



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

RESOLUCIÓN NÚMERO 9800 - - - - DE 2019

(25 ABR 2019)

"Por la cual se impone una sanción y se imparten órdenes"

Radicación 18-89592

VERSIÓN PÚBLICA

EL DIRECTOR DE INVESTIGACIÓN DE 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 y el numeral 5 del artículo 17 del Decreto 4886 de 2011 y,

CONSIDERANDO

PRIMERO: Que el 23 de octubre de 2017, esta Superintendencia mediante Resolución N° 66983 ordenó lo siguiente:

"ARTÍCULO TERCERO: trasladar la presente actuación al Grupo de Trabajo de Investigaciones Administrativas para que proceda de acuerdo con su competencia"

SEGUNDO: En virtud de la remisión efectuada por el Grupo de Hábeas Data de la queja presentada por el señor [REDACTED], esta Superintendencia tuvo conocimiento de la presunta violación de las normas de protección de datos personales contenidas en la Ley 1581 de 2012, por parte de la sociedad **RAPPI S.A.S.** identificada con Nit. 900.843.898-9; razón por la cual se inició investigación administrativa en consideración a los siguientes hechos:

- 2.1 Indicó el titular que el 3 de noviembre de 2016 presentó una petición ante la sociedad **RAPPI S.A.S.**, mediante la cual solicitó que fueran suprimidos sus datos personales para efectos de envíos de mensajes de texto a su teléfono celular y a su correo electrónico. No obstante el señor [REDACTED], señaló que siguió recibiendo mensajes por parte de la investigada.
- 2.2 Así mismo, y dentro de las actuaciones adelantadas por el Grupo de Hábeas Data de esta Dirección, no se evidenció que la sociedad investigada contará con la autorización previa, expresa e informada otorgada por el titular, pues pese a que señaló que cada usuario de su plataforma tiene que aceptar los términos y condiciones para poder tratar sus datos, no allegó a este Despacho el medio técnico correspondiente que demuestre el consentimiento otorgado por el señor [REDACTED].
- 2.3 De igual manera, el Despacho consideró que **RAPPI S.A.S.** presuntamente no garantizó el derecho de *habeas data* del titular, toda vez que continuó tratando los datos Personales del titular pese a la solicitud de eliminación de su información presentada ante la sociedad investigada.

TERCERO: Que con base en los hechos anotados, a partir de los cuales se advierte la presunta violación de las normas sobre protección de datos personales, mediante Resolución No. 21206 del 26 de marzo de 2018, la Dirección de Investigación de Protección de Datos Personales resolvió iniciar investigación administrativa contra la sociedad **RAPPI S.A.S.**, en calidad de Responsable del Tratamiento y, en esa medida, por el presunto incumplimiento le formuló los siguientes cargos:

- 3.1 Por el presunto incumplimiento a lo dispuesto en el literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y artículo 9 de la norma en mención; y inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.

3.2 Por la posible vulneración a lo dispuesto en el literal a) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal e) del artículo 8 de la norma en mención, junto con el artículo 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015.

Que mediante la Resolución N° 45746 del 29 de junio de 2018 la Dirección de Investigación de Protección de Datos Personales resolvió corregir un error de transcripción y correr nuevamente traslado para presentar Descargos a la Sociedad investigada.

CUARTO: Que mediante comunicado radicado bajo el No. 18-89592-12, la Coordinación del Grupo de Notificaciones y Certificaciones de esta Superintendencia, certificó que el 12 de julio de 2018 fue notificada por aviso la Resolución N° 45746 del 29 de junio de 2018, la cual concedió quince (15) días para que el investigado ejerciera su derecho de defensa y contradicción de acuerdo a lo establecido por el inciso tercero del artículo 47 del Código Administrativo y de lo Contencioso Administrativo. Una vez vencido el término establecido para allegar descargos y aportar pruebas, ésta guardó silencio.

QUINTO: Que mediante la Resolución N° 6915 del 19 de septiembre de 2018, y con el fin de tener mayores elementos de juicio para decidir la presente investigación este Despacho resolvió requerir a la sociedad **RAPPI S.A.S.** para que informara si procedió a atender la solicitud de supresión de los datos personales del señor [REDACTED].

A lo cual, la sociedad investigada mediante comunicado del 28 de septiembre de 2018, aportó la información requerida junto con las pruebas que pretende hacer valer para el efecto.

SEXTO: Que mediante la Resolución N° 4999 del 28 de febrero de 2019, esta Dirección procedió a correr traslado para presentar alegatos de conclusión e incorporó las siguientes Pruebas:

- 6.1 Copia de la resolución N° 66983 del 23 de octubre de 2017, obrante a folios 1 al 5 del expediente.
- 6.2 Las pruebas allegadas por el titular junto con la reclamación presentada ante esta Superintendencia el 9 de febrero de 2017, obrantes a folios 6 al 8 del expediente.
- 6.3 Comunicado allegado por la sociedad investigada el 7 de abril de 2017, obrante a folios 9 al 15 del expediente.
- 6.4 Copia de los mensajes de correo electrónico enviados por el Titular a la sociedad investigada, obrantes a folios 17 al 26 del expediente.
- 6.5 Documentos allegados por la sociedad investigada junto con el escrito radicado el 28 de septiembre de 2018, obrantes a folios 48 al 90 del expediente.

SÉPTIMO: Que mediante escrito presentado el 26 de marzo de 2019 la sociedad **RAPPI S.A.S.**, allegó sus alegatos de conclusión señalando lo siguiente:

- 7.1 Indicó que, de acuerdo con las pruebas aportadas por la investigada, se puede evidenciar que *"los datos personales del señor [REDACTED] fueron eliminados de las bases de datos de la compañía (...) es claro que Rappi S.A.S. cumplió con la orden impartida por el titular de los datos la cual era eliminar sus datos de las bases de datos de la compañía"*.
- 7.2 Igualmente señaló que *"(...) Rappi S.A.S. en todo momento salvaguardó los derechos que le otorga la ley al titular de los datos personales y, en vista de ello, es claro que a partir del material probatorio aportado por Rappi S.A.S., no existen razones para aplicar algún tipo de sanción frente a esta compañía, toda vez que su accionar siempre estuvo ajustado a la ley y en ningún momento se vulneraron los derechos del titular de los datos personales"*.

