REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 91422 **DE 2018**

(17 DIC 2018)

Por la cual se resuelve un recurso de apelación

Radicación 17-70745

VERSIÓN PÚBLICA

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCION DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por el artículo 17 de la Ley 1266 de 2008, el numeral 7 del artículo 16 del Decreto 4886 de 2011 y,

CONSIDERANDO:

PRIMERO: Que mediante Oficio con radicado No. 17-70745-00 de fecha 23 de marzo de 2017, la señora [redacted], presentó ante esta Superintendencia una queja en contra de **Avon Colombia S.A.S.** por una presunta vulneración a su derecho constitucional de *habeas data*. (fl. 1)

En particular, menciona lo siguiente: "*Tengo conocimiento de que se han realizado transacciones de carácter comercial en la plataforma virtual de la compañía Avon Colombia, a mi nombre, con el uso de mis datos alojados en este portal, actividades comerciales que no he realizado yo y han sido tomadas como efectivas, bajo el procedimiento de compra a crédito dispuesto por la compañía; con lo cual expreso mi preocupación, indignación y prejuicio provocado por vulneración de mis derechos y omisión a los deberes referentes al tratamiento y seguridad esencial de mis datos personales solicito se retire mi información del portal se anule cualquier compromiso de pago sobre la orden 3247799 y cualquier otra que bajo investigación no haya realizado yo se verifique y exponga que yo no recibí el pedido referente a esta orden y reparación e indemnización por los daños causados, Cito, suplantación de personalidad, abuso de confianza y tratamiento inadecuado e incumplimiento de norma sobre la disposición de datos personales*"[1]

Sobre este punto, Avon Colombia S.A.S. mediante comunicación del 6 de julio de 2018 manifestó lo que sigue a continuación. "*De conformidad con el concepto de buena fe por pasiva la Compañía confía que quien suscribe el respectivo contrato es el titular de los datos personales que presenta a través del mismo y que el pedido solicitado llega a manos de dicha persona, por lo que podemos predicar el derecho que se tiene de proceder con las gestiones de cobro cuando se incumplen las obligaciones contraídas para con nosotros*"[2]

SEGUNDO: Que una vez efectuado el análisis de la respuesta suministrada por el operador de información Experian Colombia S.A. (DataCrédito)[3], y los demás documentos obrantes dentro de la actuación administrativa, la Dirección de Investigación de Protección de Datos Personales, mediante Resolución No. 20499 del 23 de marzo de 2018 (fls. 68 a 70), resolvió

[1] Folios 2-3 (Comunicación del 13 de febrero de 2016)
[2] Folio 90
[3] Folios 30 a 32

lo siguiente:

> *"**ARTÍCULO PRIMERO:** Archivar la presente actuación según lo expuesto en la parte motiva de la presente resolución respecto de la solicitud de eliminación de la información crediticia reportada, toda vez que existe un hecho superado".*

TERCERO: Que en el término legal establecido para el efecto[4], mediante escrito radicado con el número 17-70745-15 del 17 de agosto de 2018, la señora [redacted] (en adelante la **RECURRENTE),** interpuso recurso de apelación contra la Resolución No. 20499 del 23 de marzo de 2018, con fundamento en los siguientes argumentos:

3.1 Manifiesta la **RECURRENTE** que en el acto administrativo recurrido se menciona *"en el parágrafo 10.1 respecto de la suplantación de identidad, que la declarante denuncio (sic) ante fiscalía y solicito (sic) que la sociedad investigada elimine el reporte negativo de su historial de crédito efectuado en las bases de datos de los operadores de información. Lo cual no fue dicho, ni está escrito en denuncia a la cual se hace referencia, como que se procede a indicar en base a lo anterior que no fue solicitado, ni dicho, mi historial crediticio con registro ante los operadores de la información citando a Cifin S.A. y a Experian Colombia compañías que no fueron nombradas ni expuestas en declaración ante fiscalía ni ante esta superintendencia, entes a lo que no se dijo de formal vernal ni escrita sobre solicitud de eliminación de reporte negativo hecho por la empresa Avon Colombia ante operadores de información, por la obligación referenciada ante Fiscalía ni en solicitud presentada a SIC, y tampoco en derecho de petición interpuesto a Avon Colombia."*

3.2 Teniendo en cuenta la situación descrita en la queja presentada ante esta Superintendencia, que a la letra dice: *"Avon Colombia permitió a personal vinculado a la compañía acceder y usar mis datos personales para realizar a mi nombre compra a crédito de sus productos sin mi conocimiento y autorización al informarlo se me indico que habían suplantado pese a mi petición de anular el pedido se me informo que lo entregarían."*, solicita la **RECURRENTE** en el recurso de alzada, se de aplicación a las normas establecidas en los artículos 23 y 24 (sic) de la Ley 1266 de 2008 (folio 51).

