REPUBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 64902 --- DE 2018

(04 SEP 2018)

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

VERSIÓN PÚBLICA

Radicación 16-90648

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 mediante escrito radicado el 6 de abril de 2016 por la señora [redacted] presentó denuncia en contra del **INSTITUTO DE DIAGNÓSTICO MÉDICO S.A- IDIME S.A.,** (en adelante **IDIME S.A.**) identificada con el Nit. 800.065.396-2 por los siguientes hechos:

1.1. Manifestó que en el mes de marzo de 2016 ingresó al sitio web de la investigada con el propósito de descargar los resultados de unos exámenes médicos que se había practicado, sin embargo, olvidó la contraseña con la cual se había registrado, por lo que eligió la opción *"recordar Contraseña"* para que a través del sistema le fuera enviado un correo automático con los datos asociados a la cédula digitada.

1.2. Señaló que recibió un correo electrónico en el cual se suministraban los datos de una persona distinta a ella.

SEGUNDO: Que con ocasión a la queja presentada por la referida Titular, esta Dirección llevó a cabo la preservación del sitio web: *"www.idime.com.co"* a través del Laboratorio de Informática Forense de esta Superintendencia, en aras de establecer si en desarrollo de los procesos de recolección y tratamiento información personal se observaban las disposiciones de la Ley 1581 de 2012, arrojando los siguientes resultados (Ver fls 11 al 20):

- *"En la denuncia nos indican que IDIME permite a través de su página web descargar resultados de exámenes médicos, así que por favor revisemos el modulo dispuesto para el efecto para ver si es posible encontrar brechas de seguridad que puedan provocar la filtración de datos personales relacionados con la salud de la personas `Para la realización de esta parte se hace necesario crear un usuario, registrado en el sistema y realizar el envió de correo o mensajes al sistema de la empresa IDIME, la directriz de la delegatura es no realizar este tipo de procedimientos por eso no es posible evidenciar este procedimiento sin realizar técnicas intrusivas, se sugiere realizar una visita administrativa al sitio.*

- *El denunciante indica que ingreso al módulo de `recordar contraseña 'y en cambio de recibir la descripción del procedimiento para cambiar de contraseña. Se le envió un correo automático con los datos de otra persona, así que este sería un punto que también podría verificarse para encontrar fallas en la seguridad de la información. Para la realización de esta parte se hace necesario crear un usuario, registrarlo en el sistema y realizar el envió de correo o mensaje al sistema de la empresa IDIME. La directriz de la delegatura es no realizar este tipo de procedimientos por eso no es posible evidenciar este procedimiento sin realizar técnicas intrusivas, se sugiere realizar una visita administrativa al sitio.*

- *La página web cuenta con políticas de tratamiento de información (privacidad y tratamiento de datos) Ver hallazgo y anexo 4.*

TERCERO: Que de la información recaudada en desarrollo de la etapa de averiguación preliminar y del análisis de la misma, la Dirección de Investigación de Protección de Datos Personales mediante Resolución No. [redacted] del 23 de abril de 2018[1], resolvió iniciar investigación administrativa en contra de la sociedad **IDIME S.A.,** por la presunta vulneración al deber que el investigado ostenta en su calidad de Responsable de la información contemplado en: (i) el literal b) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal c) del artículo 4 y el artículo 9 de la misma norma asi como los artículos 2.2.2.25.2.2 y 2.2.2.25.2.5 del Decreto Único Reglamentario 1074 de 2015; (ii) el literal d) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales f) y g) del artículo 4 de la misma norma y (iii) el literal k) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la misma norma y el artículo 2.2.2.25.6.1 del Decreto único Reglamentario 1074 de 2015, otorgándosele un término de quince (15) días al investigado para que rindiera los respectivos descargos y aporta las pruebas que pretendía hacer valer dentro la presente actuación administrativa.

El anterior acto administrativo fue debidamente notificado a la investigada el 25 de abril de 2018 de forma personal conforme la certificación de acuse de recibo, certificado que obra a folio 26 del expediente.