OCTAVO: Competencia de la Superintendencia de Industria y Comercio

El artículo 19 de la Ley 1581 de 2012, establece la función de vigilancia que le corresponde a la Superintendencia de Industria y Comercio para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la ley.

NOVENO: Análisis del caso

9.1 Adecuación típica

La Corte Constitucional mediante sentencia C-748 de 2011¹, estableció lo siguiente en relación con el principio de tipicidad en el derecho administrativo sancionatorio:

"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 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".

Atendiendo los parámetros señalados por la citada jurisprudencia, para el caso específico se tiene que:

(i) El artículo 17 de la Ley 1581 de 2012 establece los deberes que les asisten a los Responsables del Tratamiento respecto del manejo de los datos personales de los Titulares. El incumplimiento de tales requisitos dará lugar a la aplicación de las sanciones definidas específicamente en el artículo 23 de la Ley 1581 de 2012.

(ii) De conformidad con los hechos alegados por el reclamante y el acervo probatorio que obra en el expediente, se puede establecer que la conducta desplegada por la investigada se concreta en la posible vulneración de los literales a) y b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4, el artículo 9 y el literal e) del artículo 8 de la norma en mención, así como de los artículos 2.2.2.25.2.2 y 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015.

En ese orden de ideas, este Despacho procederá a tener en cuenta: (i) los hechos narrados por el denunciante; (ii) las razones de hecho y de derecho aducidas por la investigada al momento de dar respuesta a los alegatos de conclusión; (iii) el material probatorio que obra dentro del expediente; (iv) las normas que comprenden el régimen general de protección de datos personales y, finalmente, (v) la jurisprudencia que ha proferido la Corte Constitucional sobre la materia.

9.2 Valoración probatoria y conclusiones

9.2.1 Deber de garantizar al Titular en todo tiempo, el pleno y efectivo ejercicio del derecho de *habeas data*.

El título II de la Ley 1581 de 2012 contiene los principios rectores del Régimen General de Protección de Datos Personales, los cuales deben ser interpretados y aplicados armónicamente al momento de realizar una investigación por infracciones al mencionado régimen. Específicamente el literal c) del artículo 4 se encuentra relacionado con el caso en concreto, que expresamente señala:

"Artículo 4°. Principios Para el Tratamiento de Datos Personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

(...)

c) Principio de Libertad: 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"

¹ Corte Constitucional, Magistrado Ponente Jorge Ignacio Pretelt Chaljub, seis (6) de octubre de dos mil once (2011).

Los principios rectores, además, deben confluir en cuanto a su aplicación con los deberes y derechos contenidos en la Ley 1581 de 2012, específicamente en el presente caso, es relevante mencionar los deberes que tienen los Responsables de garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

Por su parte, el literal a) del artículo 17 de la Ley 1581 de 2012, establece uno de los deberes a cargo de los Responsables de la Información en los siguientes términos:

(...)

a) *Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.*"

En relación, la Corte Constitucional ha definido el derecho de habeas data en los siguientes términos:

"El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales".²
(Negrilla fuera de texto).

De igual manera, la misma corporación en la sentencia C-748 de 2011, mediante la cual realiza el análisis constitucional de la Ley estatutaria 1581 de 2012, manifestó:

"De conformidad con la jurisprudencia de esta Corporación, dentro de las prerrogativas – contenidos mínimos- que se desprenden de este derecho encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificadas o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa." (subrayado fuera de texto).

Al respecto, debe precisar este Despacho que, tal como lo manifiesta la Corte Constitucional, el derecho de hábeas data otorga la facultad al Titular de los datos personales de exigir el acceso, corrección, adición, actualización y eliminación de su información, por lo que resulta apenas claro, que corresponde a los Responsables y Encargados de la información implementar los mecanismos necesarios que le permita al Titular ejercer de manera efectiva los derechos antes mencionados .

Ahora bien, frente a la posibilidad que tienen los Titulares de revocar la autorización y/o solicitar la supresión de su información, el literal e) del artículo 8 de la Ley 1581 de 2012 establece lo siguiente:

"Artículo 8°. Derechos de los Titulares. El Titular de los datos personales tendrá los siguientes derechos:

(...)

e) *Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;*

(...)"

De esta manera, es oportuno señalar que el citado artículo 8 establece que los Titulares pueden solicitar la supresión de su información personal cuando en el Tratamiento no se respeten los

² Sentencia C-748 de 2011; MP: Jorge Ignacio Pretelt Chaljub

principios, derechos y garantías constitucionales y legales. La Corte Constitucional, en la sentencia que analizó la exequibilidad de la citada ley³, determinó que *“el individuo también es libre de decidir cuales informaciones desea que continúen y cuáles deben ser excluidas de una fuente de información, siempre y cuando no exista un mandato legal que le imponga tal deber, o cuando exista alguna obligación contractual entre la persona y el controlador de datos, que haga necesaria la permanencia del dato”*.

Entonces, es claro que de conformidad con los principios que regulan la administración de datos personales, el ejercicio del derecho fundamental de *habeas data* permite a los Titulares solicitar la exclusión de información que haya sido recogida en bases de datos.

Superada la anterior discusión, se observa en el presente caso que el 3 de noviembre de 2016 el señor [REDACTED] presentó una petición ante la sociedad **RAPPI S.A.S.**, mediante la cual solicitó *“(...) abstenerse de (i) utilizar mi información y mis datos para todo y cualquier propósito; y (ii) enviarme cualquier correo electrónico o mensaje de datos a mis direcciones de correo electrónico y mi número de celular”*. Sin embargo, y pese a la clara e inequívoca revocatoria de autorización hecha por el titular, la sociedad investigada continuó tratando la información personal del señor [REDACTED]. Es decir, RAPPI S.A.S. no respetó la decisión del titular del dato e hizo caso omiso a su solicitud vulnerando los derechos de la persona citada.