3.3 Más adelante transcribe la **RECURRENTE** tanto el derecho de petición que presentara ante Avon Colombia S.A.S., como la denuncia[5] que hizo ante la Fiscalía General de la Nación, por la comisión del delito de Falsedad Personal de conformidad con lo establecido en el artículo 296 del Código Penal, del que presuntamente fue víctima.

3.4 Indica que *"Si bien La Compañía Avon Colombia tiene autorización de usos de datos personales es en lo referente a lo permitido por la norma., Ahora bien, Avon Colombia no actuó bajo el principio de la buena Fe como se indica en resolución, referente a lo señalado en el art. 18 de ley La Ley 1266 de 2008".* Como sustento de lo dicho anteriormente, reseña los deberes de los Encargados[6] del Tratamiento de datos personales.

3.5 Culmina la sustentación del recurso señalando que *"El fallo que emite esta superintendencia referente a la solicitud de eliminación de eliminación de reporte negativo da lugar a la eliminación del reporte positivo suministrado a Experian Colombia dejando vectores de comportamiento sin información podría obstaculizar la claridad para trámites de crédito con otras entidades., también la honra y mi buen nombre…"*

---

[4] Conforme a constancia suscrita por la Secretaria General AD – HOC de la Superintendencia de Industria y Comercio, visible a folio 61 la Resolución No. 20499 del 23 de marzo de 2018, fue notificada al correo electrónico de la señora Carolina Ramos Perea el 23 de marzo de 2018, con lo cual el término para presentar los recursos vencía el 9 de abril de 2018, por lo que éstos fueron presentados oportunamente.

[5] Folios 33 y 34

[6] Folio 53 Artículo 18 de la Ley 1581 de 2012.

Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

CUARTO: Que mediante Resolución No. 66797 del 11 de septiembre de 2018 (fls. 102 a 106), 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. 20499 del 23 de marzo de 2018, así mismo, concede el recurso de apelación presentado de forma subsidiaria.

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 contra la Resolución No. 20499 del 23 de marzo de 2018, en los siguientes términos:

5.1 Respecto de la decisión contenida en la Resolución No. 20499 del 23 de marzo de 2018.

Indicó la **RECURRENTE**, que en la Resolución objeto del presente recurso, ordenó a la Compañía Avon Colombia S.A.S., la eliminación del reporte positivo generado ante el operador de información Experian Colombia S.A. dejando los vectores de comportamiento sin información.

Sobre este punto en particular, el artículo primero de la Resolución 20499 del 23 de marzo de 2018, dispuso:

> *"**ARTÍCULO PRIMERO:** Archivar la presente actuación según lo expuesto en la parte motiva de la presente resolución respecto de la solicitud de eliminación de la información crediticia reportada, toda vez que existe un hecho superado".*

Así las cosas, contrario a lo alegado por la **RECURRENTE**, por parte de la Dirección de Investigación de Protección de Datos Personales, no se emitió ninguna orden tendiente a la eliminación de información negativa o positiva que hubiese sido reportada por parte de la Fuente Avon Colombia S.A.S., al operador de información Experian Colombia S.A. (DataCrédito), razón por la cual no son de recibo por parte de este Despacho los argumentos esbozados sobre este aparte en el recurso de apelación.

5.2 Respecto de lo solicitado por parte de la recurrente en la queja inicialmente presentada.

Sobre este punto, sostuvo la **RECURRENTE**, que en el caso particular no se dio el trámite por ella solicitado, pues su requerimiento estaba dirigido a la protección de sus datos personales, pues de acuerdo con lo relatado en la queja, éstos fueron utilizados para realizar un pedido en la plataforma de Avon Colombia S.A.S., sin que haya existido para tal efecto autorización alguna.

