REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 38281 DE 2020

(14 de Julio)

VERSIÓN PÚBLICA

Radicación: **18-233399**

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 Resolución No. 78705 de 22 de octubre de 2018[1], la Dirección de Investigación de Protección de Datos Personales, resolvió iniciar una investigación administrativa con el fin de determinar si Mervicol S.A.S, identificada con el Nit. 900.369.378-8, infringió las normas sobre protección de datos personales consagradas en el literal b) del artículo 17 en concordancia con el literal c) del artículo 4 así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.

SEGUNDO. Que una vez agotada la etapa probatoria, y efectuado el análisis de los elementos probatorios que reposan en el expediente, así como del escrito de descargos[2] allegado por Mervicol S.A.S, la Dirección de Investigación de Protección de Datos Personales mediante la Resolución No. 17629 de 29 de mayo de 2019[3], resolvió:

> **ARTÍCULO PRIMERO: IMPONER** una sanción pecuniaria a la sociedad **MERVICOL S.A.S** identificada con el Nit. 900.369.378 – 8 de DOCE MILLONES CUATROCIENTOS VEINTIÚN MIL SETECIENTOS CUARENTA PESOS **M/CTE** ($12.421.740), equivalente a quince (15) salarios mínimos legales mensuales vigentes, por la violación a lo dispuesto en el literal b) del artículo 17 en concordancia con el literal c) del artículo 4 y el artículo 9 de la Ley 1581 de 2012, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.
>
> (...)
>
> **ARTÍCULO SEGUNDO: ORDENAR** a la sociedad **MERVICOL S.A.S.** identificada con el Nit. 800.153.993-7, cumplir la instrucción de conservar prueba de la autorización previa, expresa e informada de los titulares y no continuar tratando información respecto de aquellos titulares frente a los cuales no haya obtenido autorización.

TERCERO. Que en el término legal establecido, mediante escrito[4] de 21 de junio de 2019, el apoderado especial de Mervicol S.A.S (en adelante el recurrente), interpuso recurso de reposición y en subsidio de apelación, contra la Resolución Nº. 17629 de 29 de mayo de 2019, con fundamento en los siguientes argumentos:

---

[1] Folios 50-53.
[2] Comunicación con número de radico No. 18-233399-00013-0000 de 16 de abril de 2019. Folios 62-27
[3] Folios 71-75.
[4] Comunicación con número de radicado No. 18-233399-00021-0000 de 21 de junio de 2019.

1. VIOLACIÓN AL DEBIDO PROCESO.

El recurrente alega la violación al debido proceso durante la actuación de instancia toda vez que, en su opinión, no se cumplió el requisito establecido en el artículo 16 de la Ley 1581 de 2012 relativo a que el titular del dato debía elevar queja ante esta entidad una vez hubiese realizando el "tramite de consulta o reclamo al responsable o encargado del tratamiento"[5].

En adición, arguye el recurrente que la entidad "*no puede realizar una investigación sobre hechos que no tienen ningún asidero probatorio tal y como se enunció anteriormente pues esto iría en contravía de principio de seguridad jurídica, el debido proceso y cualquier persona podría bajo hechos falsos entrar a realizar denuncias temerarias con el fin de promover investigaciones como la presente basadas en hechos fictos*"[6].

2. AUSENCIA DE DAÑO SOBRE LA CONDUCTA DESPLEGADA.

La recurrente afirma que el denunciante no tuvo un daño particular por lo que asevera que no existe una configuración entre un hecho generador, un nexo causal y un daño. A punto seguido, se arguye que "*únicamente se realizó una oferta amparada en el Código de Comercio artículo 845 y siguientes de un servicio que el aceptó se enviara al correo electrónico que asintió en otorgar itero (sic) de una manera inequívoca (…)*"[7].

3. DESPROPORCIÓN EN LA SANCIÓN ADMINISTRATIVA.

Sostiene que la multa impuesta por la entidad lesiona gravemente los intereses económicos de Mervicol S.A.S. En sus palabras, el valor de la multa "*lesiona gravemente los intereses económicos (…) pues (…) la multa impuesta fue de $12.421.740 configurándose un 64.6% sobre la utilidad generada, esto quiere decir que la multa es exagerada*"[8].

Finalmente, solicita la revocatoria de la Resolución Nº. 17629 de 29 de mayo de 2019 y subsidiariamente reconsiderar el valor de la sanción.

CUARTO. Que mediante la Resolución Nº. 29636 de 22 de julio de 2019, la Dirección de Investigación de Protección de Datos Personales resolvió el recurso de reposición interpuesto por la recurrente, confirmando en todas sus partes la Resolución No. 17629 de 29 de mayo de 2019.

QUINTO. Que mediante el artículo primero de la Resolución No. 12169 del 31 de marzo de 2020 de esta entidad se ordenó lo siguiente: *"SUSPENDER los términos de las actuaciones administrativas sancionatorias y disciplinarias en curso, que se surten ante las dependencias de esta Superintendencia, desde el 1º de abril del 2020 y hasta la vigencia del Estado de Emergencia Económica, Social y Ecológica decretada por el Presidente de la República, fechas en que no correrán los términos legales, incluidos los de caducidad de la facultad sancionatoria de la administración prevista de manera general en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y en las normas especiales aplicables a las actuaciones de la Superintendencia de Industria y Comercio."*

---

[5] 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 o reclamo ante el Responsable o Encargado del Tratamiento.
[6] Folio 89.
[7] Folio 89.
[8] Folio 91.

Que en el presente caso no se trata de una actuación relacionada con la garantía del habeas data contenido en el artículo 15 de la Constitución Política y cuyo texto es el siguiente: "*Todas las personas (…) tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*".

Que mediante el artículo 1 de la Resolución 28182 del 12 de junio de 2020 de la Superintendencia de Industria y Comercio se ordenó *"REANUDAR a partir del 16 de junio de 2020, los términos de las actuaciones administrativas sancionatorias y disciplinarias que se surten ante las dependencias de esta Superintendencia (…)"*

SEXTO. Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, y con base en lo expuesto por la recurrente en el escrito de reposición y en subsidio apelación contra la Resolución No. 17629 de 29 de mayo de 2019, se procede a resolver el recurso interpuesto, de acuerdo con las siguientes:

CONSIDERACIONES DEL DESPACHO

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

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011[9] 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. PRECISIÓN PRELIMINAR.

Estando el expediente en esta instancia, se procedió a verificar la citada Resolución Nº 17629 del 29 de mayo de 2019 que sancionó a la sociedad Mervicol S.A.S, evidenciándose lo siguiente:

- En el artículo segundo de la parte resolutiva de la Resolución Nº 17629 del 29 de mayo de 2019 existe un error formal e involuntario en la digitación del Nit de la sociedad, quedando el número 800.153.993-7 cuando en realidad es 900.369.378-8.