Por su parte, la sociedad investigada mediante escrito allegado el día 28 de septiembre de 2018, señaló que *“(...) que desde el día 28 de marzo de 2017, el señor Santiago Varela Torres fue eliminado de la base de datos desde la cual se envían mensajes de texto”*. Igualmente, indicó que desde el 10 de marzo de 2017 el titular dejó de recibir mensajes de texto por parte de la investigada, tal como se evidencia a continuación:

Todos los números en la lista negra Q AÑADIR

100
TOTAL DE NÚMEROS EN LA LISTA
NEGRA

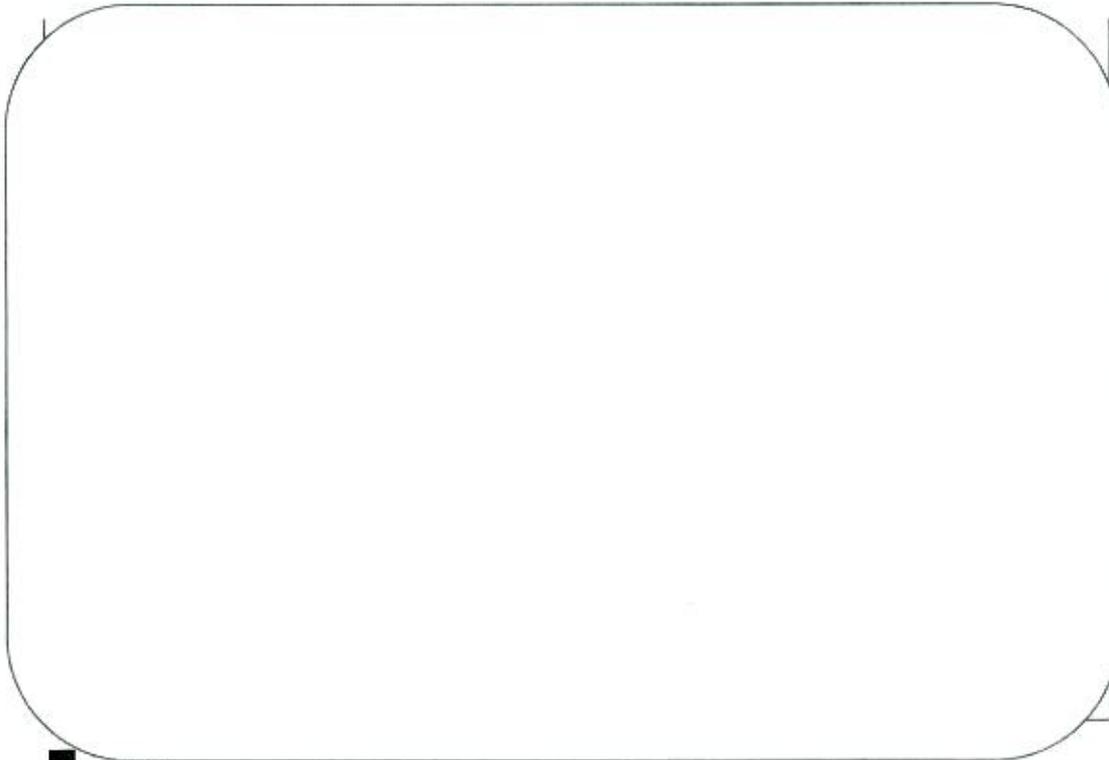
• TODAS LAS CUENTAS

GSM	FUENTE	CUENTA	CREADO EL
[REDACTED]	CUSTOM	Cuenta principal	16/11/2016 14:37:08
[REDACTED]	CUSTOM	Cuenta principal	26/11/2016 23:29:34
[REDACTED]	CUSTOM	Cuenta principal	25/09/2016 13:26:53
[REDACTED]	CUSTOM	Cuenta principal	03/11/2016 05:55:27
[REDACTED]	CUSTOM	Cuenta principal	05/12/2016 17:41:13
[REDACTED]	CUSTOM	Cuenta principal	07/12/2016 18:09:48
[REDACTED]	CUSTOM	Cuenta principal	13/10/2016 11:04:10
[REDACTED]	CUSTOM	Cuenta principal	13/10/2016 11:45:31
[REDACTED]	CUSTOM	Cuenta principal	25/10/2016 10:33:56

[REDACTED]

BORRAR Primero 1 2 3 4 5 Último 21/30 DE 100

³ Corte Constitucional, sentencia C-748 de 2011. M.P.: Jorge Ignacio Pretelt Chaljub.



Logo of the National Administrative Department of Justice (DAJ) and the National Office of Information Protection (ONIP).
NIT 900588221
República de Colombia - Calle 110 # 67-98 Oficina 204 - Bogotá, Colombia

Page 1

Sumado a lo anterior, la sociedad **RAPPI S.A.S.** manifestó que el correo electrónico del titular fue suprimido de su base de datos desde el 27 de abril de 2018, toda vez que el 15 de marzo de dicha anualidad, el señor [REDACTED] solicitó nuevamente ser incluido en la base de datos.

Al respecto, este Despacho encuentra probado dentro del expediente, que el titular en ejercicio de su derecho de *habeas data* solicitó la supresión de su información personal de las bases de datos de la sociedad **RAPPI S.A.S.**, sin lograr que su petición fuera atendida de manera diligente y oportuna. Pues tal y como se evidencia en las respuestas emitidas por la investigada, los datos personales para efectos de los envíos de mensajes de texto, solo fueron suprimidos hasta el 28 de marzo de 2017, es decir que señor [REDACTED], tuvo que esperar cuatro (4) meses y veinticinco (25) días para que fuera atendida su solicitud y por consiguiente dejara de vulnerarse su derecho fundamental de *habeas data*.

De igual manera, para esta Dirección no son de recibo los argumentos de la sociedad investigada, al afirmar que el 15 de marzo de 2018, el titular suministró nuevamente su correo electrónico y autorizó el tratamiento del mismo, pues aunque aporta una prueba obrante a folio 89 del expediente, la misma no demuestra el consentimiento previo, expreso e informado otorgado por el señor [REDACTED].

