



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

RESOLUCIÓN NÚMERO 8 5 6 5 3 DE 2016

(13 DIC 2016)

"Por el cual se impone una sanción"

Radicación 15-184674

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 con ocasión a la queja presentada por la señora [REDACTED] en contra de la sociedad **CODENSA S.A. E.S.P.** (en adelante **CODENSA**), identificada con Nit. 830.037.248, 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 referida sociedad, por lo que de oficio, este Despacho decidió iniciar investigación administrativa con fundamento en los siguientes hechos:

- 1.1 Manifestó la señora [REDACTED] que el día 8 de agosto de 2015 el servicio de energía eléctrica presentó una falla en el sistema, por lo que a través de la red social Twitter decidió comunicarse con **CODENSA** por ser esta la empresa prestadora del referido servicio público y, así, reportar la falla y conocer cuándo se haría efectivo el restablecimiento del servicio.
- 1.2 Por su parte, **CODENSA** respondió dicha solicitud mediante un mensaje público en el servicio de microblogging **TWITTER**, en el que manifestaron que había una falla en el sector.
- 1.3 La denunciante una vez conoció la respuesta de **CODENSA** decidió responder el mensaje, manifestando su inconformidad, ya que ellos conocían donde se presentaba el daño, sin que ella suministrará esa información.
- 1.4 Posteriormente, dando respuesta al cuestionamiento de la señora [REDACTED] y nuevamente mediante el servicio de microblogging Twitter, la investigada publicó la dirección de domicilio en donde se había presentado la falla.
- 1.5 Por dichas razones, la señora [REDACTED] presentó una Reclamación ante **CODENSA** para que la información que allí se había publicado fuera eliminada, y posteriormente la Titular puso en conocimiento a esta Superintendencia de la presunta vulneración a la normas de protección de datos personales por parte de la sociedad investigada.

SEGUNDO: Que en vista de la denuncia presentada por la Titular, este Despacho dentro de las averiguaciones preliminares requirió a la sociedad **CODENSA**, con el fin de que informara entre otras cosas, si cuenta con la autorización previa, expresa e informada por parte de la señora [REDACTED] para compartir sus datos personales con terceros, a lo cual a investigada indicó que la información de la Titular solo es de "uso exclusivo para todo lo relacionado con la prestación del servicio público de energía" (fl.12).

TERCERO: Que mediante Resolución N° 24150 del 29 de abril de 2016¹ esta Dirección de Investigación de Protección de Datos Personales procedió a formular cargos de iniciar investigación administrativa en contra de la sociedad **CODENSA** por la presunta vulneración a los deberes contemplados en los literales b) y b) del artículo 17 de la Ley 1581 de 2012.

CUARTO: Que la investigada, el día 23 de junio de 2016 encontrándose dentro del término para ello, presentó los descargos que pretende hacer valer dentro de la presente actuación, al interior de los cuales manifestó lo siguiente:

4.1 Respecto al incumplimiento del literal b) del artículo 17 de la Ley 1581 de 2012.

"Frente a este punto es importante indicar que CODENSA como empresa prestadora del servicio de energía eléctrica, actividad reglada principalmente en la Ley 142 de 1994 y ley 143 de 1994, cuenta para el desarrollo de sus actividades de origen legal con un sistema de información, base de datos, en el cual reposa información de usuarios de la Empresa. El uso de los datos que se encuentran en esa base, es utilizado única y exclusivamente para lo relacionado con la actividad de la prestación del servicio público domiciliario de energía eléctrica y no para fines comerciales. Por lo tanto, y por tratarse del ejercicio de sus funciones legales, CODENSA, como Empresa Prestadora (sic) de un servicio público, le es permitido el uso de la información de los usuarios sin su autorización, conforme lo dispone el artículo 10 de la ley (sic) 1581 de 2012.

Por otra parte es importante tener en cuenta que en este caso Codensa actuó de acuerdo al interés legítimo que tienen los clientes, ya que en este caso Codensa lo que buscaba era revisar un reclamo de la señora [REDACTED] que consistía en la prestación del servicio público de energía eléctrica".