De conformidad con el artículo 45[10] del Código de Procedimiento Administrativo y de lo Contencioso Administrativo se procederá a corregir dicho error.

---

[9] 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.

[10] "**Artículo 45. Corrección de errores formales**. En cualquier tiempo, de oficio o a petición de parte, se podrán corregir los errores simplemente formales contenidos en los actos administrativos, ya sean aritméticos, de digitación, de transcripción o de omisión de palabras. En ningún caso la corrección dará lugar a cambios en el sentido material de la

3. DEL TRATAMIENTO DE NÚMEROS TELEFÓNICOS MEDIANTE "MARCADORES PREDICTIVOS", ROBOCALLS, INTELIGENCIA ARTIFICIAL Y OTRAS TECNOLOGÍAS O PROCEDIMIENTOS AUTOMATIZADOS PARA CONTACTAR PERSONAS.

La Ley Estatutaria 1581 de 2012 es neutral tecnológica y temáticamente. Ello significa que aplica a cualquier Tratamiento con independencia de las técnicas, procesos o tecnologías –*actuales o futuras*- que se utilicen para dicho efecto. Por ende, debe observarse en la recolección, uso y Tratamiento de datos personales para diversos fines (marketing, políticos, cobro de cartera, etc) mediante el uso de técnicas o herramientas como "*marcadores predictivos*", "robocalls", "nuisance calls" e inteligencia artificial (IA).

Dicha ley define el Dato Personal como "*cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*"[11]. En este orden de ideas, los números telefónicos son datos personales cuando puedan asociase a una persona natural determinada o determinable. Aunque, en principio, el número telefónico, por sí solo, no se refiera directamente a una persona natural específica, a partir del mismo o con la interrelación con otros datos se puede establecer el nombre de la persona a que se refiere la información. Es decir, al final se puede establecer la persona Titular del dato (número telefónico).

Tratamiento, por su parte, significa "*cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*" [12]. Este término es de enorme importancia no sólo porque ha sido incluido en el artículo 15 de nuestra Constitución, sino porque determina el ámbito de aplicación[13] de la Ley 1581 de 2012 en la medida que cualquier actividad que se realice, a través de medios manuales o automatizados, con o sin intervención humana, debe observar las reglas establecidas en la citada ley.

Según el artículo 9 de la Ley en comento, "*sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior*". La autorización, por su parte, es definida como el "*consentimiento previo, expreso e informado del Titular[14] para llevar a cabo el Tratamiento de datos personales*"[15]. Esta se encuentra vinculada al principio de libertad según el cual "*el Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento*;"[16].

---

decisión, ni revivirá los términos legales para demandar el acto. Realizada la corrección, esta deberá ser notificada o comunicada a todos los interesados, según corresponda".

[11] Cfr. Literal c) del artículo 4 de la Ley Estatutaria 1581 de 2012
[12] Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012
[13] En este sentido, el artículo 2 de la Ley 1581 dice, entre otras, lo siguiente: "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." (Destacamos)
[14] El Titular es la "persona natural cuyos datos personales sean objeto de Tratamiento" (Literal –f- del artículo 3 de la Ley 1581 de 2012)
[15] Cfr. Literal a) del artículo 3 de la Ley 1581 de 2012
[16] Cfr. Literal c) del artículo 4 de la Ley 1581 de 2012

La Ley 1581 de 2012 impone el siguiente deber a los Responsables del Tratamiento "*solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular*"[17]. Deber legal que es imperativo cumplir para garantizar el siguiente derecho del Titular del dato: "*solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley*"[18].

En el presente caso se sancionó a la recurrente porque utilizó números telefónicos (datos personales) sin Autorización del Titular del Dato para contactarlo con fines de marketing a través de un mecanismo de llamadas automáticas y aleatorias *(marcador predictivo o Predictive Dialing)*.

Esto se puso de presente en la Resolución 17629 de 2019:

> En este sentido, este Despacho encontró que la sociedad MERVICOL S.A.S., a pesar de reconocer que en sus bases de datos se encontraba alojada la información del titular[4], no allegó la autorización previa, expresa e informada otorgada por este para que su información personal fuera objeto de tratamiento.
>
> Al respecto, la investigada señaló que (i) no posee ninguna base de datos y que la empresa tiene un marcador predictivo que llama de manera aleatoria a teléfonos; (ii) "*[el denunciante] de manera libre y voluntaria suministra dos correos electrónicos para el envío de la información pertinente*" y (iii) consideró que sí existió autorización del titular de los datos, la cual está contenida en la grabación de audio.
>
> Revisado el material probatorio, se encuentran cuatro (4) llamadas, las cuales fueron hechas por medio del marcador predictivo[5]. En ellas, una funcionaria de la investigada efectúa los reiterados contactos al denunciante para ofrecerle los servicios de la sociedad **MERVICOL S.A.S.**
>
> Sin embargo, posterior al análisis individual de cada una de ella, se encuentra que en ninguna de ellas se evidencia que el Titular haya dado su autorización de manera previa, expresa e informada; el Titular se limita a informar algunas direcciones de correo electrónico a las que le pueden enviar la propuesta comercial para contratar el servicio de la sociedad **MERVICOL S.A.S.**
>
> No obstante que la investigada asume tal comportamiento como una conducta inequívoca del Titular para que esa entidad trate sus datos, en ningún momento se demuestra que el Titular haya manifestado estar de acuerdo con que la investigada trate sus datos personales para los fines comerciales de la sociedad **MERVICOL S.A.S.**

Ahora bien, al recurrente, como Responsable del Tratamiento, le corresponde obtener la Autorización del Titular. No se ajusta a derecho excusarse en que los datos se obtuvieron a través de mecanismos electrónicos para justificar inexistencia de la Autorización del Titular del dato. Sobre el particular, se señaló lo que sigue a continuación en la Resolución 17629 de 2019:

> *Por otra parte, es importante resaltar el medio por el cual la sociedad **Mervicol S.A.S,** obtuvo la información del titular, ya que indican que "**no posee base de datos y estos números se marcan de forma aleatoria" (fl. 7)**", razón por la cual, es deber de este Despacho aclarar que dicha situación bajo ninguna circunstancia exime a la sociedad mencionada el deber de solicitar la autorización para el tratamiento de sus datos. De tal manera que, independientemente de cómo se obtienen los datos del titular, el Responsable de dicha información tendrá siempre la obligación de solicitar la autorización en los términos señalados por la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015, por lo cual para este Despacho es claro que la sociedad **Mervicol S.A.S.**, no demostró haber adoptado un procedimiento legal para obtener la autorización del titular, sobre el cual construyó su base de datos, ya que en dicha grabación el titular no autoriza el tratamiento de sus datos personales".*
> Lo anterior por cuanto en las grabaciones aportadas como prueba, el titular no autoriza el tratamiento de sus datos personales.