CUARTO: Que de conformidad con la certificación expedida por la Coordinadora del Grupo de Notificaciones y Certificaciones[2] y la constancia de notificación de la secretaria general AD-HOC[3], la Resolución No. [redacted] del 23 de abril de 2018 le fue notificada personalmente a la sociedad **IDIME S.A.,** el día 25 de abril de 2018 y que una vez vencido el término para presentar descargos la investigada guardó silencio.

QUINTO: Que mediante oficio [redacted] enviado por este Despacho a la sociedad **IDIME S.A.,** se requirió aportara información referente a la queja presentada por la señora [redacted]

SEXTO: Que mediante comunicación del 8 de junio de 2017 la sociedad **IDIME S.A.,** allegó respuesta al requerimiento efectuado por este Despacho (fls.6 al 10) señalando lo siguiente:

6.1 Que realizaron una revisión de la operación de la plataforma tecnológica realizando *"paso a paso"* que realizó la reclamante sin encontrar falla alguna.

6.2 Que *"como plan de mejora adoptado por nuestra institución para la prevención de los presuntos hechos aducidos por la Usuaria, se ha dispuesto efectuar un cambio en proceso establecido para el mecanismo de 'recordación de la contraseña' disponible en nuestro portal web que consiste el procedimiento en cuestión y aporte copia de la política de tratamiento de datos"* (fl.6 anverso).

6.3 Que dentro de la Política de Tratamiento de Datos personales implementada se incluyó la facultad para supresión de datos personales de los titulares de la entidad.

SÉPTIMO: Que mediante la Resolución No. [redacted] del 19 de junio de 2018 este Despacho incorporó las pruebas dentro de la presente actuación, declaró agotada la etapa probatoria dentro de la presente investigación administrativa y corrió traslado a la investigada para que presentara alegatos de conclusión.

Que de conformidad con la certificación expedida por la Coordinadora del Grupo de Notificaciones y Certificaciones y la constancia de notificación de la secretaria general AD-HOC, la Resolución No. [redacted] del 19 de junio de 2018 le fue notificada por aviso a la sociedad **IDIME S.A.,** el día 20 de junio de 2018 y que una vez vencido el término para presentar descargos la investigada guardó silencio.

---

[1] Obrante a folios 27 al 30.
[2] Obrante a folio 26
[3] Obrante a folio 21

Conforme a lo anterior se aclara que previo a efectuar la notificación por aviso, se surtió la notificación personal al correo electrónico contabilidad@idime.com.co la cual no resultó efectiva.

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 2011[4], 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 la preservación del sitio web: *"www.idime.com.co"* 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 a los literales b), c) y d) del artículo 17 de la Ley 1581 de 2012.

En ese orden de ideas, corresponde a este Despacho establecer si la conducta desplegada por la investigada dará lugar o no a la imposición de una sanción para lo cual se deberán tener en cuenta los hechos narrados por los reclamantes, así como las razones de hecho y de derecho aducidas por la investigada en los escritos de descargos y alegatos de conclusión, y el conjunto de pruebas allegadas al expediente.

9.2 Valoración probatoria y conclusiones

9.2.1. <u>Concepto de Responsable del tratamiento de datos personales</u>

Esta Dirección considera oportuno distinguir los conceptos de Responsable y Encargado del tratamiento, comoquiera que los mismos resultan relevantes para determinar las condiciones en que se entrega la información a un tercero. El literal e) del artículo 3 de la Ley 1581 de 2012, define al Responsable del tratamiento de la siguiente manera:

> *"**Artículo 3°. Definiciones**. Para los efectos de la presente ley, se entiende por:*
> *(...)*
> ***e) Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;*
> *(...)".*

Esta norma fue declarada exequible mediante Sentencia C-748 de 2011 en el siguiente entendido:

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

"(...) el concepto 'decidir sobre el tratamiento' empleado por el literal e) parece coincidir con la posibilidad de definir –jurídica y materialmente- los fines y medios del tratamiento".

Esto significa que es Responsable del tratamiento la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, determine - **de hecho o de derecho** - los fines del tratamiento y los medios para alcanzarlos.

9.2.2 <u>Del deber de solicitar la respectiva autorización otorgada por el titular.</u>

El artículo 15 de la Constitución Política establece que las personas, en desarrollo de sus derechos a la autodeterminación informática y el principio de libertad, son quienes de forma expresa deben autorizar que la información que sobre ellos sea recaudada pueda ser incluida en una base datos.