4.2 Respecto al incumplimiento del literal d) del artículo 17 de la Ley 1581 de 2012.

"En este punto de acuerdo al caso concreto la información solicitada a la señora [REDACTED] [REDACTED] corresponde a los datos básicos que reposan en nuestro Sistema de Información Comercial y los cuales sirven para identificar el predio y es utilizada para agilizar la atención, frente a futuros reportes o consultas relacionadas con la prestación del servicio de energía. Esta información solamente se utiliza para temas relacionados con la prestación del servicio de energía y no para fines comerciales.

En cuanto al cumplimiento de la Ley de Protección de Datos[,] Codensa informa que da estricto cumplimiento a la Ley de Protección de Datos Personales (sic) y por esta razón tiene una política y una norma de Protección de Datos (sic), desarrolladas en todo un programa integral de Protección de Datos (sic) que consiste entre otros en diferentes campañas y sensibilización a los trabajadores de Codensa y sus empresas colaboradoras, con el fin de que se tenga el conocimiento necesario de la Ley, la Política y la Norma (sic) de Protección de Datos (sic) para garantizar en todo momento su cumplimiento.

En cuanto a las medidas de seguridad, los sistemas de información de Codensa cuentan con controles de acceso a la misma, las bases de datos están en servidores con altos estándares de seguridad y son monitoreados permanentemente".

QUINTO: Que mediante Resolución N° 65576 del 10 de octubre de 2016, se corrió traslado a la sociedad investigada para que presentara alegatos de conclusión. De igual manera, se incorporaron las pruebas decretadas y aportadas por la investigada. Las cuales se relacionan a continuación:

- 5.1 Las pruebas llegadas con la denuncia presentada por la señora [REDACTED] [REDACTED] (fls. 1 al 7).
- 5.2 Los Documentos allegados con el comunicado allegado por la sociedad **CODENSA** el 16 de septiembre de 2015 radicado bajo el N° 15-184674-00002 (fls.11 al 17).
- 5.3 Los Documentos allegados con el escrito de descargos radicado el 23 de junio de 2016 bajo el bajo el N° 15-184674-00010 (fls.18 al 47).

¹ Ver folios 68 al 71

SEXTO: Que de conformidad con el radicado N° 15-184674-14² del 17 de noviembre de 2016, la Coordinadora del Grupo de Notificaciones y Certificaciones, certificó que la resolución aludida en el numeral anterior fue comunicada a la investigada el día 14 de octubre de 2016.

No obstante lo anterior, una vez vencido el plazo otorgado mediante Resolución 65576 del 10 de octubre de 2016, la investigada no se sirvió aportar los alegatos que pretendía hacer valer dentro de la presente investigación.

SÉPTIMO: 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.

OCTAVO: Análisis del caso

8.1 Adecuación típica

La Corte Constitucional mediante sentencia C-748 de 2011³, 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 b) y d) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal e) del artículo 8 de la misma norma.

En ese orden de ideas, este Despacho procederá a tener en cuenta: (i) los hechos narrados por la denunciante; (ii) las razones de hecho y de derecho aducidas por la investigada al momento de presentar los alegatos; (iii) el material probatorio que obra dentro del expediente; (iv) la Ley 1581 de 2012 y, finalmente, (v) la jurisprudencia que ha proferido la Corte Constitucional sobre la materia.

8.2 Valoración probatoria y conclusiones

8.2.1 Respecto al no cumplimiento del requisito de procedibilidad

En atención a que uno de los argumentos esgrimidos por la investigada en su escrito de descargos, se dirige a cuestionar el cumplimiento del debido proceso consagrado en la Ley 1581 de 2012, pues a su juicio, la reclamación allegada por la denunciante, no agotó el requisito de procedibilidad contemplado en el artículo 16 de la ley 1581 de 2012.

Al respecto, es pertinente mencionar que el artículo 19 de la Ley 1581 de 2012 establece las facultades otorgadas a esta Superintendencia, para el ejercicio de la función de vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos y garantías y procedimientos previstos en dicha norma.

² Ver folio 48

³ Corte Constitucional, Magistrado Ponente Jorge Ignacio Preteit Chaljub, seis (6) de octubre de dos mil once (2011).

Igualmente, el literal b) del artículo 21 de la citada norma, señala que esta Superintendencia puede "(a)delantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos; (...)".

