no se refieren a la responsabilidad civil de los Responsables del Tratamiento de Datos.
- VI. La vulneración del derecho de *habeas data o la protección de datos personales* no solo afecta al Titular, también pone en riesgo los derechos de toda la sociedad. Por esto, las sanciones no pueden ni deben tratarse como una cuestión insignificante o de poca cuantía, ni mucho menos como si las incidencias del proceso lo convirtieran en uno de indemnización de daños y perjuicios. Esto, en razón a que existe de por medio una trasgresión flagrante a los derechos humanos de un ciudadano, lo cual es suficiente para entender la gravedad de la conducta, sin necesidad de acudir a forzosos razonamientos o teorías complicadas, a fin de desentender o negar una verdad inconcusa, cual es la del quebrantamiento de derechos constitucionales.

Recuérdese que, según la Declaración Universal de los Derechos Humanos, “*el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad*”²⁷. Por eso, según dicho documento, se considera “*esencial que los derechos humanos sean protegidos por un régimen de Derecho*”. No debe olvidarse que el respeto de los Derechos Humanos es un elemento esencial de la democracia²⁸. Así las cosas, recalcamos, la violación de Derechos Humanos es una conducta gravísima que no solo atenta contra los intereses de un individuo en particular sino de la sociedad en general.

Con apoyo en estos argumentos, se confirmará la Resolución 53373 del 2 de septiembre de 2020 con las modificaciones realizadas por medio de la Resolución No. 9275 del 26 de febrero de 2021.

8. RESPECTO DE LA ORDEN IMPARTIDA EN EL ACTO ADMINISTRATIVO IMPUGNADO

La recurrente solicita que se aclare la orden impartida en el artículo segundo de la Resolución No. 53373 de 2020, de desarrollar y documentar un manual interno a través del cual se describan los procedimientos para garantizar la seguridad en la custodia de la información personal a cargo de la COOPERATIVA, en relación con el exhorto al representante legal de la sociedad establecido en el artículo noveno de la parte considerativa de la resolución recurrida.

Nuevamente manifiesta que con los descargos se adjuntó el "Manual Interno de Políticas y Procedimientos y de atención de consultas y reclamos" el cual contiene todos los aspectos

²⁷ Organización de las Naciones Unidas (1948). Declaración Universal de los Derechos Humanos.

²⁸ Artículo 3 de la Carta Democrática Interamericana la cual se puede consultar en: http://www.oas.org/OASpage/esp/Documentos/Carta_Democratica.htm

Por la cual se resuelve un recurso de apelación

regulados por la Ley 1581 de 2012 y solicita se indique cuales son las deficiencias del manual frente a la política de tratamiento de seguridad implementado por la Cooperativa.

Este Despacho encuentra que la Dirección de Investigación de Protección de Datos Personales por medio de la Resolución No. 9275 del 26 de febrero de 2021, aclaró la orden contenida en la Resolución No. 53373 del 2 de septiembre de 2020 estableciendo lo siguiente:

“En primer lugar, la orden administrativa impartida es independiente al exhorto al representante legal. La primera de ellas busca que la recurrente establezca un Manual Interno de Políticas y Procedimientos de Seguridad para que la sociedad dé cumplimiento al deber previsto en el literal k) del artículo 17 de la Ley 1581 de 2012 y se propenda hacia la seguridad de las bases de datos que son sometidas a Tratamiento. El segundo, es una recomendación que este Despacho hace al representante legal de la compañía para que se garantice el pleno cumplimiento del régimen general de protección de datos personales y el efectivo ejercicio del derecho fundamental de hábeas data por parte de los Titulares y así, también evite la recurrente incurrir nuevamente en vulneraciones a los deberes que en calidad de Responsable de la información están a su cargo por mandato de la Ley 1581 de 2012.”

Ahora, como ya se expuso, la Cooperativa no cuenta con una Política de Seguridad de la información, por lo que esta orden esta encaminada a que la sociedad documente e implemente dicho manual.

Es de resaltar que el literal g del artículo 4 de la Ley 1581 de 2012, antes citado, establece de manera específica que las medidas de seguridad se deben adoptar teniendo en cuenta diversos factores **que son propios de cada organización** entre los que se encuentran su tamaño y naturaleza jurídica, la naturaleza de los datos tratados, el tipo de tratamiento al que se someta la información y los riesgos potenciales que implique para los titulares la recolección y posterior uso o circulación de esos datos.