[17] Literal b) del artículo 17 de la Ley 1581 de 2012
[18] Literal b) del artículo 8 de la Ley 1581 de 2012

En suma, la regulación sobre Tratamiento de Datos Personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar, usar o tratar ese tipo de información. La ley colombiana permite el uso de tecnologías para Tratar Datos pero, al mismo tiempo, exige que se haga de manera respetuosa del ordenamiento jurídico. Quienes crean, diseñan o usan "innovaciones tecnológicas" deben cumplir todas las normas sobre tratamiento de datos personales

Sobre las marcaciones predictivas, la Dirección puso de presente lo siguiente en la resolución recurrida:

> Esta circunstancia ya fue objeto de pronunciamiento por parte de esta Dirección en Resolución 13234 del 26 de febrero de 2018.
>
> En dicha oportunidad, este Dirección determinó que *"[s]egún informó la investigada (…) [ésta] 'realiza la selección de un numero al azar, utilizando la metodología de un marcador predictivo ASTERIK, que realiza la combinación de los números (…), para lo cual se llama al POSIBLE usuario del servicio que la empresa (…) pretende ofrecer, para este fin se realiza una encuesta' (…).*
>
> *Por otra parte el 26 de julio de 2017 junto con el escrito de descargos allegó la investigada un CD que contiene llamadas realizadas a diferentes Titulares en el cual se les adelante una encuesta y se pretende demostrar el procedimiento utilizado para recolectar los datos personales.*
>
> *De acuerdo con lo anterior, se evidencia que la sociedad investigada lleva a cabo actividades de tratamiento de datos, y n este punto tenemos que hacer mención a la definición legal de tratamiento de datos 'Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, **uso**, circulación o supresión' (subrayado y negrilla fuera del texto).*
>
> *Concluyendo entonces que en ese primer contacto que se tiene con los prospectos de cliente utilizando números al azar es un tratamiento sin el lleno de los requisitos impuestos por la Ley 1581 de 2012, pues la recolección de datos de sus potenciales clientes la efectuó con base en la marcación predictiva que no cambian la calidad de privacidad de estos datos, más aún cuando con una llamada puede identificar al titular de la información. (…)"*
>
> Así las cosas, ya se tiene un precedente frente a las marcaciones aleatorias, frente a las se dispuso que ese primer contacto que se tiene con los prospectos de cliente utilizando números al azar es un tratamiento sin el lleno de los requisitos impuestos por la Ley 1581 de 2012, pues la recolección de datos de sus potenciales clientes la efectuó con base en la marcación predictiva que no cambian la calidad de privacidad de estos datos.
>
> Con base en lo expuesto, como quedó demostrado que la sociedad **Mervicol S.A.S**., incurrió en una vulneración a la norma contenida en el literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y el artículo 9 de la misma norma, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015, razón por la cual se impondrá la sanción correspondiente.

Los marcadores predictivos son sistemas automatizados que utilizan miles o millones de números telefónicos para marcar aleatoria y automáticamente a algunos o todos ellos con miras a comunicarse con la persona Titular de ese número. Se trata de una técnica para contactar a las personas Titulares de esos datos personales (números telefónicos). Usualmente se utiliza ese procedimiento para contacto masivo de personas con fines comerciales, políticos, entre otros. En últimas, con el uso de marcadores predictivos se está realizando Tratamiento automatizado de Datos Personales (números telefónicos).

En adición a los marcadores predictivos, se utilizan, entre otras, las "*robocalls" y* las *"nuisance calls"* (llamadas no deseadas) para contactar personas. Las primeras –*robocalls*- hacen referencia a llamadas telefónicas pregrabadas que se utilizan para enviar mensajes a

determinadas bases de datos[19]. Las segundas -*nuisance calls*- son llamadas telefónicas no deseadas que, entre otras, intentan promocionar un producto, servicio o idea al Titular[20] por medio de una base de datos a la que se le asigna un algoritmo de marketing (u otras finalidades). Las mismas pueden ser realizadas por personas o por máquinas (*robocalls*) y han sido consideradas como un medio intrusivo de la vida privada que perturba la tranquila[21] de las personas.

Las anteriores técnicas se han venido perfeccionando con herramientas de inteligencia artificial para mejorar su efectividad y, en algunos casos, ocultar el hecho de que el Titular está hablando con una máquina[22]. También se utilizan algoritmos predictivos en las campañas del call center para identificar y contactar las personas con las cuales existe mayor probabilidad de venderle un producto. Para el efecto, la organizaciones realizan directamente esta labor o acuden a terceros (como, por ejemplo, las empresas BPO -*Business Process Outsourcing-)* para efectuar dicha labor que, entre otras, involucra el Tratamieto de datos personales.

Aunque no existe una definición de Inteligencia Artificial (IA) que sea aceptada universalmente, la RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD) ha señalado que "*en su concepción amplia, se trata de un término ´sombrilla´ que incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar muchas actividades, los que comprenden desde modelos algorítmicos, pasando por los sistemas de machine learning, hasta llegar a las técnicas de deep learning. Particularmente se vincula el uso de algoritmos a la IA, los cuales son un conjunto de reglas o una secuencia de operaciones lógicas que proporcionan instrucciones para que las máquinas tomen decisiones o actúen de determinada manera*[23"24]*.*

La IA comprende sistemas que: a) piensan como humanos (por ejemplo, arquitecturas cognitivas y redes neuronales); b) actúan como seres humanos (por ejemplo, razonamiento automatizado y aprendizaje); c) piensan racionalmente (por ejemplo, inferencias), o d) actúan racionalmente (por ejemplo, agentes de software inteligentes y robots incorporados que logran objetivos mediante la percepción, la planificación, el razonamiento, el aprendizaje, la comunicación, la toma de decisiones y la actuación)[25].