Al respecto la Corte Constitucional ha señalado lo siguiente:

*"**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.*

*Este principio, **pilar fundamental de la administración de datos**, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente.*

El literal c) del Proyecto de Ley Estatutaria no sólo desarrolla el objeto fundamental de la protección del habeas data, sino que se encuentra en íntima relación con otros derechos fundamentales como el de intimidad y el libre desarrollo de la personalidad. En efecto, el ser humano goza de la garantía de determinar qué datos quiere sean conocidos y tiene el derecho a determinar lo que podría denominarse su 'imagen informática'[5].

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.

Al respecto la Corte Constitucional 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 rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien por que se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa."

De esta manera, 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 los Responsables y Encargados de la información deben implementar mecanismos que le permita al Titular acceder en cualquier momento a su información.

Igualmente, es importante indicar que en virtud del principio de libertad, citado líneas atrás, el legislador impuso a los Responsables del Tratamiento de datos personales la exigencia de requerir la autorización previa, expresa e informada del Titular, consagrada en el artículo 9 de la Ley 1581

[5] Ver en: Corte Constitucional Sentencia C-748 del 6 de octubre de 2011 MP. Jorge Ignacio Pretelt Chaljub.

de 2012[6] y, además, el deber de solicitar y conservar copia de la autorización de Tratamiento otorgada por el mismo, dispuesto en el literal b) del artículo 17 del mismo compendio normativo[7].

De lo anterior, vale la pena precisar que la jurisprudencia constitucional, en sentencia mencionada líneas atrás, se refiere a las características de los datos personales al analizar la constitucionalidad del proyecto de ley de protección de datos personales, a saber: *"i) Estar referidos a aspectos exclusivos y propios de una persona natural; ii) Permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otro datos; iii) Su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera licita o ilícita; iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación"*, características que se adicionan al concepto de dato personal establecido en la Ley, consistente en un derecho de propiedad sobre éste, que se radica en cabeza del titular.

Sumado a lo anterior, el mismo Responsable debe conservar una copia de la autorización otorgada por el Titular de la información de forma tal que, en el momento en que sea solicitada para consulta, cuente con la misma.

Ahora bien, en el caso específico, esta Dirección a través de oficio N. [redacted] enviado el 24 de mayo de 2017 a la sociedad **IDIME S.A.**, a través del cual solicitó informara si contaba con la autorización previa, expresa e informada de la señora [redacted] y a través de la Resolución No. [redacted] del 23 de abril de 2018 se formularon cargos por este deber sin que la investigada se pronunciara al respecto y según las pruebas recaudadas por esta Dirección (fls.11 al 20), se pudo evidenciar que la investigada realizó tratamiento de los datos personales recolectados de datos tales como los nombres, apellidos, cédula, teléfono y correo.

De lo anterior se tiene que la investigada realiza recolección y tratamiento de datos personales, sin que demostrara que adelanta procedimiento alguno para la obtención las autorizaciones previas, expresas e informadas, para el tratamiento de datos personales en los términos señalados en la Ley.

Igualmente, debe aclarar este Despacho que la investigada, no demostró que se contaba con la autorización previa, expresa e **informada** de la reclamante en los términos señalados por el artículo 9 de la Ley 1581 de 2 2012, el cual indica lo siguiente:

> *"**Artículo 9°. Autorización del Titular.** Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior."*

En consecuencia de lo anterior, tampoco fue demostrado que se contara con la autorización para realizar el tratamiento de datos en los términos del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario de 2015 que señala lo siguiente:

> ***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"*

En conclusión se tiene que (i) La investigada recolectó y trató información personal privada ~~la titular~~, sin contar con la autorización previa, expresa e informada de la señora [redacted] y ~~como~~ como consecuencia de lo anterior, esta Dirección encuentra que la sociedad investigada incumplió con el deber establecido en el literal b) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal c) del artículo 4, y el artículo 9 de la misma norma, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015, razón por la cual se impondrá la correspondiente sanción

---

[6] **Ley 1581 de 2012. "*Artículo 9. Autorización del Titular.*** *Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior".*