Por lo anterior, son los Responsables y Encargados quienes deben establecer los lineamientos y/o políticas administrativas, humanas y técnicas que dependiendo de sus necesidades, tamaño, estructura organizacional, naturaleza de los datos que tratan, crean se deben adoptar en el cuidado de los datos personales. Así no puede esta Superintendencia establecer de manera específica las medidas que debe llevar a cabo la sociedad para adecuar sus acciones a lo establecido en la Ley.

Aunque las razones anteriores son suficientes para confirmar la Resolución 53373 del 2 de septiembre de 2020, esta Delegatura considera pertinente destacar lo siguiente respecto de (i) Responsabilidad Demostrada (Accountability) y Compliance en el Tratamiento de Datos Personales, y (ii) Responsabilidad Personal de los Administradores.

9. RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY) Y “COMPLIANCE” EN EL TRATAMIENTO DE DATOS PERSONALES

La regulación colombiana le impone al Responsable del tratamiento la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia “existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante”²⁹.

²⁹ Cfr. Corte Constitucional, sentencia T-227 de 2003

Por la cual se resuelve un recurso de apelación

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

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

El artículo 26³⁰ -titulado DEMOSTRACIÓN- establece que “los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012”. Así resulta imposible ignorar la forma en que el responsable o encargado del tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales.

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la “Guía para implementación del principio de responsabilidad demostrada (accountability)”³¹.

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

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

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

³⁰ El texto completo del artículo 26 del decreto 1377 de 2013 ordena lo siguiente: Artículo 26. Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

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

³¹ El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

Por la cual se resuelve un recurso de apelación

El principio de responsabilidad demostrada –*accountability*– demanda implementar acciones de diversa naturaleza³² para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los Responsables del tratamiento implementen medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

Dichas medidas deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

El principio de responsabilidad precisa menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido tratamiento de los datos personales. El éxito del mismo dependerá del compromiso real de todos los miembros de una organización. Especialmente, de los directivos de las organizaciones, pues, sin su apoyo sincero y decidido cualquier esfuerzo será insuficiente para diseñar, llevar a cabo, revisar, actualizar y/o evaluar los programas de gestión de datos.

Adicionalmente, el reto de las organizaciones frente al principio de responsabilidad demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones.

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que “la autorregulación sólo redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que **no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales**”³³ (Destacamos)

El principio de responsabilidad demostrada busca que los mandatos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las organizaciones sean proactivos respecto del tratamiento de la información de manera que por iniciativa propia adopten medidas estratégicas capaces de garantizar los derechos de los titulares de los datos personales y su gestión siempre sea respetuosa de los derechos humanos.

Aunque no es espacio para explicar cada uno de los anteriores aspectos mencionados en la guía³⁴, ponemos de presente que el principio de responsabilidad demostrada se articula con el concepto de “compliance” en la medida que éste hace referencia al “conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos”³⁵.

³² Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humanas y de gestión que involucran procesos y procedimientos.

³³ Cfr. Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Mayo de 5 de 2006. En aquel entonces, la RIPD expidió un documento sobre autorregulación y protección de datos personales que guarda cercana relación con “accountability” en la medida que la materialización del mismo depende, en gran parte, de lo que internamente realicen las organizaciones y definan en sus políticas o regulaciones internas.

³⁴ El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

³⁵ Cfr. World Compliance Association (WCA). <http://www.worldcomplianceassociation.com/> (última consulta: 6 de noviembre de 2018)

Por la cual se resuelve un recurso de apelación

También se ha afirmado que “*compliance es un término que hace referencia a la gestión de las organizaciones conforme a las obligaciones que le vienen impuestas (requisitos regulatorios) o que se ha autoimpuesto (éticas)*”³⁶. Adicionalmente se precisa que “ya no vale solo intentar cumplir” la ley sino que las organizaciones “deben asegurarse que se cumple y deben generar evidencias de sus esfuerzos por cumplir y hacer cumplir a sus miembros, bajo la amenaza de sanciones si no son capaces de ello. Esta exigencia de sistemas más eficaces impone la creación de funciones específicas y metodologías de compliance”³⁷.

Por tanto, las organizaciones deben “implementar el *compliance*” en su estructura empresarial con miras a acatar las normas que inciden en su actividad y demostrar su compromiso con la legalidad. Lo mismo sucede con “*accountability*” respecto del tratamiento de datos personales.

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del *compliance* y buena parte de lo que implica el principio de responsabilidad demostrada (*accountability*). En la mencionada guía se considera fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un “*sistema de administración de riesgos asociados al tratamiento de datos personales*”³⁸ 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*”³⁹.