Ahora bien, respecto del incumplimiento del requisito consagrado en el artículo 16 de la Ley 1581 de 2012, la institución investigada alega que la reclamación relacionada con los hechos aquí cuestionados no fue presentada previamente ante el Responsable, es importante precisar que con la comunicación allegada el 10 de agosto de 2015, este Despacho tuvo conocimiento de las irregularidades presentadas respecto del presunto incumplimiento de los deberes que como Responsable de la información ostenta la sociedad **CODENSA**, y teniendo en cuenta que presuntamente se puso en peligro la información de la Titular, esta Dirección decidió iniciar de manera oficiosa una investigación administrativa en contra de la sancionada, pues esta Superintendencia tiene el deber legal de iniciar directamente la investigación respectiva, sin esperar a que se agote el requisito de procedibilidad ante el Responsable de la información.

De otra parte, en aras de orientar e ilustrar a la investigada se aclara que el requisito de procedibilidad es indispensable mientras que se pretenda amparar el derecho fundamental de *habeas data* de conocer, actualizar y rectificar la información personal de un Titular. Sin embargo, al observar los hechos narrados en la denuncia, este Despacho decidió abrir de manera oficiosa la presente investigación administrativa, en ejercicio de sus facultades legales de velar por el cumplimiento del régimen de protección de datos personales.

8.2.2 Concepto de Responsable del Tratamiento de datos personales

Esta Dirección considera oportuno distinguir los conceptos de Responsable 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:

*"(...) 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"*⁴.

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.

De esta manera, una vez adelantadas las indagaciones preliminares se ha establecido que, presuntamente, **CODENSA S.A.** (i) divulgó los datos personales de la señora [REDACTED] sin contar con autorización de la referida Titular para ello y; (ii) no conservó la información suministrada por esta bajo las condiciones de seguridad necesaria para impedir el acceso y/o uso de terceros no autorizados a la misma.

Estas circunstancias le confieren la calidad de Responsable del Tratamiento de datos personales en los términos del literal e) del artículo 3 de la Ley 1581 de 2012, de forma tal que debe velar por el cumplimiento de los principios y deberes de que trata el mencionado régimen estatutario.

8.2.3 Deber de solicitar autorización para divulgar datos personales de los Titulares.

⁴ Ibidem.

De conformidad con el literal a) del artículo 3 de la Ley 1581 de 2012, la autorización para el Tratamiento de la información personal de los Titulares debe ser previa, expresa e informada. Así mismo, el literal c) del artículo 4 de la norma en comento ha consagrado el principio de libertad, según el cual, el Tratamiento de la información solamente se puede ejercer cuando el Titular haya exteriorizado su consentimiento. Adicionalmente, complementa la disposición aludida, que los datos de las personas no podrán ser obtenidos o **divulgados** sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Ahora bien, de cara a este respecto la Corte Constitucional en sentencia de constitucionalidad C-748 de 2011, expuso lo siguiente:

"En la sentencia T-022 de 1993, se estableció por primera vez el principio de libertad. En dicha oportunidad, la Corte resolvió el caso de la circulación de datos personales de contenido crediticio sin el consentimiento del titular de los datos. Es así como la Corte, bajo la necesidad de 'favorecer una plena autodeterminación de la persona' y ante la 'omisión de obtener la autorización expresa y escrita del titular para la circulación de sus datos económicos personales', resolvió conceder la tutela de los derechos a la intimidad y al debido proceso y ordenó a la central de información financiera el bloqueo de los datos personales del actor.

Desde allí, se ha dicho entonces que los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular. La Corporación ha relacionado el principio de libertad, con la prohibición del manejo de la información adquirida de manera ilícita, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos, sin la previa autorización del titular o en ausencia de mandato legal o judicial. Así, en la sentencia SU-082 de 1995, afirmó: 'los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular.' En el mismo sentido, en la Sentencia T-176 de 1995, se consideró como una de las hipótesis de la vulneración del derecho al habeas data el de la recolección de la información 'de manera ilegal, sin el consentimiento del titular de dato'.

Es entonces el principio de libertad el que permite que el Titular tenga la garantía de comprobar que los datos que circulen sobre él, han sido previamente autorizados, solicitar prueba de ello y también puede revocar su autorización para que cesen dichas actividades como formas de Tratamiento. En consecuencia, el único legitimado para permitir la divulgación de datos concernientes a su vida privada es el Titular pues su finalidad es la de asegurar la protección de sus intereses y evitar que surjan consecuencias adversas para este, ya que es a partir de la divulgación de la información privada y el uso que terceros le puedan dar a la misma, que podría logarse la efectiva identificación o posibilidad de identificar a las personas que son propietarias del dato con fines ilícitos y, en todo caso, afectando la intimidad de su Titular a partir de su uso indebido

Como conciencia del principio de libertad, pero igualmente interrelacionado, surge el deber de solicitar autorización para el Tratamiento de la información, el cual se incorpora en el literal b) del artículo 17 de la Ley 1581 de 2012, el cual es del siguiente tenor:

"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.