[7] **Ley 1581 de 2012. "*Artículo 17. Deberes de los Responsables del Tratamiento.*** *Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: (...) b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular; (...)".*

9.2.3. <u>Deber de conservar la información bajo las condiciones de seguridad necesarias.</u>

El artículo 15 de la Constitución Política debe interpretarse de manera armónica con los principios de circulación restringida y de seguridad, de tal manera que se debe tener presente que los responsables del tratamiento deben garantizar, entre otras cosas, que la información personal no sea divulgada a través de correo electrónico a otros titulares. Ahora bien, aun existiendo el consentimiento de éste, la divulgación, circulación y acceso de los datos tiene que estar controlado y restringido frente a terceros no autorizados, razón por la cual la ley ha impuesto a los responsables del tratamiento una serie de deberes encaminados a dicho fin, como lo es el de *"conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración pérdida consulta, uso o acceso no autorizado o fraudulento".*

Precisamente el artículo 4 de la Ley 1581 de 2012 establece los principios para el Tratamiento de los datos personales, entre los cuales se encuentran el principio de acceso y circulación restringida y el de seguridad que señalan lo siguiente:

> *"(...)*
> ***f) Principio de acceso y circulación restringida:*** *El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;*
> *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;*
>
> *g)* ***Principio de seguridad:*** *La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*
> *(...)".*

Como se advierte, tanto el principio de acceso y circulación restringida como el de seguridad deben ser cumplidos por los Responsables y Encargados de información para garantizar el derecho de habeas data de los titulares, pues de la adopción de medidas de conservación de la información y de los controles de seguridad implementados depende que se minimicen los riesgos de filtración de los datos personales.

En el caso específico, fue posible determinar a través de la queja presentada por la reclamante, que la investigada realizó el envío de un correo electrónico con datos personales de un tercero al solicitar recordar su contraseña, dicho correo contenía nombre, cédula, correo y teléfono tal como se desprende de la afirmación efectuada por la denunciante y la prueba documental que obran a folios 2 y 3.

En éste punto, vale la pena volver a traer a colación el Principio de Seguridad de la Información establecido en el literal g) del artículo la ley 1581 de 2012 que impone a los Responsables y Encargados de Tratamiento de Datos Personales el deber de implementar la medidas técnicas, **humanas y administrativas** necesarias para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, lo que procede es establecer si obra en el expediente alguna prueba que demuestre que, con antelación a la divulgación masiva e indiscriminada de información personales de una titular, la investigada había documentado e implementado las medidas, técnicas humanas y administrativas necesarias para evitar que sucediera una situación como la que en este caso ocurrió. Más aún, resulta relevante establecer si tales medidas fueron conocidas y aceptadas por los empleados de la sociedad investigada.

La sociedad **IDIME S.A.,** en comunicación del 8 de junio de 2017 manifestó a este Despacho que *"como plan de mejora adoptado por nuestra institución para la prevención de los presuntos hechos aducidos por la Usuaria, se ha dispuesto efectuar un cambio en proceso establecido para el mecanismo de 'recordación de la contraseña' disponible en nuestro portal web que consiste el procedimiento en cuestión y aporte copia de la política de tratamiento de datos"* (fl.6 anverso).

Ahora bien, se encuentra demostrado que la Responsable expuso información privada de una titular de información a un tercero, lo que se traduce en que para la fecha de ocurrencia de los hechos la entidad no había implementado las medidas apropiadas y efectivas para impedir el acceso no autorizado a información personal semi pivada y el plan de mejora que informan haber adoptado se adelantó con posterioridad a la exposición de la información.

Como consecuencia de lo anterior, esta Dirección encuentra que la sociedad investigada incumplió con el deber establecido en el d) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales f), g) del artículo 4 de la misma norma, razón por la cual se impondrá la correspondiente sanción y se impartirá una orden encaminada a implementar las medida apropiadas y efectivas, para cumplir las obligaciones establecidas en la Ley 1581 de 2012.