Así las cosas, en el Recurso de Apelación planteado, se alega que esta Superintendencia debió dar aplicación a las normas contenidas en los artículos 18, 23 y 24 de la Ley 1266 de 2008, normas que fueron relacionadas por la **RECURRENTE**, como deberes de los encargados de información, sanciones y sus criterios de graduación, respectivamente.

De acuerdo con lo anterior, y en aras de dar claridad respecto de la normatividad a la que deberá dársele aplicación al caso que nos ocupa, procederá el Despacho a realizar una breve diferenciación entre el ámbito de aplicación de la Ley 1266 de 2008 *"por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales. en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"* y la Ley 1581 de 2012 *"por la cual se dictan disposiciones generales para la protección de datos personales"*.

Pues bien, el artículo 1 de la Ley 1266 de 2008, determina lo siguiente:

> ***"Artículo 1°. 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****". (Subraya y negrilla fuera de texto)*

Por su parte, el artículo 2 de la Ley 1581 de 2012, respecto de su ámbito de aplicación, dispone:

> ***Artículo 2°. 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:*
> ***(...)***
>
> ***e)*** ***A las bases de datos y archivos regulados por la Ley 1266 de 2008.*** *(Subraya y negrilla fuera de texto)*
>
> ***(...)***

Con base en las normas anteriormente citadas, y de acuerdo con la naturaleza de la relación comercial existente entre Avon Colombia S.A.S. y la señora [redacted], concuerda el Despacho con la primera instancia al haber dado aplicación a las normas contempladas en la Ley 1266 de 2008, en la medida que de acuerdo con lo establecido en su artículo 3[7], la sociedad investigada cuenta con las características de Fuente de Información.

Ahora bien, al analizar nuevamente los argumentos expuestos por la **RECURRENTE** en su escrito, entiende el Despacho que los mismos están dirigidos a la aplicación de las normas contenidas en los artículos 18, 23 y 24 de la Ley 1581 de 2012, por el indebido tratamiento de sus datos personales al ser utilizados presuntamente para realizar a su nombre una compra a crédito de los productos ofrecidos por la sociedad investigada, sobre este punto, y teniendo en cuenta las circunstancias que dieron lugar a la queja, la señora [redacted] interpuso ante la Fiscalía General de la Nación denuncia[8] por la presunta comisión del delito de Falsedad Personal establecido en el artículo 296 del Código Penal Colombiano.

---

[7] ***Artículo 3°. Definiciones.*** *Para los efectos de la presente ley, se entiende por:*
(...)
b) Fuente de información. ***Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular,*** *suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos;*
(...)

[8] Folios 33 y 34

Bajo esta perspectiva, considera el Despacho que en el presente caso no es posible acceder a lo pretendido por la **RECURRENTE** en la medida que, la situación que dio lugar a la presente actuación administrativa está siendo investigada por parte de la autoridad competente para ello, lo que lleva a concluir que hay duda respecto de la existencia misma de la conducta que pretende ser investigada por parte de esta Superintendencia.

No obstante lo anterior, la primera instancia con el fin de dar respuesta al recurso de reposición, consideró pertinente mediante Oficio con radicado No. 17-70745-22 del 26 de junio de 2018, solicitar a la sociedad Avon Colombia S.A.S., información referente a: **i)** la política de seguridad implementada por la sociedad, así como el detalle de las medidas de seguridad utilizadas para manejar la información de los Titulares; **ii)** el sistema de protocolo de asignación de usuario y contraseña de los Titulares y **iii)** el procedimiento para los registros de creación del usuario y cambio de contraseña de la quejosa.

En el mismo sentido se le solicitó información[9] a la **RECURRENTE,** de la cual no se obtuvo respuesta alguna.

Como respuesta a la solicitud hecha, la sociedad Avon Colombia S.A.S., mediante Oficio con radicado No. 17-70745-24 de fecha 6 de julio de 2018[10], informó el procedimiento que deben seguir las Representantes cuando van a realizar algún pedido en la plataforma, y respecto del cual la primera instancia indicó al resolver el recurso de reposición[11] que, y sobre lo cual este Despacho está de acuerdo, *"esta Dirección determina que no se evidencia un indebido manejo de la información crediticia de la Titular, toda vez que en principio, la sociedad investigada detalló el paso a paso del procedimiento para el registro de creación del usuario y cambio de contraseña de la señora* [redacted]*, y además, cuenta con una política para el tratamiento de los datos personales tal y como lo establecen las disposiciones que rigen el sistema general de datos personales en Colombia. Adicionalmente, en los procedimientos detallados por* ***AVON COLOMBIA S.A.S.*** *no se evidencia de alguno que contravía las disposiciones legales enunciadas"*

De acuerdo con lo anteriormente indicado, considera el Despacho que la sociedad investigada cuenta con los mecanismos pertinentes para dar el tratamiento a los datos de conformidad con el Régimen de Protección de Datos Personales.