(...)"

Es dable entonces señalar tal como lo ha hecho la Corte Constitucional, que el núcleo esencial del *habeas data* está integrado por el derecho a la autodeterminación informática y por la libertad. La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales, por lo que sin el consentimiento del Titular se viola el derecho fundamental de *Habeas Data*, en tanto restringe injustificadamente la autodeterminación del sujeto respecto de su información personal, pues la administración de sus datos, en cuanto al acopio, Tratamiento y divulgación, se estaría haciendo a sus espaldas.

Debe tenerse en cuenta que no solamente es necesario solicitar el consentimiento del Titular para el Tratamiento de sus datos, en especial si se pretende divulgar la misma, sino que adicionalmente ese consentimiento debe ser calificado, por cuanto debe ser previo, expreso e informado.

Tales características implican que para la recolección del dato; primero, la autorización debe ser suministrada en una etapa anterior a la incorporación de la información; segundo, la autorización debe ser inequívoca y; tercero, que se le comuniquen al Titular las finalidades del tratamiento y los usos que se dará a la información recolectada.

De todo lo anterior, puede entonces concluirse que el principio de libertad no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de restringir el uso que se hará de la información. Adicionalmente, que sólo pueden ser registrados y **divulgados** los datos personales con el consentimiento libre, previo, expreso e informado del Titular, lo que conduce inexorablemente a señalar que no está permitido el consentimiento tácito del Titular del dato y, consecuentemente, sólo podrá prescindirse de él por expreso mandato legal o por orden de autoridad judicial; lo que nos permite introducirnos al siguiente punto de la presente actuación. Objeto de consideraciones

8.2.4 Casos en que no es necesaria la solicitud de autorización.

De acuerdo con lo establecido en el artículo 10 de la Ley 1581 de 2012, únicamente en cinco casos taxativamente establecidos por el legislador se puede prescindir de solicitar autorización. Así, la norma consagra expresamente lo siguiente:

"Artículo 10. Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:

- a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.*
- b) Datos de naturaleza pública.*
- c) Casos de urgencia médica o sanitaria.*
- d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.*
- e) Datos relacionados con el Registro Civil de las Personas".*

Si bien se señaló en el numeral 9.2.2 de la presente decisión que uno de los supuestos para considerar la legalidad y legitimidad de los procesos de recolección, uso o divulgación de los datos es el otorgamiento de la autorización por parte de su Titular, el legislador consagró un grupo de situaciones en las que no es necesaria la autorización, las cuales responden a la naturaleza misma del dato y al tipo de funciones que cumplen, y que en todo caso responden a intereses constitucionales que justifican dicha limitación.

De cara a estas excepciones, la Corte Constitucional en la sentencia C-748 de 2011 efectuó las siguientes precisiones:

*"En relación, con las autoridades públicas o administrativas, señaló la Corporación que tal facultad 'no puede convertirse en un escenario proclive al abuso del poder informático, esta vez en cabeza de los funcionarios del Estado. Así, el hecho que el legislador estatutario haya determinado que el dato personal puede ser requerido por toda entidad pública, bajo el condicionamiento que la petición se sustente en la conexidad directa con alguna de sus funciones, de acompasarse con la garantía irrestricta del derecho al hábeas data del titular de la información[']. En efecto, amén de la infinidad de posibilidades en que bajo este expediente puede accederse al dato personal, **la aplicación del precepto bajo análisis debe subordinarse a que la entidad administrativa receptora cumpla con las obligaciones de protección y garantía que se derivan del citado derecho fundamental, en especial la vigencia de los principios de finalidad, utilidad y circulación restringida.***

Para la Corte, esto se logra a través de dos condiciones: (i) el carácter calificado del vínculo entre la divulgación del dato y el cumplimiento de las funciones de la entidad del

poder Ejecutivo; y (ii) la adscripción a dichas entidades de los deberes y obligaciones que la normatividad estatutaria predica de los usuarios de la información, habida consideración que ese grupo de condiciones permite la protección adecuada del derecho.