En atención a lo anterior, es menester destacar que uno de los pilares fundamentales de la regulación en materia de protección de datos personales es la exigencia de contar con la autorización previa, expresa e informada del Titular, esto es, la expresión de la voluntad inequívoca otorgada por el mismo para que sus datos personales sean recolectados, ingresen a la base de datos del caso y se utilicen para los fines que fueron autorizados. Sin embargo, dicho consentimiento que en algún momento fue brindado por el Titular, no es inamovible, pues este puede ser revocado a solicitud del mismo.

Por ello mismo, es importante traer a colación el artículo 2.2.2.25.2.6 del Decreto Reglamentario 1074 de 2015⁴, el cual dispone lo siguiente:

“ARTÍCULO 2.2.2.25.2.6. Revocatoria de la autorización y/o supresión del dato. Los Titulares podrán en todo momento solicitar al responsable o encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos,

⁴ Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, norma que compiló, entre otros, el Decreto 1377 de 2013 que reglamentó parte del articulado de la Ley 1581 de 2012.

mediante la presentación de un reclamo, de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

El responsable y el encargado deben poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada.

Si vencido el término legal respectivo, el responsable y/o el encargado, según fuera el caso, no hubieran eliminado los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012".

Entonces, es claro que de conformidad con los principios que regulan la administración de datos personales, el ejercicio del derecho fundamental de hábeas data permite a los Titulares solicitar la exclusión de información que haya sido recogida en bases de datos, pues este podrá revocar la autorización y solicitar la supresión del dato cuando, además de que no se respeten los principios, derechos y garantías constitucionales y legales⁵, no exista una obligación legal o contractual que imponga al titular el deber de permanecer en la referida base de datos. En este caso, no existe la obligación de los titulares de los datos de recibir la publicidad o mensajes de **RAPPI S.A.S.**, quien debe ser muy profesional y diligente para garantizar los derechos de las personas.

En este orden de ideas está plenamente demostrado que el Responsable del Tratamiento hizo caso omiso a la solicitud de supresión efectuada el 3 de noviembre de 2016, por el señor [REDACTED] y dejó asociado a su nombre su cuenta de correo electrónico y su número telefónico en su plataforma.

Sumado a lo anterior, esta Dirección tampoco observa que, de acuerdo a lo previsto por el artículo 2.2.25.2.6 del Decreto Reglamentario 1074 de 2015, exista una justificación legal o contractual para no dar trámite a la solicitud elevada por el Denunciante en este sentido.

Dicho de otra forma, el ejercicio del derecho de revocatoria de la autorización inicial que de forma clara y suficiente comunicó el señor [REDACTED], la sociedad **RAPPI S.A.S.**, fue desatendido por la investigada, razón suficiente para imponer la correspondiente sanción e impartir las órdenes pertinentes en aras de velar por la protección del derecho de *habeas data* tanto del denunciante como de todos los titulares que utilizan los servicios brindados por la investigada.

Por lo anterior, se encuentra probado que la sociedad investigada no respetó el derecho del Titular de suprimir sus datos, por lo cual infringió el deber de garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de *habeas data*, consignado en el literal a) del artículo 17 de la Ley 1581 de 2012.

9.2.2 Deber de solicitar y conservar copia de la autorización para el Tratamiento de los datos personales de los Titulares

Sobre el particular, este Despacho considera pertinente señalar que la Constitución Política reconoce el derecho de las personas a decidir libremente frente al uso de la información que sobre ellas se haya recogido en banco de datos o archivos de entidades públicas o privadas. El artículo en cuestión señala lo siguiente:

"ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, 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.

⁵ En cuyo caso, y con el fin de garantizar el debido proceso, corresponderá a la Superintendencia de Industria y Comercio determinar que en el tratamiento el Responsable o el Encargado han incurrido en conductas contrarias al ordenamiento.

En la recolección, Tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución” (Subrayado fuera del texto original).

La Corte Constitucional ha tenido la oportunidad de definir el derecho al habeas data o autodeterminación informativa de la siguiente manera:

“[e]l derecho fundamental al habeas data, es aquel que otorga la facultad al Titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales”⁶.

De igual manera, en Sentencia T-987 de 2012, la Sala Novena de Revisión de la Corte Constitucional agregó:

“la autorización será compatible con el derecho al hábeas data cuando la misma es idónea para garantizar las facultades de conocimiento, actualización y rectificación, al igual que la cláusula general de libertad. Esto significa que el sujeto concernido manifiesta su consentimiento de tratamiento del dato personal (i) para que sea consignado en una base o registro de datos particular e identificable; y (ii) para unas finalidades y usos que son expuestos y puestos a consideración del Titular del dato, como condición previa para el otorgamiento de la autorización. Este requisito, por ende, implica que son violatorias del derecho hábeas data aquellas formas de recopilación de información personal que sean secretas o que se fundamenten en desnaturalizar o falsear la voluntad del sujeto concernido para la incorporación del dato personal” (Subrayado fuera del texto original)⁷.

Así, se tiene entonces que el derecho al *habeas data* se concreta en la facultad del Titular de la información de decidir, **voluntariamente**, que la información sobre sí mismo sea sometida a Tratamiento por parte de terceros.

Por ello mismo es que en el literal c) del artículo 4 de la Ley 1581 de 2012 se señala que *“[e]l tratamiento sólo puede ejercerse con consentimiento, previo, expreso, 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 revele el consentimiento” (Subrayado fuera del texto original).*

En desarrollo de tal principio, el literal b) del artículo 17 del mismo precepto normativo, establece como un deber de los Responsables del Tratamiento el de *“[s]olicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular”.*

No obstante lo anterior, hay casos en los cuales el Responsable puede recolectar información sin que se requiera el consentimiento de su Titular, entre otros, cuando realiza el Tratamiento sobre datos de naturaleza pública⁸.

En este orden de ideas, se debe determinar en primer lugar si el uso de una dirección de correo electrónico requiere la autorización de su Titular, a la luz de la clasificación de los datos personales elaborada por la jurisprudencia y recogida en la Ley 1266 de 2008⁹; entonces, según el artículo 3 de la citada ley, los datos personales se clasifican de la siguiente forma:

“(…)

e) DATO PERSONAL. *Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados;*

⁶ Cfr. Corte Constitucional, Sentencia T-729 de 2002. M.P. Eduardo Montealegre Lynett.