SEXTO: Aunque las razones anteriores son suficientes para confirmar la Resolución No. 20499 del 23 de marzo de 2018esta Delegatura considera pertinente destacar lo siguiente respecto de:

(i) Responsabilidad personal de los administradores
(ii) Responsabilidad demostrada (accountability) y "compliance" en el tratamiento de datos personales
(iii) De la suplantación de identidad y el tratamiento de datos personales

6.1 Responsabilidad de los Administradores en materia de tratamiento de datos personales.

Según el artículo 22 de la ley 222 de 1995[12] la expresión administradores comprende al "*representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y*

---

[9] Folio 71
[10] Folios 78 y 79

[11] Folio 104 reverso
[12] 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"

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. Es por eso que el artículo 23 de la ley en mención establece que los administradores no sólo deben "*obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios*", sino que en el ejercicio de sus funciones deben "*velar por el estricto cumplimiento de las disposiciones legales o estatutarias*"[13] (subrayamos)

Obsérvese que la regulación no exige cualquier tipo de cumplimiento de la ley, sino uno calificado, es decir, estricto o ajustado 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 (no formal), efectiva y rigurosa. Por eso, los administradores deben cuidar con esmero este aspecto y no sólo ser guardianes sino promotores de la correcta y precisa aplicación de la ley. Esto, desde luego, implica que los administradores deben verificar permanentemente si la ley se está cumpliendo en todas las actividades que realiza su empresa u organización.

Nótese que el artículo 24[14] de la ley en comento presume la culpa del administrador "*en los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos*". Dicha presunción de responsabilidad exige que los administradores estén en capacidad de probar que han obrado con lealtad y la diligencia de un experto, es decir, como un "*buen hombre de negocios*" tal y como lo señala el precitado artículo 23. Adicionalmente, no debe perderse de vista que los administradores jurídicamente responden "*solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros*"[15]

Todo lo anterior pone de presente no sólo el alto nivel de responsabilidad jurídica y económica en cabeza de los administradores, sino el enorme profesionalismo y diligencia que debe rodear su gestión en el tratamiento de datos personales.

6.2. 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 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*"[16].

---

[13] Cfr. Numeral 2 del artículo 23 de la ley 222 de 1995

[14] 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."

[15] Cfr. Parte inicial del artículo 24 de la ley 222 de 1995

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

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

En virtud de lo anterior, el capítulo III del Decreto 1377 del 27 de junio de *2013 -incorporado en el decreto 1074 de 2015-* reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada. El artículo 26[17] *-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*" y dicho decreto. Nótese como le corresponde al Responsable o al Encargado probar que ha puesto en marcha medidas adecuadas, útiles y eficaces para cumplir la regulación. Lo anterior significa que un administrador no puede utilizar cualquier tipo de política o herramienta para dicho efecto sino sólo aquellas que sirvan para que los postulados legales no sean meras elucubraciones teóricas sino realidades verificables.

El artículo 27 *-denominado POLÍTICAS INTERNAS EFECTIVAS-*, por su parte, exige que los Responsables implementen medidas efectivas y apropiadas que garanticen, entre otras, lo siguiente: "*(...) 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.*"[18] Respecto de la supresión del dato, el artículo 18 señala que los procedimientos para dicho efecto deben incluirse en la política de tratamiento de información y ser informados a los titulares de los datos[19]. El artículo 22. por su parte, establece que el Responsable o Encargado del tratamiento debe adoptar "*las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean (...) actualizados, rectificados o*

---

[17] 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"

[18] El texto completo del artículo 27 del decreto 1377 de 2013 señala lo que sigue a continuación: "*Artículo 27. 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*".