(...)

En lo que se relaciona con los datos públicos y el registro civil de las personas, su naturaleza hace que no estén sujetos al principio de autorización. La información pública es aquella que puede ser obtenida sin reserva alguna, entre ella los documentos públicos, habida cuenta el mandato previsto en el artículo 74 de la Constitución Política. Esta información puede ser adquirida por cualquier persona, sin necesidad de autorización alguna para ello.

Frente a los casos de urgencia médica y sanitaria, en aras de la efectividad del derecho a la libertad en el manejo de datos, la norma debe entenderse que opera sólo en los casos en que dada la situación concreta de urgencia, no sea posible obtener la autorización del titular o resulte particularmente problemático gestionarla, dadas las circunstancias de apremio, riesgo o peligro para otros derechos fundamentales, ya sea del titular o de terceras personas.

En relación con el tratamiento para fines históricos, estadísticos o científicos, la norma no ofrece reparo de constitucionalidad en razón a que delega a la Ley la manera como estos datos deben ser protegidos, además, debe interpretarse en concordancia con el literal e) del artículo 6 que señala que en estos casos "deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares".

Empero, no puede perderse de vista que pese a que no se requiera autorización en los eventos anteriormente señalados, si resulta necesario y obligatorio que para el Tratamiento de dicha información se tenga que observar el cumplimiento íntegro de las disposiciones contenidas en la Ley 1581 de 2012.

8.2.5 Deber de conservar la información bajo las condiciones de seguridad para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado.

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 los literales f) y g) del artículo 4 se encuentra relacionados con el caso en concreto, que expresamente señala:

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

(...)

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.

(...)"

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.

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 rectificadas o corregidas, 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, que 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.

Puntualmente, frente a deber de conservar la información bajo las condiciones de seguridad suficientes para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado, el literal d) del artículo 17 de la Ley 1581 de 2012 establece lo siguiente:

"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:

(...)

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

(...)"

Por su parte, teniendo en cuenta el artículo 15 de la Constitución Política de Colombia, en concordancia con los principios rectores de seguridad y de circulación restringida, se tiene que como una extensión de los mismos, el legislador concibió en el literal d) del artículo 17 de la Ley Estatutaria de Protección de Datos Personales, como deber de los Responsables del Tratamiento de datos, la conservación de la información con todas las medidas de seguridad que sean necesarias con el fin de evitar cualquier clase de acceso no autorizado o fraudulento.

Ahora bien, es necesario precisar que las disposiciones consagradas en el literal d) previamente citado, deben interpretarse a la luz de los principios de acceso y circulación restringida y de seguridad.

De acuerdo con las normas en cita, la información que es recolectada por los sujetos obligados, debe resguardarse con las condiciones de seguridad necesarias, de tal suerte que se pueda impedir que la misma sea adulterada, consultada, usada o accedida sin autorización por parte de su titular.

En este sentido, el manejo de información personal debe hacerse bajo todas las medidas de seguridad necesarias para impedir que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el Responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular.

Por lo tanto, tal como lo ha señalado la Corte es *"deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria"*, pues los diversos avances tecnológicos han producido un crecimiento de los sistemas de

información, y fenómenos como las redes sociales que han facilitado el intercambio de información y, sobre todo, de acceso a la misma a través de la red, aumenta los riesgos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación, pues de lo contrario, el acceso y uso inadecuado de esa información puede tener graves efectos negativos, en los ámbitos personales y de buen nombre.

En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas y mecanismos de seguridad acordes con el sistema de información correspondiente. Así, por ejemplo, en el ámbito de redes sociales se deben establecer medidas de protección razonables y reforzadas siempre que se pretenda su publicación en la red, para evitar que la información almacenada en la red sea accesible a terceras personas no autorizadas, teniendo en cuenta que bajo este supuesto la información ya no se encuentra en una sencilla bases de datos, sino que ha pasado a formar parte del mundo cibernético en el que los riesgos de su almacenamiento resultan mayores y siempre están latentes.