⁷ Cfr. Corte Constitucional, Sentencia T-987 de 2012. M.P. Luis Ernesto Vargas Silva.

⁸ Cfr. Ley 1581 de 2012, literal b), artículo 10. “Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trata de: (...) b) Datos de naturaleza pública. (...)”.

⁹ “Por la cual se dictan 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”.

f) DATO PÚBLICO. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;

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

h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular.

(...):

Por su parte, en la Sentencia C-1011 de 2008, la Corte Constitucional declaró la norma exequible en el siguiente entendido:

"[e]l dato público, en los términos de la norma estatutaria, corresponde a aquellos que sean calificados de esa manera por la Constitución y la ley, al igual que todos los que no estén incluidos en las categorías de datos semiprivados y privados. El legislador prevé dentro de la categoría en comento a los documentos públicos, las sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva y los relativos al estado civil de las personas".

Los datos semiprivados corresponden a aquellos que no tienen naturaleza íntima, reservada, ni pública y que, por ende, su conocimiento puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general. Ejemplo de esta categoría es el dato financiero y crediticio de actividad comercial o de servicios, el que, como se ha indicado insistentemente en esta decisión, es el objeto de regulación del Proyecto de Ley. Por último, el dato privado es aquel que por su naturaleza íntima o reservada sólo es relevante para el Titular"¹⁰.

La anterior clasificación fue retomada de manera íntegra por el Alto Tribunal en la sentencia C-748 de 2011 al efectuar el estudio de constitucionalidad de la actual Ley 1581 de 2012. En la referida sentencia dijo esa Corporación lo siguiente:

*"la clasificación de los datos personales no es un elemento indispensable de la regulación y, dicho vacío en todo caso puede ser remediado acudiendo a la jurisprudencia constitucional y a otras definiciones legales, **especialmente al artículo 3 de la Ley 1266**, en virtud del principio de conservación del derecho, el literal c) será declarado exequible en este respecto" (Subrayado fuera de texto)¹¹.*

Claro lo anterior, es pertinente señalar que respecto a los correos electrónicos existen dos tipos de datos:

1. Los correos electrónicos se consideran datos públicos cuando (i) pertenecen a los servidores públicos en ejercicio de las funciones públicas asignadas, independientemente del servidor de correo que esté disponible (normalmente los correos institucionales de los funcionarios públicos corresponden a un servidor de correo propio de la entidad; por ejemplo, para esta Superintendencia "@sic.gov.co"; (ii) los correos corporativos que pertenecen a los empleados de una empresa para el cumplimiento del giro ordinario de los negocios¹².

¹⁰ Ídem.

¹¹ Cfr. Corte Constitucional, Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

¹² En efecto, el numeral 2 del artículo 2.2.2.25.1.3., Capítulo 25 del Decreto 1074 de 2015, señala lo siguiente: **"(d) definiciones.** Además de las definiciones establecidas en el artículo 3° de la Ley 1581 de 2012, para los efectos del presente decreto se entenderá por:

(...)

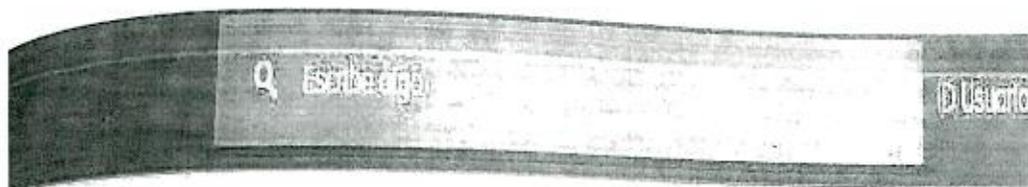
2. DATO PÚBLICO: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva".

2. Todos los demás correos de tipo personal se consideran datos semiprivados, dado que pueden interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como son los datos de contacto, entre otros.

En consecuencia, cuando un Responsable desee realizar cualquier tipo de Tratamiento sobre correos personales, deberá solicitar la autorización al Titular de la información, en cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1074 de 2015. Por lo anterior, se concluye que sin la autorización previa e informada del titular, los datos personales de carácter privado y semiprivado no podrán ser registrados, divulgados, ni tratados.

Ahora bien, retomando el caso particular se encuentra que dentro de la actuación administrativa adelantada por el Grupo de Trabajo de Hábeas Data de esta Dirección, se evidenció preliminarmente la sociedad **RAPPI S.A.S.** no contaba con la autorización previa, expresa e informada otorgada por el señor [REDACTED], pues dentro de los requerimientos efectuados en dicha actuación, la investigada no aportó los medios técnicos correspondientes que evidencien el consentimiento del titular.

Por su parte, la sociedad **RAPPI S.A.S.**, mediante escrito allegado el día 28 de septiembre de 2018, reiteró que todos los usuarios al momento de descargar la aplicación de Rappi, deben aceptar los términos y condiciones del servicio que regulan la plataforma así como el aviso de privacidad donde se indica dónde pueden acceder a las políticas de tratamiento de datos personales. Así mismo, aportó la hora y la fecha en la cual el señor [REDACTED] aceptó los términos y condiciones y copia de la impresión de pantalla del registro que guarda la investigada como evidencia del consentimiento del titular.



Varias conclusiones surgen de la imagen anterior y de las pruebas que reposan en el expediente:

En primer lugar, tanto el número telefónico como la dirección de correo electrónico del señor Varela [REDACTED] no son datos personales de naturaleza pública, razón por la cual **RAPPI S.A.S.** debió obtener la autorización previa, expresa e informada que requiere la regulación colombiana para poder recolectar y usar dicha información.

En segundo lugar, una vez analizadas las pruebas aportada por la sociedad investigada, se encuentra que dentro de los registros que conserva la compañía solo indican la fecha de creación del usuario, sin que se evidencie que el titular haya realizado la validación del "check" en la casilla para aceptar los términos y condiciones dispuestos por la plataforma, si bien la sociedad **RAPPI S.A.S.** puede determinar la fecha en la que el usuario descargo e instalo su aplicación Web, esta no puede demostrar que el titular otorgó su consentimiento.