[19] El texto completo del artículo 18 del decreto 1377 de 2013 señala lo siguiente: "*ARTÍCULO 18. PROCEDIMIENTOS PARA EL ADECUADO TRATAMIENTO DE LOS DATOS PERSONALES. Los procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización deben darse a conocer o ser fácilmente accesibles a los Titulares de la información e incluirse en la política de tratamiento de la información.*"

suprimidos, (..) "[20]. Obsérvese que la norma exige que se asegure, entre otros, la supresión de los datos lo cual implica que la obligación legal no es de medio sino de resultado, en este caso, la eliminación definitiva del dato personal cuando esta sea procedente a la luz del ordenamiento jurídico.

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)"*[21]. El término *"accountability"* proviene del mundo anglosajón[22] y a pesar de las diferentes acepciones que puedan darse sobre el significado del mismo, se ha entendido que en la arena de la protección de datos dicha expresión se refiere al modo como una organización debe cumplir en la práctica las regulaciones sobre el tema y a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente.

En línea con lo anterior, la precitada guía recomienda lo siguiente a los obligados a cumplir la ley 1581 de 2012:

(1) Diseñar y poner en marcha un programa integral de gestión de datos (en adelante PIGDP), lo cual exige compromisos y acciones concretas de los directivos de la organización, así como la implementación de controles de diversa naturaleza que se enuncian en el texto de la guía;
(2) Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP, y
(3) Demostrar el debido cumplimiento de la regulación sobre tratamiento de datos personales.

El principio de responsabilidad demostrada –*accountability*- demanda implementar acciones de diversa naturaleza[23] para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo exige que los Responsables y Encargados del tratamiento implementen medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia. Dichas medidas deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

El principio de responsabilidad demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Éste exige implementar 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 pero, especialmente, de los directivos de las organizaciones ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para diseñar, implementar, revisar, actualizar y 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

---

[20] El texto completo del artículo 22 del decreto 1377 de 2013 ordena lo que sigue a continuación:' *ARTÍCULO 22. DEL DERECHO DE ACTUALIZACIÓN, RECTIFICACIÓN Y SUPRESIÓN. En desarrollo del principio de veracidad o calidad, en el tratamiento de los datos personales deberán adoptarse 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*".

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

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

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

políticas porque exige que se demuestre el cumplimiento real y efectivo en la práctica cuando realizan 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****"*[24] (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 guía[25], 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"*[26]. 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)"*[27]. Adicionalmente se precisa que *"ya no vale solo intentar cumplir" la ley* sino que las organizaciones "d*eben 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*"[28].

En virtud de lo anterior, 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

---

[24] 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.

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

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

[27] 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/

[28] Idem

"*sistema de administración de riesgos asociados al tratamiento de datos personales*"[29] 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*"[30].

6.2. Suplantaciones de identidad y tratamiento de datos personales

La eventual suplantación de identidad fue el motivo principal que generó la queja de la **RECURRENTE**. Frente a esta situación, en el expediente no constan medidas de seguridad especiales que haya adoptado **AVON COLOMBIA S.A.S.** para prevenir esa situación.

Suplantar significa, entre otras, *"ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba"*[31]; *"sustituir ilegalmente a una persona u ocupar su lugar para obtener algún beneficio"*[32]; La suplantación de identidad consiste en hacerse pasar por otra persona para diversos propósitos: engañar a terceros, obtener bienes y servicios con cargo a la persona suplantada, incurrir en fraudes y otro de conductas ilícitas. Es notorio el problema y las consecuencias que ha generado esta situación. Desde 2014, por ejemplo, los medios de comunicación han puesto de presente que la suplantación de identidad es uno de los motivos más frecuentes de las quejas de los ciudadanos. En ese entonces se señaló que:

> *"La información que la gente publica en sus redes sociales está siendo usada por manos inescrupulosas. El robo de identidad es una de las quejas más frecuentes de los usuarios ante la Superintendencia de Industria y Comercio.*
>
> *"Existen algunos delincuentes que se dedican a utilizar esa información personal para efectos de hacer un robo de la identidad de los ciudadanos y, por ejemplo, sacar productos a nombre de esos ciudadanos"*
>
> *"18 empresas han sido sancionadas en lo corrido del año por no cuidar los datos de sus clientes. En la mayor parte de los casos son empresas que han sido engañadas por delincuentes que se han dedicado a este negocio"*[33]

Mediante la suplantación de identidad los impostores obtienen créditos, adquieren productos o servicios en nombre de la persona suplantada y ésta última es la afectada porque, en muchos casos, le toca asumir el pago de dichas obligaciones. Con esto, desde la perspectiva del tratamiento de datos personales se observa que se vulneran, por lo menos y según el caso, los principios de veracidad y seguridad.