Desde las perspectiva de las competencias de esta Delegatura, es relevante destacar que la IA involucra la recolección, el almacenamiento, el análisis, procesamiento o interpretación de enormes cantidades de información (incluídos los Datos Personales) que son usados para generar diversos resultados, acciones o comportamientos por parte de las maquinas. En otras palabras, los datos personales son el alimento o el combustible de la IA y mediante la

---

[19] Jason C. Miller, Regulating Robocalls: Are Automated Calls the Sound of, or a Threat to, Democracy, 16 Mich. Telecomm. & Tech. L. Rev. 213 (2009).
[20] Information Commissioner Office . (2020). Nuisance calls. julio 2020 , de Information Commissioner Office Sitio web: https://ico.org.uk/your-data-matters/nuisance-calls/
[21] Mark S. Nadel, Rings of Privacy: Unsolicited Telephone Calls and the Right of Privacy, 4 Yale J. on Reg. (1986). Disponible en: https://digitalcommons.law.yale.edu/yjreg/vol4/iss1/5
[22] Ginger Zhe Jin. (2018). Artificial Intelligence and Consumer Privacy. julio 2020 , de University of Maryland y el National Bureau of Economic Research Sitio web: https://www.nber.org/papers/w24253
[23] Cfr. Royal Society ("Machine Learning: The Power and Promise of Computers That Learn by Example," Royal Society,
[24] RED IBEROAMERICANA DE PROTECCIÓN DE DATOS -RIPD- (2019). Recomendaciones generales para el tratamiento de datos en la inteligenciar artificial. Pág 7. El texto puede consultarse en la página web de la RIPD: https://www.redipd.org/es/documentos/guias
[25] Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (3rd Edition) (Essex, England: Pearson, 2009).

misma se realizan Tratamientos de dicha información los cuales deben ser respetuosos de la Ley 1581 de 2012 y sus normas reglamentarias[26].

En síntesis, es legítimo el Tratamiento de datos personales (números telefónicos) a través de cualquier metodología o tecnología, como, por ejemplo, el "marcador predictivo", "*robocalls" y "nuisance calls",* inteligencia artificial, siempre y cuando se haya obtenido la Autorización previa, expresa e informada de las personas destinatarias de las llamadas telefónicas.

4. **LA AUTORIZACIÓN DEL TITULAR ES UN PRERREQUISITO PARA PODER TRATAR SUS DATOS CON FINES DE MARKETING O PUBLICIDAD.**

Las actividades de marketing, publicidad y comercio electrónico son lícitas y para su realización debe aplicarse la regulación sobre tratamiento de datos personales. Durante 2019 esta entidad emitió las siguientes dos (2) guías[27] para que sean tenidas en cuenta por parte de quienes efectúan esas labores:

- GUÍA SOBRE EL TRATAMIENTO DE DATOS PERSONALES PARA FINES DE COMERCIO ELECTRÓNICO
- GUÍA SOBRE EL TRATAMIENTO DE DATOS PERSONALES PARA FINES DE MARKETING Y PUBLICIDAD

Estas no son de obligatorio cumplimiento pero presentan orientaciones o recomendaciones para cumplir mandatos legales como, entre otros, los artículos 9 y 10 de la Ley Estatutaria 1581 de 2012, a saber:

> "***ARTÍCULO 9o. AUTORIZACIÓN DEL TITULAR.*** *Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.*
>
> ***ARTÍCULO 10. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN.*** *La autorización del Titular no será necesaria cuando se trate de:*
> *a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;*
> *b) Datos de naturaleza pública;*

[26] Sobre este tema, en junio de 2019 la RED IBEROAMERICANA DE PROTECCIÓN DE DATOS -RIPD- expidió el siguiente documento: ."Recomendaciones generales para el tratamiento de datos en la inteligenciar artificial", en donde se realizan las siguientes sugerencias a quienes desarrollan productos de IA, con el fin de orientarlos para que desde el diseño del producto se tengan en cuenta las exigencias de las regulaciones sobre tratamiento de datos personales: I. Cumplir las normas locales sobre Tratamiento de Datos Personales (TDP); II. Efectuar estudios de impacto de privacidad; III. Incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto; IV. Materializar el principio de responsabilidad demostrada (accountability); V. Diseñar esquemas apropiados de gobernanza sobre TDP en las organizaciones que desarrollan productos de IA; VI. Adoptar medidas para garantizar los principios sobre TDP en los proyectos de IA; VII. Respetar los derechos de los titulares de los datos e implementar mecanismos efectivos para el ejercicio de los mismos; VIII. Asegurar la calidad de los datos personales; IX. Utilizar herramientas de anonimización X. Incrementar confianza y la transparencia con los titulares de los datos personales. El texto puede consultarse en la página web de la RIPD: https://www.redipd.org/es/documentos/guias

[27] Los textos están disponibles en la **sección de publicaciones** de la Delegatura para la protección de datos personales: https://www.sic.gov.co/tema/proteccion-de-datos-personales

c) Casos de urgencia médica o sanitaria;
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
e) Datos relacionados con el Registro Civil de las Personas.
Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

Como se observa, por regla general se requiere la Autorización previa, expresa e informada para tratar los datos personales que no sean de naturaleza pública. En algunos casos excepcionales, el artículo 10 de la Ley 1581 de 2012 permite el Tratamiento de datos sin el consentimiento del Titular del Dato.

No obstante lo anterior, la recolección de Datos sin Autorización no significa que quede sin protección esa información, o los ciudadanos Titulares de los Datos. En efecto, la parte final del artículo 10 de la Ley 1581 de 2012 esa norma señala que "*quien acceda a los datos personales sin que medie autorización previa* ***deberá en todo caso cumplir con las disposiciones contenidas en la presente ley***". (Destacamos). La falta de Autorización no genera la desaparición de la protección jurídica de los datos personales y de los Titulares de los mismos porque el Responsable o Encargado debe cumplir todas las demás obligaciones legales establecidas en la citada ley y sus decretos reglamentarios.

Así pues, la Autorización es un mecanismo muy importante de legitimación para tratar Datos personales, pero no es, *per se*, una forma de protección de los derechos. La efectiva protección de éstos, dependerá, entre otros, de las medidas que implementen los Responsables del Tratamiento para cumplir la regulación sobre la materia.

5. LA RECURRENTE NO PROBÓ TENER LA AUTORIZACIÓN PREVIA, EXPRESA E INFORMADA DEL TITULAR DEL DATO PERSONAL

Ahora bien, en el numeral 9.1.1. de la Resolución 17629 de 2019 se especifica el motivo y monto de la sanción impuesta en los siguientes términos:

> En el caso sub-examine, quedó demostrado que la investigada no cumplió con su deber de solicitar y obtener copia de la autorización del Titular de los Datos.
>
> En virtud de lo expuesto, se impondrá una sanción equivalente a quince (15) salarios mínimos legales mensuales vigentes, por el incumplimiento su apego a lo establecido en el literal b) del artículo 17 en concordancia con el literal c) del artículo 4 y el artículo 9 de la Ley 1581 de 2012, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.

Nótese que la regulación sobre protección de datos impone al Responsable la carga probatoria de acreditar la autorización del Titular del Datos. Es necesario tener presente 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*" [28] y en el Decreto 1377 de 2013.

[28] Cfr. Artículo 26 del Decreto 1377 de 2013.