Ahora bien, los términos y condiciones no deben confundirse con la autorización previa, expresa e informada que exige la ley. Aunque no son excluyentes, los primeros no necesariamente cumplen los requisitos legales de la autorización, la cual le corresponde probar al Responsable del Tratamiento tal y como se deriva del literal b) del artículo 17 de la ley 1581 de 2012.

En tercer lugar, tampoco existe prueba de que **RAPPI S.A.S.** informó oportunamente lo que ordena el artículo 12¹³ de la ley 1581 de 2012.

En cuarto lugar, **RAPPI S.A.S.** no acredita que fue [REDACTED], y no otra persona, quien suministro los datos mencionados. Lo anterior, pone en evidencia la carencia de un proceso o método para establecer la identidad plena de los titulares de los datos que supuestamente autorizan el tratamiento de los mismos. Nótese que en la página web de **RAPPI S.A.S.** se establece lo siguiente:

"Todos los visitantes de las Plataformas de RAPPI S.A.S deben registrarse y autorizar el tratamiento de los datos personales para poder hacer uso de los servicios ofrecidos. Por tanto, en cada uno de los sistemas se encuentra una casilla que dice "Política de privacidad y Tratamiento de Datos Personales" la cual debe ser leída y aceptada para poder continuar con el uso de los servicios de RAPPI S.A.S "

De lo anterior se deduce que no es claro cómo **RAPPI S.A.S.** establece la identidad de cada uno de los visitantes. En otras palabras, surge la siguiente pregunta: ¿de qué manera **RAPPI S.A.S.** puede establecer que un visitante es efectivamente [REDACTED] y no otra persona?. Esto es fundamental para tener certeza de la plena individualización e identificación de cada uno de los titulares de los datos y evitar, entre otras, eventuales suplantaciones de identidad.

Lo anterior no es menor si se tiene en cuenta lo que establece el decreto 1074 de 2015 en los siguientes términos:

"Artículo 2.2.2.25.2.2. Autorización. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento."

Recuérdese que el titular del dato es la "persona natural cuyos datos personales sean objeto de Tratamiento"¹⁴. Por lo tanto para obtener la autorización es necesario establecer previamente la identidad de la persona natural cuyos datos serán recolectados y usados con miras a obtener su consentimiento para dicho efecto.

Finalmente, la imagen anterior no es prueba, por sí sola, de que [REDACTED] haya autorizado el tratamiento de sus datos a [REDACTED]. La misma solo contiene unos datos (número, dirección de correo electrónico, fecha, nombre y teléfono) pero no prueba el consentimiento previo, expreso e informado de esa persona para llevar a cabo el Tratamiento de sus datos personales.

Ahora bien, la regulación permite diferentes medios para probar la autorización. En ese sentido, establece lo que sigue a continuación el decreto 1074 de 2015:

¹³ Este artículo de la ley 1581 de 2012 ordena lo siguiente: "ARTÍCULO 12. DEBER DE INFORMAR AL TITULAR. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

- El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
- Los derechos que le asisten como Titular;
- La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

PARÁGRAFO. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta."

¹⁴ Cfr. Literal f) del artículo 3 de la Ley 1581 de 2012.

"Artículo 2.2.2.25.2.4. Modo de obtener la autorización. Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 2.2.2.25.4.1., del presente Decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada.

Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

(Decreto 1377 de 2013, art. 7)"

Como quiera que en el presente caso no se acreditó autorización escrita u oral, a continuación, se establecerá si existe consentimiento del titular del dato mediante conductas inequívocas:

Para el efecto, este Despacho deberá considerar si se puede predicar una conducta inequívoca del titular al descargar e instalar la aplicación de Rappi o con el mero hecho de registrarse en cualquiera de las "Plataformas de [REDACTED]". Se deberá tener en cuenta que, no solo estas conductas inequívocas deben traer consigo la voluntad de la persona, toda vez que la norma indica que dicha conducta debe concluir de forma razonable que el titular otorgó la autorización, es decir, que dicha autorización debe cumplir con los requisitos impuesto por la Ley 1581 de 2012, que al tenor de su artículo 9 establece que "(...) 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**", Por ende aunque el consentimiento puede ser obtenido través de medios electrónicos en los términos previstos por la ley 527 de 1999, no debe perderse de vista que las conductas inequívocas deben cumplir todos los requisitos que exige la ley 1581 de 2012 y sus decretos reglamentarios, esto es, que de ellas se concluya razonablemente que existe un consentimiento previo, expreso e informado.

Sin embargo, en el caso que nos ocupa, no puede deducirse que los titulares, aunque de forma voluntaria entreguen sus datos personales, hayan sido informados de todo lo que ordena el artículo 12 de la ley 1581 de 2012, pues como bien se señaló líneas atrás, no existe prueba de que, en este caso, [REDACTED] haya no sólo aceptado los términos y condiciones dispuestos por el Responsable sino que haya otorgado su autorización a **RAPPI S.A.S.** para que pudiese tratar sus datos, puesto que la investigada no aportó evidencia alguna de lo anterior.

Así las cosas, no es de recibo para este Despacho, que del mero registro de una fecha de suscripción se infiera la obtención de una autorización de una persona específica, porque como ya se mencionó, el Responsable debe demostrar por un medio idóneo que obtuvo la autorización previa, expresa e informada de [REDACTED].

De esta manera, este Despacho encuentra que la sociedad **RAPPI S.A.S.**, no conservó en las condiciones previstas en la Ley 1581 de 2012, copia de la respectiva autorización otorgada por el Titular, motivo por el cual se impondrá la sanción correspondiente y se emitirán órdenes pertinentes para que dicha sociedad garantice el derecho de *habeas data* de los titulares.