Se infringe el principio de veracidad porque la información tratada, difundida o reportada sobre una deuda adquirida por un suplantador no es veraz respecto de la persona suplantada ya que ella no fue quien adquirió dicha obligación. Esos datos inducen a error porque faltan a la realidad y presentan como obligada o morosa a una persona respecto de una deuda que no adquirió. Recuérdese que el tratamiento de este tipo de datos está proscrito por nuestra regulación, tanto la ley 1266 de 2008 como la 1581 de 2012 expresamente prohíben "*el*

---

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

[30] Ibid. P 16

[31] Cfr. Diccionario de la lengua española. Actualización 2017. http://dle.rae.es/?id=YIZNKd0

[32] Cfr. WordReference.com: http://www.wordreference.com/definicion/suplantar

[33] Cfr. Noticias RCN. Suplantación de identidad, una de las quejas más frecuentes de ciudadanos. Octubre 29 de 2014. Disponible en: https://noticias.canalrcn.com/nacional-pais/suplantacion-identidad-una-las-quejas-mas-frecuentes-ciudadanos

registro y divulgación de datos (...) que induzcan a error"[34] o el "*tratamiento de datos (...) que induzcan a error*"[35]

Se desconoce el principio de seguridad porque el suplantador puede incurrir en "*consulta, uso o acceso no autorizado o fraudulento*"[36] a los datos personales de la persona suplantada, que será el titular del dato afectado. En línea con lo anterior, también se quebranta el principio de circulación restringida porque el suplantador accede a datos personales del titular suplantado sin estar autorizado para ello.[37] En ese sentido, el literal f) del artículo 4 (Principio de acceso y circulación restringida) de la ley 1581 de 2012 señala que "*Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley*".

Proteger la información es una condición crucial del tratamiento de datos personales. Una vez recolectada debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos Responsables y Encargados del tratamiento de los datos. El acceso, la consulta y el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos naturales y humanos que se quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa o técnica.

La seguridad de la información ha sido una preocupación del legislador *y la Corte Constitucional.* Esta última concluyó que "*debe reiterarse que el manejo de información no pública debe hacerse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el Responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular*".[38]

No debe perderse de vista que la suplantación de identidad a través de internet sigue siendo un problema muy grave. En el informe "Balance Cibercrimen Colombia 2017" publicado por el Centro Cibernético Policial de la Policía Nacional de Colombia, por ejemplo, se señala lo siguiente:

> "*el 55.3% de los incidentes atendidos a través de @CaiVirtual fueron estafas en Internet, constituyéndose como el delito con mayor afectación a los colombianos. Dentro de las modalidades con mayor impacto se destacan: Compra y venta de productos en Internet*"
>
> *Por otra parte 6372 ciudadanos han reportado este tipo de defraudaciones.*
>
> • *El 60% de las estafas corresponden al fraude por compra o venta de productos en internet: 3846 reportes*"[39]

Dada esta situación no es de recibo la siguiente afirmación de AVON: "*De conformidad con el concepto de buena fe por pasiva la Compañía confía que quien suscribe el respectivo contrato es el titular de los datos personales que presenta a través del mismo y que el pedido*

---

[34] Cfr. Parte final del literal a) del artículo 4 (Principio de veracidad o calidad de los registros o datos) de la ley 1266 de 2008.

[35] Cfr. Parte final del literal d) del artículo 4 (Principio de veracidad o calidad) de la ley 1581 de 2012.

[36] Cfr. Literal g) del artículo 4 (Principio de seguridad) de la ley 1581 de 2012. En este mismo sentido, el literal f) del artículo 4 (Principio de seguridad) de la ley 1266 de 2008 señala que los datos "se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su (...) consulta o uso no autorizado".

[37] Cfr. Literal c) del artículo 4 (Principio de circulación restringida) de la ley 1266 de 2008.

[38] Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.6.5.2.6.