La obtención de la Autorización puede hacerse mediante cualquiera de los medios autorizados en el artículo 7 del Decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015), incluso las conductas inequívocas. No obstante, no debe perderse de vista que el Responsable del Tratamiento debe estar en capacidad de probar que obtuvo el consentimiento previo, expreso e informado del Titular del Datos. De hecho, no sólo el Titular tiene el derecho de "*solicitar prueba de la citada autorización*"[29], sino que es deber del Responsable del Tratamiento "*solicitar y conservar, en las condiciones previstas en esta ley, copia de la respetiva autorización otorgada por el titular*"[30].

Reiteramos que la Autorización puede obtenerse utilizando diversos mecanismos o procedimientos, pero es estrictamente necesario tener la prueba de la Autorización individual y concreta de todos y cada uno de los Titulares cuyos datos se recolectan, usan o tratan.

Es preciso resaltar que la regulación sobre datos personales impone cargas probatorias en cabeza de los Responsables del Tratamiento como, entre otras, las siguientes:

a) Conservar prueba de haber informado al titular, al momento de solicitarle la autorización, de manera clara y expresa lo que ordena el artículo 12 de la Ley 1581 de 2012 y, cuando el Titular lo solicite, entregarle copia de de ello[31]
b) *"Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular"*[32].
c) *"Proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso"*[33]
d) *"Documentar los procedimientos para el Tratamiento, conservación y supresión de los datos personales de conformidad con las disposiciones aplicables a la materia de que se trate"*[34].
e) *"Desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas"*[35]
f) *"Conservar el modelo del Aviso de Privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los Titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven"*[36]
g) Adoptar *"las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento"*[37].

En suma, quienes desarrollen actividades de marketing o publicidad deben establecer medidas útiles, apropiadas y efectivas para cumplir sus obligaciones legales. Adicionalmente, tendrán que evidenciar y demostrar el correcto cumplimiento de sus

---

[29] Cfr. Literal b) del artículo 8 de la Ley Estatutaria 1581 de 2012
[30] Cfr. Literal b) del artículo 17 de la Ley Estatutaria 1581 de 2012.
[31] Cfr. Parágrafo del artículo 12 de la Ley 1581 de 2012.
[32] Cfr. Literal (b) del artículo 17 de la Ley 1581 de 2012 y artículo 8 del Decreto 1377 de 2013 *"Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos".*
[33] Cfr. Artículo 4 del Decreto 1377 de 2013.
[34] Cfr. Artículo 11 del Decreto 1377 de 2013.
[35] Cfr. Artículo 13 del Decreto 1377 de 2013.
[36] Cfr. Artículo 16 del Decreto 1377 de 2013.
[37] Cfr. Artículo 22 del Decreto 1377 de 2013.

deberes. En el presente caso, la recurrente no acreditó la prueba de la autorización del titular del dato personal. Por tanto, la Resolución recurrida se ajusta a derecho.

6. DEBIDO PROCESO.

Señala lo siguiente la Ley Estatutaria 1581 de 2012:

> **"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."
>
> **"ARTÍCULO 21. FUNCIONES**. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:
>
> (…)
>
> b) Adelantar las investigaciones del caso, **de oficio o a petición de parte** y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. (…) "
>
> **"ARTÍCULO 22. TRÁMITE.** La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes."

Como se observa, el artículo 16 impone una condición para que el Titular del dato pueda presentar una queja ante esta entidad, pero sin que ello sea un requisito para que la Superintendencia de Industria y Comercio (SIC) pueda iniciar de oficio investigaciones administrativas para establecer eventuales irregularidades en el tratamiento de datos personales. En otras palabras, la ley ordena a la SIC iniciar investigaciones de oficio sin que sea necesario que el Titular del dato agote el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

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

> *"El poder sancionador estatal ha sido definido como "un instrumento de autoprotección, en cuanto contribuye a preservar el orden jurídico institucional mediante la asignación de competencias a la administración que la habilitan para imponer a sus propios funcionarios y a los particulares el acatamiento, inclusive por medios punitivos, de una disciplina cuya observancia contribuye a la realización de sus cometidos.*
>
> *Esa potestad es una manifestación del jus punendi, razón por la que está sometida a los siguientes principios: (i) el principio de legalidad, que se traduce en la existencia de una ley que la regule; es decir, que corresponde sólo al legislador ordinario o extraordinario su definición. (ii) El principio de tipicidad que, si bien no es igual de riguroso al penal, sí obliga al legislador a hacer una descripción de la conducta o del comportamiento que da lugar a la aplicación de la sanción y a determinar*

expresamente la sanción. (iii) El debido proceso que exige entre otros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (iv) El principio de proporcionalidad que se traduce en que la sanción debe ser proporcional a la falta o infracción administrativa que se busca sancionar. (v) La independencia de la sanción penal; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal"[38].

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

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

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

Al respecto, este Despacho advierte que en ningún momento los actos o actuaciones de esta Delegatura, han estado en contravía del Derecho. Esta entidad aplicó y respetó las garantías procesales necesarias, y en todas las etapas respectivas se emitieron las resoluciones y actos administrativos a que hubo lugar. Los que, en ninguna circunstancia fueron arbitrarios.

Por lo expuesto previamente, no le cabe razón al recurrente cuando afirma que se configuró una violación al debido proceso. Primero, por cuanto la Superintendencia de Industria y Comercio si puede realizar una investigación de oficio tendiente a establecer la infracción de una disposición legal. Segundo, no se desvirtuó por el recurrente el respeto de los postulados que el debido proceso enmarca. Y, tercero, confunde el recurrente el ejercicio del derecho de *protección de datos personales* que le asiste al quejoso con la facultad de investigación, control y vigilancia en cabeza de la Superintendencia de Industria y Comercio.

7. AUSENCIA DE DAÑO SOBRE LA CONDUCTA DESPLEGADA.

Causar un daño no es un requisito jurídico para que la SIC pueda imponer multas o impartir órdenes. Acá no estamos frente a un proceso de responsabilidad civil para indemnizar perjuicios sino ante una actuación administrativa para establecer si se cumplió o no la regulación sobre tratamiento de dato personales.

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

Es suficiente desconocer cualquiera de las disposiciones de la Ley 1581 de 2012, para que la administración ejerza su poder sancionatorio dentro del marco legal vigente y observando el debido proceso.

Al hacer referencia al principio de legalidad en materia de protección de datos personales, la Corte Constitucional mediante la Sentencia C-1011 de 2008, manifestó:

> *"(…) Para la Corte, en consecuencia,* ***la flexibilidad que puede establecer el legislador en materia de derecho administrativo sancionador es compatible con la Constitución, siempre que esta característica no sea tan amplia que permita la arbitrariedad de la administración. Un cierto grado de movilidad a la administración para aplicar las hipótesis fácticas establecidas en la ley guarda coherencia con los fines constitucionales de esta actividad sancionatoria administrativa, en la medida que le permite cumplir eficaz y eficientemente con las obligaciones impuestas por la Carta. Sin embargo, ha advertido que la flexibilidad del principio de legalidad no puede tener un carácter extremo, al punto que se permita la arbitrariedad de la administración en la imposición de las sanciones o las penas"***[39]*.* (Énfasis añadido).