De esta manera, el Responsable deberá tener en cuenta tanto el volumen de la base de datos a la que realiza Tratamiento, como la naturaleza de los datos que trata, haciendo que dichas medidas o controles de seguridad sean directamente proporcionales al tipo de base de datos que trate. Especialmente, se debe tener presente que a pesar de que exista previamente una autorización por parte del Titular para divulgar su información personal, la divulgación, circulación y acceso de los datos tiene que estar controlado y restringido frente a terceros no autorizados. Únicamente de esta forma, se cumplirá con los estándares exigidos por la ley.

8.2.6 Análisis del caso en particular.

Como se expuso a punto quinto de la presente providencia, una vez vencido el plazo otorgado mediante Resolución 65576, la investigada no ejerció su derecho de defensa y contradicción, pues no aportó los alegatos que pretendía hacer valer dentro de la presente investigación. Razón por la cual pasará este Despacho a pronunciarse en consideración a los descargos que en su momento se radicaron en esta Dirección.

8.2.6.1 Cargo primero.

Respecto a este primer cargo, se tiene que esta Dirección reprocha a la investigada el no haber solicitado autorización de la Titular [REDACTED] para divulgar su información en la red social Twitter. De acuerdo con lo anterior, se aportó captura de pantalla a través del cual salta a la vista que a través de la referida red social, la investigada, a modo de respuesta a uno de los cuestionamientos efectuados por la usuaria, publicó la dirección de domicilio de su residencia, dando a entender que tenía conocimiento exacto del lugar en el que se estaba presentando la falla del servicio, de acuerdo con ello, se cuenta con la siguiente imagen:



Llegados a este punto, resulta necesario hacer alusión a las diversas categorías de datos personales, los cuales por desarrollo jurisprudencial constitucional se han clasificado en las categorías recogidas en el artículo 3 de la Ley 1266 de 2008⁵, de acuerdo con la cual, los datos personales son: públicos, semiprivados y privados, y se definen así:

(...)

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;*

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.*

(...)"

Partiendo de los anteriores preceptos, se tiene que la información publicada por CODENSA a través del servicio de microblogging Twitter, es decir, la dirección de residencia de la Titular, detenta el carácter de privado, por lo que para su divulgación se hacía necesario que previamente se hubiese otorgado autorización por parte de la señora [REDACTED].

Téngase en cuenta que el vocablo "divulgar" hace referencia a "publicar, extender, poner al alcance del público algo"⁶; y a través del mensaje mediante el cual se dio respuesta a las observaciones de la usuaria, se puso al alcance del público la dirección de residencia de la señora [REDACTED] y, sin embargo, no se ofreció prueba alguna de que el Responsable del Tratamiento hubiese cumplido con su deber de obtener el consentimiento expreso de la Titular para llevar a cabo dicha acción.

Ahora, la investigada argumenta en sus descargos que "El uso de los datos que se encuentran en esa base, es utilizado única y exclusivamente para lo relacionado con la actividad de la prestación del servicio público domiciliario de energía eléctrica y no para fines comerciales". De cara a este respecto, sea lo primero mencionar que en momento alguno se está cuestionando a **CODENSA** por la finalidad que se le pueda estar dando a la información que ellos recolectan, es decir, la controversia no se suscita a partir del cuestionamiento de si la información está siendo usada con fines comerciales o estrictamente para la prestación del servicio público de energía. Pues el reproche se efectuó porque la investigada hizo una publicación en twitter en el que quedaba al descubierto un dato privado de una de sus usuarias sin contar con autorización para ello. Por lo tanto, este argumento no está llamado a prosperar.

Igual suerte corren los argumentos planteados a través de los cuales la investigada refiere que "como Empresa Prestadora (sic) de un servicio público, le es permitido el uso de la información de los usuarios sin su autorización, conforme lo dispone el artículo 10 de la ley (sic) 1581 de 2012" y

⁵ Cfr. Corte Constitucional, Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub: "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 del texto original).

⁶ Diccionario de la Lengua Española; edición tricentenario. Real Academia Española

que "en este caso Codensa actuó de acuerdo al interés legítimo que tienen los clientes, ya que en este caso Codensa lo que buscaba era revisar un reclamo de la señora [REDACTED] que consistía en la prestación del servicio público de energía eléctrica".

Al respecto es importante precisar que si bien la autorización para realizar el Tratamiento de los datos personales de la Titular respecto a la prestación del servicio público de energía se enmarca entre las excepciones de dicho requisito impuestas por la Ley 1581 de 2012, dicho Tratamiento debe solo efectuarse para dicho fin, es decir que si una empresa prestadora de servicios públicos hace uso de los datos personales de naturaleza privada de los Titulares para un fin distinto a la prestación del servicio público deberá contar con una autorización previa, expresa e informada.