9.2.4 Respecto al deber de -adoptar un manual interno de políticas y procedimientos.

Conforme al principio de legalidad en materia de datos personales, cualquier forma de Tratamiento de información personal desde su recolección hasta su disposición final se encuentra orientada por las normas contenidas no solamente en la Ley 1581 de 2012 sino también en la normatividad que sobre la materia se ha expedido, la cual, para el caso en particular, corresponde al Decreto Único Reglamentario 1074 de 2015[8]; lo que traduce en el hecho de que las disposiciones del referido decreto tienen la misma obligatoriedad y carácter vinculante que la ley estatutaria.

Es deber de los responsables *adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos*, contemplado en el literal k) del artículo 17 de la Ley 1581 de 2012, toda vez que las políticas de tratamiento de la información hacen parte del manual interno de políticas y procedimientos adoptado por los Responsables y Encargados del Tratamiento, ya que por medio de este se le informa a los Titulares cuáles son sus derechos, quien es el Responsable de la información y el fin para el cual van a ser tratados sus datos.

De otra parte el artículo 2.2.2.25.6.1 del Decreto Único Reglamentario 1074 de 2015, se establece el contenido mínimo que debe una política de tratamiento de la información, el cual indica lo siguiente:

> *"**ARTÍCULO 2.2.2.25.6.1. 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 capítulo, 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. (**Decreto 1377 de 2013, artículo 26).**"*

Así las cosas, en el caso particular, se tiene que a pesar de que a la sociedad **IDIME S.A.**, se le requirió para que informara cuales eran sus políticas de seguridad y confidencialidad

[8] 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.

implementadas, la investigada no respondió y guardo silenció en el término establecido para presentar descargos por lo que se considera que la entidad no ha implementado el manual interno de políticas y procedimientos, de igual forma no se evidenció por parte de este Despacho que se adoptara una política de seguridad de la información documentada, situación, a partir de la cual este Despacho considera que la sociedad IDIME S.A., no contaba ni cuenta con las medidas de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Como consecuencia de lo anterior, esta Dirección encuentra que la sociedad investigada incumplió con el deber establecido en el k) del artículo 17 de la Ley 1581 de 2012 en concordancia con el artículo 2.2.2.25.6.1 del Decreto único Reglamentario 1074 de 2015, razón por la cual se impondrá la correspondiente sanción e impartirá la orden correspondiente a fin de que la investigada, documente e implemente el manual interno de políticas y procedimientos para la recolección, almacenamiento, uso, circulación y supresión de información y la atención de quejas y reclamos.

DECIMO: 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 en el caso concreto, así:

10.1.1 *Imposición y graduación de la sanción*

Respecto de 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 sancionatorio, 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 que la norma establece, 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 el principio de proporcionalidad en materia sancionatoria administrativa, éste (sic) exige que tanto la falta descrita como la sanción correspondiente a la misma 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 que ella resulte excesiva en rigidez frente a la gravedad de la conducta, ni tampoco carente de importancia frente a esa misma gravedad*[9].
> *(...)"*

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, así como la colaboración del investigado para esclarecer los hechos materia de investigación[10].

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

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.

---

[9] Corte Constitucional. Sala Plena. Sentencia C-125 del 18 de febrero de 2003. Ex. Rad. D-4059 Magistrado Ponente Dr. Marco Gerardo Monroy Cabra.,
[10] Artículo 24 de la Ley 1581 de 2012.

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.

Para el caso que nos ocupa es claro que la sociedad investigada vulneró los deberes contemplados en (i) el literal b) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal c) del artículo 4 y el artículo 9 de la misma norma así como los artículos 2.2.2.25.2.2 y 2.2.2.25.2.5 del Decreto Único Reglamentario 1074 de 2015; (ii) el literal d) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales f) y g) del artículo 4 de la misma norma y (iii) el literal k) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la misma norma y el artículo 2.2.2.25.6.1 del Decreto único Reglamentario 1074 de 2015. Por lo indicado, esta Superintendencia impondrá por esta conducta como sanción, la suma de DOSCIENTOS (200) salarios mínimos legales mensuales vigentes y se impartirán las ordenes que correspondan.