Así las cosas, la administración no puede exceder los límites impuestos por el legislador al momento de aplicar una sanción. Por lo que, la conducta objeto de investigación debe tener el carácter de sancionable. Es aquí donde surge el principio de tipicidad, el cual no es otra cosa que el previo establecimiento por parte del legislador, de la forma más clara y precisa, *"de infracciones, penas, castigos o sanciones que pueden ser impuestas por las autoridades administrativas en ejercicio del poder punitivo estatal"*[40].

Sobre dicho principio, la Corte Constitucional precisó lo siguiente en la Sentencia C-748 de 2011:

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

Resulta útil reiterar la diferencia que existe entre los elementos que configuran la responsabilidad civil extracontractual y la facultad sancionatoria del Estado. Confunde el recurrente estas dos instituciones cuando afirma que "*el denunciante no tuvo un daño en particular, para que existiese este se tenía que realizar una configuración entre un hecho generador, un nexo causal y finalmente un daño que fue el que en el expediente el denunciante nunca demuestra (…)*"[41].

La protección de los datos personales no está sujeta a demostrar el acaecimiento de un daño y/o perjuicio. Incluso, los deberes que al Responsable le asigna el ordenamiento jurídico, no pueden ser evaluados a la luz del daño que ocasione su tratamiento al Titular del dato. Los derechos que la Constitución Política de Colombia en su artículo 15 inciso segundo le confiere al Titular, le corresponden por su mera existencia y no al probar una situación fáctica. Recuérdese que la vulneración del debido tratamiento de los datos personales no solo

---

[39] Corte Constitucional. Sentencia C-406 de 2004.
[40] Corte Constitucional. Sentencias C-1161 de 2000.
[41] Folio 89.

lesiona los derechos de una persona en particular, pero también, pone en riesgo los derechos humanos de toda la sociedad.

Bajo esta premisa, el ordenamiento jurídico colombiano le ha conferido a la Superintendencia de Industria y Comercio el deber de ejercer la vigilancia necesaria para garantizar que "en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley"[42]. De este modo, no se enmarcan dentro de las competencias atribuidas a esta entidad aquellas que se desprenden de la configuración de la responsabilidad civil extracontractual.

Es decir, las normas sobre Tratamiento de datos personales no se refieren a la responsabilidad civil de los Responsables o Encargados del Tratamiento de datos. Resulta entonces que se trata es de una responsabilidad administrativa de la cual, pueden derivar multas y/o sanciones con el fin de promover y garantizar el cumplimiento del Régimen General de Protección de Datos Personales con el único propósito de amparar el derecho fundamental[43] a la protección de datos[44].

En suma, la Superintendencia de Industria y Comercio, esta facultada para sancionar una vez se hubiese probado el desconocimiento de cualquiera de las disposiciones de la Ley 1581 de 2012.

En el caso concreto, el recurrente no allegó pruebas tendientes a demostrar que adoptó un procedimiento legal para obtener la autorización del titular, sobre el cual construyó su base de datos. En este caso, existe suficiente material probatorio para demostrar que el recurrente realizó un tratamiento de los datos personales del quejoso sin la debida autorización (previa, expresa y exigible) de su titular.

Por ende, concluye este Despacho que, en el presente caso, se dan los presupuestos requeridos para concluir que la recurrente no cumplió el deber legal establecido en el literal b) del artículo 17 de la Ley Estatutaria 1581 de 2012.

8. PROPORCIONALIDAD DE LA SANCIÓN ADMINISTRATIVA.

Se reitera que la sanción impuesta además de obedecer a la desatención de los deberes legalmente establecidos en la regulación sobre tratamiento de datos personales, resulta proporcional en consideración a: i) los supuestos fácticos y jurídicos que motivaron el acto administrativo recurrido; y ii) los documentos y demás elementos probatorios valorados en el curso de esta actuación administrativa. En todo caso, es fundamental que el operador jurídico realice un análisis conjunto y sistemático de los criterios mencionados. Así como de los elementos y pautas que estime convenientes, con el propósito de ponderar la gravedad de la conducta y la capacidad de pago de la entidad infractora.

Por este motivo, es necesario reiterar lo siguiente:

---

[42] Artículo 19 de la Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
[43] El derecho fundamental a la protección de datos personales, derecho humano (universal, inalienable, indivisible, irrenunciable e imprescriptible) que fue positivizado por el Constituyente Primario en el artículo 15 de la Constitución de 1991, y que en muchas ocasiones es conexo a otros derechos fundamentales de gran relevancia constitucional como la dignidad humana, el buen nombre, la intimidad, etc.
[44] Las sanciones impuestas en función del derecho administrativo sancionatorio pretenden asegurar el orden público y el correcto funcionamiento de la administración. Al respecto ver: Corte Constitucional, Sala Plena, C-703 de 2010, Magistrado Ponente Gabriel Eduardo Mendoza, Considerando 5; Corte Constitucional, Sala Plena, C-010-03, Magistrada Ponente Clara Inés Vargas.

En primer lugar, 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. De tal suerte que, la recurrente al desatender el deber de solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva Autorización otorgada por el Titular vulneró los derechos que le asisten al Titular del dato. De igual forma, desatendió sus deberes legales cuando por medio del marcador predictivo, en ausencia de una Autorización, realizó un Tratamiento de los datos personales del quejoso.

En segundo lugar, la Resolución No. 17629 del 29 de mayo de 2019 fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Los cuales están contemplados en el artículo 3 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, *"debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad".* De ahí que, la decisión emitida se ajuste a Derecho, pues fue producto de la aplicación del mandato legal y constitucional (artículo 209). Asimismo, también fue el resultado de la valoración fáctica y probatoria de la primera instancia que llevó a concluir y comprobar la vulneración de la ley por parte de la recurrente.

Resulta útil mencionar, para efectos de poner en perspectiva el monto a pagar por parte de la recurrente, que la multa equivalente a quince (15) salarios mínimos legales mensuales vigentes, lo cual representa porcentualmente al 0.75% del límite legal de dos mil (2.000) salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012.

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

Así las cosas, la defensa de un derecho fundamental no puede doblegarse ante los intereses económicos de un Responsable que violentó el ordenamiento jurídico. Por esto, le cabe razón a la Dirección de Investigación de Protección de Datos Personales cuando afirma que no resulta adecuado relacionar la "multa" con la "utilidad generada" por la sociedad, por cuanto el mismo solamente denota el estado temporal de la empresa en un año fiscal y no su estabilidad y crecimiento futuro.