DÉCIMO: Imposición y graduación de la sanción

10.1 Facultad sancionatoria

La Ley 1581 de 2012 le confirió a la Superintendencia de Industria y Comercio una potestad sancionatoria que se concreta en el artículo 23 de la Ley 1581 de 2012, estableciendo algunos criterios de graduación que se encuentran señalados en el artículo 24 ibídem, por lo tanto, atendiendo dichos criterios, este Despacho entrará a determinar cuáles deberá tener en cuenta el caso concreto, así:

10.1.1 La dimensión del daño o peligro a los intereses jurídicos tutelados por la ley

De la lectura de la norma citada, resulta claro que para que haya lugar a la imposición de una sanción por parte de este Despacho, basta que la conducta desplegada por la investigada haya puesto en peligro los intereses jurídicos tutelados por la Ley 1581 de 2012.

Respecto a las sanciones que se imponen por la infracción al Régimen de Protección de Datos, debe precisarse que conforme al principio de proporcionalidad que orienta el derecho administrativo sancionador, la autoridad administrativa debe ejercer su potestad sancionatoria en forma razonable y proporcionada, de modo que logre el equilibrio entre la sanción y la finalidad de la norma que establezca, así como la proporcionalidad entre el hecho constitutivo de la infracción y la sanción aplicada. Sobre la aplicación de este principio, la Corte Constitucional ha señalado:

"En cuanto al principio de proporcionalidad en materia sancionatoria administrativa, éste exige que tanto la falta descrita como la sanción correspondiente a las mismas que resulten adecuadas a los fines de la norma, esto es, a la realización de los principios que gobiernan la función pública. Respecto de la sanción administrativa, la proporcionalidad implica también que ella no resulte excesiva en rigidez frente a la gravedad de la conducta, ni tampoco carente de importancia frente a esa misma gravedad"¹⁵

De esta forma, para la correcta adecuación de los hechos y la sanción aplicable, el operador jurídico en materia de protección de datos personales, debe en primera medida, analizar la dimensión del daño o peligro a los intereses jurídicos tutelados, así como el posible beneficio económico, para luego analizar otras circunstancias concurrentes de graduación, tales como la capacidad económica del investigado, la reiteración de la infracción, colaboración del investigado para esclarecer los hechos investigados¹⁶.

También se tendrán en cuenta para la dosificación de la sanción, el tamaño de la empresa, sus ingresos operacionales, patrimonio y, en general, su información financiera, de tal forma que la sanción resulte disuasoria más no confiscatoria. Así como, la conducta de la investigada durante el trámite de la investigación administrativa.

En el caso sub-examine, quedó demostrado que no sólo se puso en peligro sino que se quebrantaron los intereses jurídicos tutelados por la ley 1581 de 2012, toda vez que, es claro que la sociedad investigada vulneró el derecho de *habeas data* del reclamante, pues no atendió efectivamente la solicitud de supresión de datos personales, ni probó haber obtenido la autorización para poder recolectar y usar los datos de [REDACTED].

En virtud de lo anterior, este Despacho impondrá una multa equivalente a TRESCIENTOS SESENTA (360) salarios mínimos legales mensuales vigentes por el incumplimiento de lo dispuesto en: (i) el literal a) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal e) del artículo 8 de la norma en mención, junto con el artículo 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015 y (ii) el literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y artículo 9 de la norma en mención; y inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.

10.1.2 Otros criterios de graduación

Se aclara que los criterios de graduación de la sanción señalados en los literales b), c), d) y e) del artículo 24 de la Ley 1581 de 2012 no serán tenidos en cuenta debido a que dentro de la

¹⁵ Corte Constitucional, Sala Plena, Sentencia C-125 del 18 de febrero de 2003, Exp. Rad. D-4059, Magistrado Ponente Dr. Marco Gerardo Monroy Cabra.

¹⁶ Ley 1581 de 2012 "Artículo 23. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones: a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó; b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar; c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio; d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles; Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva."

investigación realizada no se encontró que la investigada hubiera obtenido beneficio económico alguno por la comisión de la infracción, no hay reincidencia en la comisión de la infracción, no hubo resistencia u obstrucción a la acción investigativa de la Superintendencia y tampoco hubo renuencia o desacato a cumplir las órdenes e instrucciones del Despacho.

El criterio de atenuación señalado en el literal f) del artículo citado no se aplica toda vez que la investigada no reconoció o aceptó la comisión de las infracciones.

DÉCIMO PRIMERO: En este orden de ideas, una vez analizadas las pruebas obrantes en el expediente y en virtud del literal e) del artículo 21 de la Ley 1581 de 2012, mediante el cual se le asigna, entre otras funciones, esta Superintendencia el "(i)mpartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disipaciones previstas en la presente Ley", esta Instancia procederá a impartir la siguientes órdenes a cargo de **RAPPI S.A.S.**

En el término de tres (3) meses contados a partir de la ejecutoria de la presente decisión y en virtud de los artículos 2.2.2.25.6.1. (*Demostración*) y 2.2.2.25.6.2. (*Políticas internas efectivas*) adoptar medidas efectivas, apropiadas y verificables para:

- (a) Abstenerse de enviar mensajes de texto, correos electrónicos, realizar llamadas telefónicas o comunicarse por cualquier medio con los titulares de los datos respecto de los cuales no tenga plena prueba de la autorización, previa, expresa e informada para dicho efecto.
- (b) Establecer la identidad plena de los visitantes de su página web o usuarios de sus plataformas cuyos datos son recolectados, usado o tratados por **RAPPI S.A.S.**
- (c) Suprimir de manera definitiva y oportuna los datos personales de los titulares cuya información es recolectada, usada o tratada por **RAPPI S.A.S.**, una vez cualquier titular del dato le solicite por cualquier medio la eliminación de sus datos o revoque la autorización del tratamiento de sus datos personales frente a todos los servicios ofrecidos por la plataforma digital de la aplicación Rappi, o para servicios específicos que no desea seguir recibiendo.
- (d) Conservar prueba de la autorización previa, expresa e informada otorgada por cada uno de los titulares de los datos.
- (e) Poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada. Estos deben implementarse a través de los mismos medios o canales mediante los cuales **RAPPI S.A.S.** se contacta o comunica con los titulares de los datos

Adicionalmente la investigada deberá implementar un mecanismo de monitoreo permanente respecto de la efectividad de las medidas adoptadas para dar cumplimiento a las anteriores órdenes.