10.1.2 *Otros criterios de graduación*

Por último 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 2008 no serán tenidos en cuenta debido a que (i) dentro de la investigación realizada no se encontró que la investigada hubiera obtenido beneficio económico alguno por la comisión de la infracción, (ii) no hubo reincidencia en la comisión de la infracción, (iii) no hubo resistencia u obstrucción a la acción investigativa de la Superintendencia y, (iv) no hubo renuencia o desacato a cumplir las órdenes e instrucciones del Despacho.

Por último se aclara que los criterios de graduación de la sanción señalados en los literales b), d), e) y f) del artículo 24 de la Ley 1581 de 2012 no serán tenidos en cuenta debido a que (i) dentro de la investigación realizada no se encontró que la investigada hubiera obtenido beneficio económico alguno por la comisión de la infracción, (ii) no hubo reincidencia en la comisión de la infracción, (iii) no hubo resistencia u obstrucción a la acción investigativa de la Superintendencia y, (iv) no hubo renuencia o desacato a cumplir las órdenes e instrucciones del Despacho.

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

UNDÉCIMO: Orden administrativa

En este orden de ideas, y una vez analizadas las pruebas obrantes en el expediente y en virtud del literal b) del artículo 21 de la Ley 1581 de 2012, mediante el cual se le asigna, entre otras funciones, a esta Superintendencia el *"(a)delantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. (...)"*, esta Instancia procederá a impartir la siguiente orden:

11.1 Demostrar que implementó las medidas apropiadas y efectivas para que la información de los titulares permanezca bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado.

11.3 Documentar e implementar el manual interno de políticas y procedimientos para la recolección, almacenamiento, uso, circulación y supresión de información y la atención de quejas y reclamos en especial para la atención de peticiones, consultas y reclamos de los titulares de información de acuerdo al deber establecido en el literal k) del artículo 17 de la Ley 1581 de 2012.

En mérito de lo expuesto este Despacho,

RESUELVE

ARTÍCULO PRIMERO: Imponer una sanción pecuniaria al **INSTITUTO DE DIAGNÓSTICO MÉDICO S.A- IDIME S.A.,** identificado con el Nit. 800.065.396-2, de **CIENTO CINCUENTA Y SEIS MILLONES DOSCIENTOS CUARENTA Y OCHO MIL CUATROCIENTOS PESOS** M/cte. ($156.248.400.oo), equivalente a DOSCIENTOS (200) salarios mínimos legales mensuales vigentes, por el incumplimiento de los deberes establecidos en (i) el literal b) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal c) del artículo 4 y el artículo 9 de la misma norma así como los

artículos 2.2.2.25.2.2 y 2.2.2.25.2.5 del Decreto Único Reglamentario 1074 de 2015; (ii) el literal d) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales f) y g) del artículo 4 de la misma norma y (iii) el literal k) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal g) del artículo 4 de la misma norma y el artículo 2.2.2.25.6.1 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. 05000024-9, 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 al **INSTITUTO DE DIAGNÓSTICO MÉDICO S.A- IDIME S.A.,** identificado con el Nit. 800.065.396-2, que (ii) demuestre que implementó las medidas apropiadas y efectivas para que la información de los titulares permanezca bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado y, (iii) un manual interno de políticas y procedimientos en especial para la atención de peticiones, consultas y reclamos de los titulares de información de acuerdo al deber establecido en el literal k) del artículo 17 de la Ley 1581 de 2012.

ARTÍCULO TERCERO: Notificar personalmente el contenido de la presente resolución al **INSTITUTO DE DIAGNÓSTICO MÉDICO S.A- IDIME S.A.,** identificado con el Nit. 800.065.396-2, a través de su apoderado o representante legal, 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: Comunicar a la señora [redacted] la presente decisión.

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D. C., 04 SEP 2018

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

Proyectó: JCRR
Aprobó: CESM

NOTIFICACIÓN:

Entidad: **INSTITUTO DE DIAGNÓSTICO MÉDICO S.A- IDIME S.A.**
Identificación: Nit. 800.065.396-2
Representante legal: **LIDA YAMILE GONZÁLEZ BOLÍVAR**
Identificación: C.C. No.52.173.813
Dirección: Calle 76 No. 13-46
Ciudad: Bogotá D.C.
Correo electrónico: contabilidad@idime.com.co

COMUNICACIÓN:

[redacted]