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

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

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

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

³⁶ Cfr. Bonatti, Francisco. Va siendo hora que se hable correctamente de compliance (III). Entrevista del 5 de noviembre de 2018 publicada en Canal Compliance: <http://www.canal-compliance.com/2018/11/05/va-siendo-hora-que-se-hable-correctamente-de-compliance-iii/>

³⁷ Idem

³⁸ Cfr. Superintendencia de Industria y Comercio (2015) “*Guía para implementación del principio de responsabilidad demostrada (accountability)*”. Págs 16-18

³⁹ Ibid. P 16

Por la cual se resuelve un recurso de apelación

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

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

Ahora, según el artículo 22 de la ley 222 de 1995⁴⁰ la expresión administradores comprende al “representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones”. Cualquiera de ellos tiene la obligación legal de garantizar los derechos de los titulares de los datos y de cumplir la ley 1581 de 2012 y cualquier otra norma concordante. Por esto, el numeral segundo del artículo 23 de la Ley 222 de 1995 determina que los administradores deben “**obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios**”, y además, en el ejercicio de sus funciones deben “**velar por el estricto cumplimiento de las disposiciones legales o estatutarias**”. (Destacamos)

En vista de lo anterior, la regulación no exige cualquier tipo de cumplimiento de la ley, sino uno calificado. Es decir, ajustado o con exactitud a lo establecido en la norma. Velar por el estricto cumplimiento de la ley exige que los administradores actúen de manera muy profesional, diligente y proactiva para que en su organización la regulación se cumpla de manera real y no formal con la efectividad y rigurosidad requeridas.

Por eso, los administradores deben cuidar al detalle y con perfecta seguridad este aspecto. No basta solo con ser guardianes, deben ser promotores de la correcta y precisa aplicación de la ley. Esto, desde luego, los obliga a verificar permanentemente si la ley se está o no cumplimiento en todas las actividades que realiza su empresa u organización.

El artículo 24⁴¹ de la Ley 222 de 1995, presume la culpa del administrador “*en los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos*”.

⁴⁰ Ley 222 de 1995 “Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones”

⁴¹ El texto completo del artículo 24 de la ley 222 de 1995 dice lo siguiente: “Artículo 24. RESPONSABILIDAD DE LOS ADMINISTRADORES. El artículo 200 del Código de Comercio quedará así:

Artículo 200. Los administradores responderán solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros.

No estarán sujetos a dicha responsabilidad, quienes no hayan tenido conocimiento de la acción u omisión o hayan votado en contra, siempre y cuando no la ejecuten.

En los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos, se presumirá la culpa del administrador.

De igual manera se presumirá la culpa cuando los administradores hayan propuesto o ejecutado la decisión sobre distribución de utilidades en contravención a lo prescrito en el artículo 151 del Código de Comercio y demás normas sobre la materia. En estos casos el administrador responderá por las sumas dejadas de repartir o distribuidas en exceso y por los perjuicios a que haya lugar.

Si el administrador es persona jurídica, la responsabilidad respectiva será de ella y de quien actúe como su representante legal.

Se tendrán por no escritas las cláusulas del contrato social que tiendan a absolver a los administradores de las responsabilidades antedichas o a limitarlas al importe de las cauciones que hayan prestado para ejercer sus cargos.”

Por la cual se resuelve un recurso de apelación

Dicha presunción de responsabilidad exige que los administradores estén en capacidad de probar que han obrado con lealtad y la diligencia de un experto. Es decir, como un *“buen hombre de negocios”*, tal y como lo señala su artículo 23.

Adicionalmente, no debe perderse de vista que los administradores responden “solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros”⁴². Las disposiciones referidas, prevén unos elementos de juicio ciertos, (i) *el alto nivel de responsabilidad jurídica y económica en cabeza de los administradores*, y (ii) *el enorme profesionalismo y diligencia que debe rodear su gestión en el tratamiento de datos personales*.

En virtud de todo lo anterior, este Despacho encuentra ajustado a derecho el exhorto realizado al Representante Legal de la COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A..