Para demostrar lo anterior, **RAPPI S.A.S.** deberá:

Primero: Acreditar ante esta entidad y dentro del término de tres (2) meses contados a partir de la ejecutoria de la presente decisión una certificación de cumplimiento de las órdenes impartidas por esta entidad. Dicha certificación debe ser emitida por una persona jurídica nacional o extranjera la cual debe ser un tercero imparcial y especializado en los temas que involucra la implementación de cada orden.

Segundo: Realizar una auditoria externa enfocada en la verificación de la aplicación de las medidas efectivas y apropiadas para cumplir todo lo ordenado por esta entidad. Los resultados de la auditoría deben ser remitidos a la Superintendencia de Industria y Comercio, en el término de tres meses siguientes al cumplimiento oportuno de las órdenes anteriormente descritas.

De igual manera es necesario indicar que el incumplimiento a las órdenes aquí impartidas, darán lugar al inicio de una investigación administrativa de carácter sancionatorio, la cual faculta a esta

superintendencia a (i) imponer multas hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes; (ii) Suspensión de las actividades relacionadas con el Tratamiento; y (iii) Cierre temporal de las operaciones relacionadas con el Tratamiento.

En mérito de lo expuesto este Despacho,

RESUELVE

ARTÍCULO PRIMERO: Imponer una sanción pecuniaria a la sociedad **RAPPI S.A.S.**, identificada con el Nit. 900.843.898-9, de **DOSCIENTOS NOVENTA Y OCHO MILLONES CIENTO VEINTIÚN MIL SETECIENTOS SESENTA PESOS M/cte.** (\$298.121.760.00), equivalente a **TRESCIENTOS SESENTA (360)** salarios mínimos legales mensuales vigentes, por el incumplimiento de lo dispuesto en : (i) el literal a) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal e) del artículo 8 de la norma en mención, junto con el artículo 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015, y (ii) el literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y artículo 9 de la norma en mención; y inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.

PARÁGRAFO: El valor de la sanción pecuniaria que por esta resolución se impone, deberá consignarse en efectivo o cheque de gerencia en el Banco Popular, Cuenta No. 050000249, a nombre de Dirección del Tesoro Nacional – Fondos Comunes, Código Rentístico No. 350300, Nit. 899999090-2. En el recibo deberá indicarse el número del expediente y el número de la presente resolución. El pago deberá acreditarse ante la pagaduría de esta Superintendencia, con el original de la consignación, dentro de los cinco (5) días hábiles siguientes a la ejecutoria de esta resolución.

ARTÍCULO SEGUNDO: Ordenar a la sociedad **RAPPI S.A.S.**, identificada con el Nit. 900.843.898-9, lo siguiente:

En el término de tres (3) meses contados a partir de la ejecutoria de la presente decisión y en virtud de los artículos 2.2.2.25.6.1. (*Demostración*) y 2.2.2.25.6.2. (*Políticas internas efectivas*) adoptar medidas efectivas, apropiadas y verificables para:

- (a) Abstenerse de enviar mensajes de texto, correos electrónicos, realizar llamadas telefónicas o comunicarse por cualquier medio con los titulares de los datos respecto de los cuales no tenga plena prueba de la autorización, previa, expresa e informada para dicho efecto.
- (b) Establecer la identidad plena de los visitantes de su página web o usuarios de sus plataformas cuyos datos son recolectados, usado o tratados por **RAPPI S.A.S.**
- (c) Suprimir de manera definitiva y oportuna los datos personales de los titulares cuya información es recolectada, usada o tratada por **RAPPI S.A.S.**, una vez cualquier titular del dato le solicite por cualquier medio la eliminación de sus datos o revoque la autorización del tratamiento de sus datos personales frente a todos los servicios ofrecidos por la plataforma digital de la aplicación Rappi, o para servicios específicos que no desea seguir recibiendo.
- (d) Conservar prueba de la autorización previa, expresa e informada otorgada por cada uno de los titulares de los datos.
- (e) Poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada. Éstos deben implementarse a través de los mismos medios o canales mediante los cuales **RAPPI S.A.S.** se contacta o comunica con los titulares de los datos

Adicionalmente la investigada deberá implementar un mecanismo de monitoreo permanente respecto de la efectividad de las medidas adoptadas para dar cumplimiento a las anteriores ordenes.

PARÁGRAFO: Para demostrar lo anterior, **RAPPI S.A.S.** deberá:

Primero: Primero: Acreditar ante esta entidad y dentro del término de tres (2) meses contados a partir de la ejecutoria de la presente decisión una certificación de cumplimiento de las órdenes impartidas por esta entidad. Dicha certificación debe ser emitida por una persona jurídica nacional o extranjera la cual debe ser un tercero imparcial y especializado en los temas que involucra la implementación de cada orden.

Segundo: Realizar una auditoria externa enfocada en la verificación de la aplicación de las medidas efectivas y apropiadas para cumplir todo lo ordenado por esta entidad. Los resultados de la auditoría deben ser remitidos a la Superintendencia de Industria y Comercio, en el término de tres meses siguientes al cumplimiento oportuno de las órdenes anteriormente descritas.

ARTICULO TERCERO: Notificar personalmente el contenido de la presente resolución a la sociedad **RAPPI S.A.S.**, identificada con el Nit. 900.843.898-9, a través de su representante legal y/o apoderado, entregándoles copia de la misma e informándoles que contra ella procede recurso de reposición ante el Director de Investigación de Protección de Datos personales y el de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los diez (10) días siguientes a la diligencia de notificación.

ARTÍCULO CUARTO: Comuníquese el contenido de la presente resolución al señor [REDACTED]

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D. C.,

25 ABR 2019

El Director de Investigación de Protección de Datos Personales,


CARLOS ENRIQUE SALAZAR MUÑOZ

Proyectó: AMCC
Revisó: CESN
Aprobó: CESM

NOTIFICACIÓN:

Entidad: **RAPPI S.A.S.**
Identificación: Nit. 900.843.898-9
Representante Legal: [REDACTED]
Identificación: [REDACTED]
Dirección: Carrera 93 N° 19-58
Ciudad: Bogotá D.C.
Correo electrónico: felipe@rappi.com

COMUNICACIÓN:

Reclamante:
[REDACTED]