Por los motivos expuestos, no se acogerán las consideraciones de la recurrente en la medida en que la sanción impuesta obedece a las particularidades propias de esta actuación administrativa.

Aunque las razones anteriores son suficientes para confirmar la Resolución No. 17629 de 29 de mayo de 2019, esta Delegatura considera pertinente destacar lo siguiente respecto de:

i. Responsabilidad Demostrada (*Accountability*) y "*Compliance*" en el Tratamiento de Datos Personales, y
ii. Responsabilidad jurídica de los Administradores

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

La regulación colombiana le impone al Responsable o al Encargado del Tratamiento, la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica, ni limitarse únicamente a la formalidad. Por el contrario, debe ser real y demostrable. Al respecto, nuestra jurisprudencia ha determinado que "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante*"[45].

Adicionalmente, es importante resaltar que los responsables o encargados del tratamiento de los datos, no se convierten en dueños de los mismos como consecuencia del almacenamiento en sus bases o archivos. En efecto, al ejercer únicamente la mera tenencia de la información, solo tienen a su cargo el deber de administrarla de manera correcta, apropiada y acertada. Por consiguiente, si los sujetos mencionados actúan con negligencia o dolo, la consecuencia directa sería la afectación de los derechos humanos y fundamentales de los titulares de los datos.

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

El artículo 26[46] -*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

---

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

[46] El texto completo del artículo 26 del Decreto 1377 de 2013 ordena: *"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"

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.

El artículo 27 -*Políticas Internas Efectivas*-, exige que los responsables del tratamiento de datos implementen medidas efectivas y apropiadas que garanticen, entre otras: "(*…) 3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento*."[47]
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*[48]*(accountability)*[49]".

El término "***accountability***"[50], a pesar de tener 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, son:

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.

---

[47] El texto completo del artículo 27 del Decreto 1377 de 2013 señala: *"Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar: 1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto. 2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación. 3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento. La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto".*

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

[49] *"El término "accountability" puede ser traducido por rendición de cuentas. Esta voz inglesa, que, en su uso cotidiano, significa 'responsabilidad', ha comenzado a emplearse en política y en el mundo empresarial para hacer referencia a un concepto más amplio relacionado con un mayor compromiso de los Gobiernos y empresas con la transparencia de sus acciones y decisiones (…) el término accountability puede ser traducido por sistema o política de rendición de cuentas o, simplemente, por rendición de cuentas (…)"* Recuperado de https://www.fundeu.es/recomendacion/rendicionde-cuentas-y-norendimientomejor-que-accountability-1470/ el 22 de abril de 2019.

[50] Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.

El principio de responsabilidad demostrada –*accountability*- demanda implementar acciones de diversa naturaleza[51] para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los responsables y encargados del tratamiento adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

Dichas acciones o 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* [sic] *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****"*[52]. (Énfasis añadido)

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, idóneas y suficientes, que permitan garantizar: i) los derechos de los titulares de los datos personales y ii) una gestión respetuosa de los derechos humanos.

Aunque no es espacio para explicar cada uno de los aspectos mencionados en la guía[53], es destacable que el principio de responsabilidad demostrada se articula con el concepto de *compliance*, en la medida que este hace referencia a la autogestión o "*conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y*

---

[51] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humana y de gestión. Asimismo involucran procesos y procedimientos con características propias en atención al objetivo que persiguen.

[52] 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.

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

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"[54].

También se ha afirmado que, "*compliance es un término relacionado con la gestión de las organizaciones conforme a las obligaciones que le vienen impuestas (requisitos regulatorios) o que se ha autoimpuesto (éticas)"* [55]. 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*"[56].

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 ejecuten, entre otros, un "*sistema de administración de riesgos asociados al tratamiento de datos personales*"[57] 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*"[58].

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

Según el artículo 22 de la Ley 222 de 1995[59] 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*" (énfasis añadido).

---

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

[55] 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/

[56] *Idem.*

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

[58] *Ibidem*.

[59] Ley 222 de 1995 "Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones"

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

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

El artículo 24[60] 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*". Esta 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*"[61]. 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 lo expuesto, se considera imprescindible que los Administradores de la sociedad recurrente implementen en la práctica todo lo que ordena la regulación sobre tratamiento de datos personales.

11. DE LA APLICACIÓN DEL ARTÍCULO 49 DE LA LEY 1955 DE 2019.

Establece el artículo 49 de la Ley 1955 de 2019 lo siguiente:

> ***"ARTÍCULO 49. CÁLCULO DE VALORES EN UVT.*** *A partir del 1 de enero de 2020, todos los cobros, sanciones, multas, tasas, tarifas y estampillas, actualmente denominados y establecidos con base en el salario mínimo mensual legal vigente (smmlv), deberán ser calculados con base en su equivalencia en términos de la*

---

[60] Artículo 24, Ley 222 de 1995 "*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".

[61] Cfr. Parte inicial del artículo 24 de la Ley 222 de 1995.

Unidad de Valor Tributario (UVT). En adelante, las actualizaciones de estos valores también se harán con base en el valor de la UVT vigente.

PARÁGRAFO. Los cobros, sanciones, multas, tasas, tarifas y estampillas, que se encuentren ejecutoriados con anterioridad al 1 de enero de 2020 se mantendrán determinados en smmlv". *(negrilla fuera de texto)*

Por su parte el artículo 87 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, dispone lo siguiente:

ARTÍCULO 87. FIRMEZA DE LOS ACTOS ADMINISTRATIVOS. *Los actos administrativos quedarán en firme:*
1. Cuando contra ellos no proceda ningún recurso, desde el día siguiente al de su notificación, comunicación o publicación según el caso.
2. Desde el día siguiente a la publicación, comunicación o notificación de la decisión sobre los recursos interpuestos.
3. Desde el día siguiente al del vencimiento del término para interponer los recursos, si estos no fueron interpuestos, o se hubiere renunciado expresamente a ellos.
4. Desde el día siguiente al de la notificación de la aceptación del desistimiento de los recursos.
5. Desde el día siguiente al de la protocolización a que alude el artículo 85 para el silencio administrativo positivo. (destacamos)

De conformidad con las normas anteriormente citadas, este Despacho modificará el artículo primero de la Resolución No. 17629 de 29 de mayo de 2019 para indicar en Unidades de Valor Tributario (UVT)[62] el valor de la multa impuesta en pesos colombianos, de conformidad con lo establecido en el artículo 49 de la Ley 1955 de 2019.