[39] Cfr. Policía Nacional. Centro Cibernético Policial. Balance Cibercrimen Colombia 2017. El texto del informe puede consultarse en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

solicitado llega a manos de dicha persona, por lo que podemos predicar el derecho que se tiene de proceder con las gestiones de cobro cuando se incumplen las obligaciones contraídas para con nosotros"[40]

Obrar de buena fe no es suficiente frente a fenómenos como la suplantación de identidad. Adicionalmente, el artículo 23 de la ley 222 de 1995 obliga a los administradores con la diligencia de un buen hombre de negocios. Esto último les demanda ser proactivos y adoptar acciones concretas que van mucho más allá de obrar de buena fe.

Finalmente, nótese que la redacción del principio de seguridad en las leyes 1581 y 1266 tienen un enfoque eminentemente PREVENTIVO, lo cual obliga a los Responsables o Encargados a adoptar medidas para impedir afectaciones a la seguridad de los datos.

En virtud de todo lo anterior, **EXHORTAMOS** a los Representantes Legales de **AVON COLOMBIA S.A.S** para que adopten medidas pertinentes, útiles, efectivas y verificables con miras a:

1) Evitar eventuales suplantaciones de identidad que se originen con el tratamiento de datos personales

2) Implementar 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)"*[41]. Especial énfasis se debe hacer en lo dispuesto respecto del principio de seguridad.

SEPTIMO: Que analizada la cuestión planteada, este Despacho no accederá a lo solicitados por la **RECURRENTE** y teniendo en cuenta lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirmará la decisión contenida en la Resolución No. 20499 del 23 de marzo de 2018.

En mérito de lo expuesto, este Despacho,

RESUELVE:

ARTÍCULO PRIMERO: Confirmar en todas sus partes la Resolución No. 20499 del 23 de marzo de 2018, de conformidad con lo expuesto en la parte motiva de la presente resolución.

ARTÍCULO SEGUNDO: Exhortar a los Representantes Legales de **AVON COLOMBIA S.A.S** RICARDO HINOJOSA, C.E. 570.482; GUSTAVO CRUZ MATIZ, C.C. 79.914.859; LIVIO CESAR HUGO VICCO, C.E. 539.318; ENRIQUE VALCKE MALLET, C.C. 16783.759; JULIAN DAVID VELEZ VELEZ, C.C. 3.383.501; GUILLERMO ARCINIEGAS TORO, C.C. 70.557.880; JUAREZ NICOLINI FILHO, C.E. 519.933, para que adopten las medidas pertinentes, útiles, efectivas y verificables con miras a:

a) Evitar eventuales suplantaciones de identidad que se originen con el tratamiento de datos personales

b) Implementar 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*

---

[40] Folio 90

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

(accountability)"[42]. Especial énfasis se debe hacer en lo dispuesto respecto del principio de seguridad.

ARTÍCULO TERCERO: Notificar personalmente el contenido de la presente resolución a la señora [redacted], identificado con la cédula de ciudadanía No. 1.017.146.681, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO CUARTO: Comunicar la presente decisión a la Sociedad **AVON COLOMBIA S.A.S.** identificada con el NIT No. 900.041.917-7, a través de su representante legal o quien haga sus veces.

NOTIFÍQUESE, COMUNIQUESE Y CÚMPLASE

Dada en Bogotá, D.C., 17 DIC 2018

El Superintendente Delegado para la Protección de Datos Personales,

NELSON REMOLINA ANGARITA

NTL

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

VERSIÓN PÚBLICA

Por la cual se resuelve un recurso de apelación

NOTIFICACIÓN:

Reclamante:

Señora: [redacted]
Identificación:
Dirección:
Ciudad:
Correo Electrónico:

COMUNICACIÓN

Fuente de la información:

Sociedad:	**AVON COLOMBIA S.A.S.**
Identificación:	Nit. 900.041.914-7
Representantes Legales:	**RICARDO HINOJOSA** C.E. 570.482 **GUSTAVO CRUZ MATIZ** C.C. 79.914.859 **LIVIO CESAR HUGO VICCO** C.E. 539.318 **ENRIQUE VALCKE MALLET** C.C. 16783.759 **JULIAN DAVID VELEZ VELEZ** C.C. 3.383.501 **GUILLERMO ARCINIEGAS TORO** C.C. 70.557.880 **JUAREZ NICOLINI FILHO** C.E. 519.933
Dirección:	Calle 14 No. 52 A - 272
Ciudad:	Medellín (Antioquia)
Correo Electrónico:	departamento.impuestos@avon.com – impuestos@avon.com