11. CONCLUSIONES:

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

1. Se confirmó que la recurrente infringió las normas sobre protección de Datos personales consagradas en:
 - a. El literal k) del artículo 17 de la ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la ley en cita y el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015, al probarse dentro de la actuación administrativa que la sociedad no cuenta con un manual de políticas y procedimientos que garantice la seguridad de la información frente a la administración de los datos de los titulares
 - b. El literal n) del artículo 17 de la ley 1581 de 2012 en concordancia con el artículo 19 ejúsdem, al evidenciarse en la actuación administrativa que la investigada no informó a esta Superintendencia sobre las violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los titulares.
2. La regulación colombiana no limita el campo de acción de las investigaciones a los aspectos que denuncien los ciudadanos, pues sus competencias legales van mucho más allá para cumplir los mandatos constitucionales previstos en el artículo 15 de la Constitución de la República de Colombia.
3. La ley 1581 de 2012 y las disposiciones que la reglamentan son claras al establecer que una base de datos puede ser manual o automatizada y los datos almacenados en ella encontrarse de manera física o digital. En cualquiera de estos escenarios, se aplicarán las disposiciones contenidas en la citada Ley.
4. La multa inicial de \$100,055,670 impuesta mediante la resolución 53373 de 2020 fue reducida a \$40,301,880 por la resolución 9275 de 2021 mediante la cual se resolvió el recurso de reposición. En otras palabras, la multa se disminuyó en un 59%.
5. La multa de (\$40.301.880 equivale al 2,05% del máximo legal permitido (2000 salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012).

⁴² Cfr. Parte inicial del artículo 24 de la ley 222 de 1995

Por la cual se resuelve un recurso de apelación

6. La Resolución recurrida fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Asimismo, también fue el resultado de la valoración fáctica y probatoria de la primera instancia que llevó a concluir y comprobar la vulneración de las normas citadas.
7. *“Los responsables del tratamiento de datos personales deben ser capaces de demostrar,(...) que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012”⁴³.*
8. La regulación colombiana sobre tratamiento de datos impone al Responsable del Tratamiento el deber demostrar que ha adoptado medidas efectivas para cumplir la ley (Deber de Responsabilidad demostrada). Según la Corte Constitucional, *“el principio de responsabilidad demostrada, conocido en el derecho comparado como accountability en la protección de datos personales, es incorporado por la legislación interna por el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2013. El artículo 26 de esa normativa determina que los responsables del tratamiento de datos personales deberán demostrar, a petición de la Superintendencia de Industria y Comercio, entidad que obra como autoridad colombiana de protección de datos, que han implementado medidas apropiadas y efectivas para cumplir con las citadas normas jurídicas. (...)”* (C-32 de 2021)

En razón de lo expuesto, este Despacho procederá a confirmar la Resolución 53373 del 2 de septiembre de 2020 con las modificaciones realizadas por medio de la Resolución No. 9275 del 26 de febrero de 2021

SEXTO: Que analizada la cuestión planteada, y teniendo en cuenta lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirmará la decisión contenida en la Resolución 53373 del 2 de septiembre de 2020 con las modificaciones efectuadas por medio de la Resolución No. 9275 del 26 de febrero de 2021.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO: Confirmar la Resolución 53373 del 2 de septiembre de 2020 con las modificaciones realizadas por medio de la Resolución No. 9275 del 26 de febrero de 2021 de conformidad con lo expuesto en la parte motiva de la presente resolución.

ARTÍCULO SEGUNDO: Notificar personalmente el contenido de la presente resolución a COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A. COAUTONOMA C.T.A., identificada con el NIT. 827.000.616-7, a través de su representante legal o apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

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

⁴³ Cfr. Artículo 26 del Decreto 1377 de 2013 (Incorporado en el decreto 1074 de 2015)

VERSIÓN PÚBLICA

Por la cual se resuelve un recurso de apelación

ARTÍCULO CUARTO: Informar el contenido de la presente resolución al Director de Investigación de Protección de Datos Personales y devolverle el expediente para su custodia final.

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., agosto 31 de 2021

El Superintendente Delegado para la Protección de Datos Personales

NELSON REMOLINA ANGARITA

MPM

Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

NOTIFICACIÓN:

Sociedad: COOPERATIVA AUTÓNOMA DE SEGURIDAD C.T.A.
COAUTONOMA C.T.A.,
Identificación: Nit. 827.000.616-7
Representante legal: Boris Damir Izarra Sequera
Identificación: CC. 79.763.763
Dirección: Los Almendros, Manzana 2, Casa 1, Piso 1
Ciudad: San Andrés Isla, Archipiélago de San Andrés Providencia y Santa Catalina
Correo electrónico: coautonoma@hotmail.com

COMUNICACIÓN:

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