12. CONCLUSIONES

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

i. La Ley Estatutaria 1581 de 2012 es neutral tecnológica y temáticamente. Ello significa que aplica a cualquier Tratamiento con independencia de las técnicas, procesos o tecnologías *–actuales o futuras-* que se utilicen para dicho efecto. Por ende, debe observarse en la recolección, uso y Tratamiento de datos personales para diversos fines (marketing, políticos, cobro de cartera, etc) mediante el uso de técnicas o herramientas como, entre otras, "*marcadores predictivos*", "robocalls", "nuisance calls" e inteligencia artificial (IA).

ii. La regulación sobre Tratamiento de Datos Personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar, usar o tratar ese tipo de información. La ley colombiana permite el uso de tecnologías para tratar datos pero, al mismo tiempo, exige que se haga de manera respetuosa del ordenamiento jurídico. Quienes crean,

[62] De conformidad con lo establecido en la Resolución No. 84 del 28 de noviembre expedida por la Dirección de Impuestos y Aduanas Nacionales, el valor de la UVT para el 2020 es de $35.607

diseñan o usan “innovaciones tecnológicas” deben cumplir todas las normas sobre Tratamiento de datos personales.

iii. Es legítimo el Tratamiento de datos personales (números telefónicos) a través de cualquier metodología o tecnología, como, por ejemplo, el “marcador predictivo”, “*robocalls”, “nuisance calls”,* inteligencia artificial, siempre y cuando se haya obtenido la Autorización previa, expresa e informada de las personas destinatarias de las llamadas telefónicas.

iv. La recurrente infringió las normas sobre protección de datos personales consagradas en el literal b) del artículo 17 en concordancia con el literal c) del artículo 4 así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.

v. La Superintendencia de Industria y Comercio puede realizar una investigación de oficio tendiente a establecer la infracción de una disposición legal.

vi. La multa impuesta equivale al 0.75% del límite legal de dos mil (2.000) salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012.

vii. Es suficiente desconocer cualquiera de las disposiciones de la Ley 1581 de 2012, para que la administración ejerza su poder sancionatorio.

viii. Las sanciones que se desprenden por la vulneración del derecho fundamental a la protección de datos personales 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.

ix. 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.

x. No es necesario que exista un daño o perjuicio para imponer una sanción por infringir la regulación sobre tratamiento de datos personales.

xi. La facultad sancionatoria respecto de las normas de Tratamiento de Datos personales no busca indemnizar los eventuales daños y perjuicios causados por el indebido Tratamiento de esta información, pues, no es un asunto de responsabilidad civil. Se trata de un asunto de responsabilidad administrativa del cual pueden derivar multas y/o sanciones por el solo hecho de incumplir la regulación sobre Tratamiento de Datos personales.

Así las cosas, una vez analizada toda la actuación administrativa, la información y documentos que conforman el expediente, concluye el Despacho que la resolución objeto de impugnación fue expedida observando la ley. De esta forma y conforme con lo dispuesto por

el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, se confirmará en su totalidad, la Resolución No. 17629 de 29 de mayo de 2019.

Para efectos de la notificación se procederá conforme lo ordena el artículo 4[63] del Decreto Legislativo 491 del 28 de marzo de 2020.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO: MODIFICAR el ARTÍCULO PRIMERO de la Resolución No. 17629 de 29 de mayo de 2019 de conformidad con lo expuesto en la parte motiva del presente acto administrativo:

> **ARTÍCULO PRIMERO: IMPONER** una sanción pecuniaria a la sociedad **MERVICOL S.A.S** identificada con el Nit. 900.369.378-8 de DOCE MILLONES CUATROCIENTOS VEINTIÚN MIL SETECIENTOS CUARENTA PESOS **M/CTE ($12.421.740),** equivalente a 348,8566855 Unidades de Valor Tributario (UVT), por la violación a lo dispuesto en el literal b) del artículo 17 en concordancia con el literal c) del artículo 4 y el artículo 9 de la Ley 1581 de 2012, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.

ARTÍCULO SEGUNDO. Corregir el artículo segundo de la Resolución Nº 17629 del 29 de mayo de 2019, de conformidad con lo establecido en la parte motiva de la presente Resolución, el cual quedará así:

> "**ARTÍCULO SEGUNDO: ORDENAR** a la sociedad **MERVICOL S.A.S.** identificada con el Nit. 900.369.378-8, cumplir la instrucción de conservar prueba de la Autorización previa, expresa, e informada de los titulares y no continuar tratando información respecto de aquellos titulares frente a los cuales no haya obtenido Autorización.
>
> **PARÁGRAFO PRIMERO:** La sociedad **MERVICOL S.A.S.** identificada con el Nit. 900.369.378-8, deberá acreditar el cumplimiento de lo ordenado en el presente artículo ante esta Superintendencia dentro de los cinco (5) días hábiles siguientes a la expiración del plazo previsto para su acatamiento.
>
> **PARÁGRAFO SEGUNDO:** El incumplimiento de lo ordenado en el presente acto administrativo, hará a la sociedad **MERVICOL S.A.S.** identificada con el Nit.

---

[63] El artículo 4 del Decreto Legislativo 491 de 2020 ordena lo siguiente: "*Notificación o comunicación de actos administrativos. Hasta tanto permanezca vigente la Emergencia Sanitaria declarada por el Ministerio de Salud y Protección Social,* ***la notificación*** *o comunicación de los actos administrativos* ***se hará por medios electrónicos****. Para el efecto en todo trámite, proceso o procedimiento que se inicie será obligatorio indicar la dirección electrónica para recibir notificaciones, y con la sola radicación se entenderá que se ha dado la autorización.*

En relación con las actuaciones administrativas que se encuentren en curso a la expedición del presente Decreto, los administrados deberán indicar a la autoridad competente la dirección electrónica en la cual recibirán notificaciones o comunicaciones."

900.369.378-8, acreedora de las sanciones previstas en la ley."

ARTÍCULO TERCERO. CONFIRMAR en todas sus partes la Resolución No. 17629 de 29 de mayo de 2019, de conformidad con lo expuesto en la parte motiva del presente acto administrativo.

ARTÍCULO CUARTO. Notificar personalmente el contenido de la presente resolución a **Mervicol S.A.S** identificada con el Nit. 900.369.378-8 a través de su representante legal o su apoderado o quien haga sus veces, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO QUINTO. Comunicar el contenido de la presente decisión al señor [redacted] identificado con la Cédula de Ciudadanía No. [redacted] o a su apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO SEXTO. Comunicar 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., 14 de Julio de 2020

El Superintendente Delegado para la Protección de Datos Personales

NELSON REMOLINA ANGARITA

ALC

VERSIÓN PÚBLICA

Por la cual se resuelve un recurso de apelación

Notificación

Sociedad: **MERVICOL S.A.S**
Identificación: Nit. 900.369.378-8
Representante legal: **VICTOR RAUL MERA RODRIGUEZ**
Identificación: C.C. 19.191.172
Dirección: Calle 130 No. 58 A 91 P 3.
Ciudad: Bogotá D.C.,
Correo electrónico: administración@mervicol.com

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

Comunicación

Reclamante

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