Bajo dicho entendido, este Despacho encuentra que la sociedad investigada no expone puntualmente el porqué la divulgación de los datos personales de la señora [REDACTED] de esa información se encuentra cobijada por una de las causales de exclusión del artículo 10 de la Ley 1581 de 2012, y esta Dirección considera que la divulgación de un dato privado a través de la red social twitter no se encuentra enmarcada dentro de la naturaleza de la prestación del servicio público de energía.

Así mismo, hay que indicar que si bien la investigada pudo actuar en atención a los intereses de la Titular, el derecho de *Habeas Data* tiene el rango de fundamental, razón por la cual debe darse prevalencia sobre cualquier otra prerrogativa, además, la sociedad **CODENSA** disponía de otros medios para garantizar los intereses de sus clientes sin poner en riesgo su derecho de *Habeas Data* y su seguridad personal.

En este entendido, es necesario que el Responsable del Tratamiento vele por la protección efectiva del derecho de *Habeas Data* de los Titulares, y se implemente un canal que le permita atender de forma efectiva la consulta de estos y, a la vez, impedir el acceso indebido de terceras personas a la información de los mismos.

En consecuencia, este Despacho encuentra que la sociedad investigada incumplió con el deber contemplado en el literal b) del artículo 17 de la Ley 1581 de 2012, pues pese a que pueda realizar el Tratamiento de la información Personal de la denunciante para efectos de la prestación del servicio público de energía sin requerir una autorización previa, expresa e informada de la Titular, si requería de dicha autorización para efectos de compartir y divulgar la información con Terceros.

8.2.6.2 Cargo segundo.

De cara al segundo cargo, esta Dirección reprocha a la investigada el hecho de que no haya guardado la información de la señora [REDACTED] - concerniente a su dirección de domicilio -, bajo las condiciones de seguridad necesarias para impedir que terceros no autorizados tuviesen acceso a la misma de conformidad con los postulados contenidos en el literal d) del artículo 17 de la Ley 1581 de 2012, con lo que, a su vez, se trasgredieron los principios de circulación restringida y de seguridad, previamente mencionados.

Se tiene entonces que este Despacho cuenta con la captura de pantalla del servicio de microblogging twitter (fl.4) suministrada por la Titular, en la que queda en evidencia que la sociedad **CODENSA** publicó la dirección de domicilio de la señora [REDACTED] sin contar con autorización para ello.

Al respecto y de manera posterior, haciendo uso del derecho de defensa que le asiste a la investigada, **CODENSA**, mediante el escrito de descargos argumentó que la información que de la Titular tienen almacenada "corresponde a los datos básicos que reposan en nuestro Sistema de Información Comercial y los cuales sirven para identificar el predio y es utilizada para agilizar la atención, frente a futuros reportes o consultas relacionadas con la prestación del servicio de energía. Esta información solamente se utiliza para temas relacionados con la prestación del servicio de energía y no para fines comerciales".

Frente a este argumento, debe ser tajante el Despacho al aclarar que el hecho de que el dato sea catalogado como "básico" por la investigada o que su uso consista en identificar el predio y para agilizar la atención de reportes o consultas relacionadas con la prestación del servicio de energía, no desnaturaliza su condición de dato personal de carácter privado y, por ende, deben aplicarse las medidas de seguridad necesarias y suficientes para impedir el acceso a esa información por parte

de terceros. Algo que evidentemente no se adelantó, toda vez que a través de una red social se permitió que centenares de personas conocieran la dirección de domicilio de la señora [REDACTED].

Con dicho proceder se deja en evidencia el deber de diligencia y cuidado que debió observar la investigada en su condición de Responsable del Tratamiento en las actividades que involucran el manejo de información personal dentro de los procesos de atención a las quejas y reclamos de sus clientes, que en armonía con el principio de circulación restringida, la información de los Titulares 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 Ley 1581 de 2012.

Por otro lado, en lo atinente a la manifestación de que "los sistemas de información de Codensa cuentan con controles de acceso a la misma, las bases de datos están en servidores con altos estándares de seguridad y son monitoreados permanentemente", resulta claro que el cargo no se fundamenta en la falta de implementación de controles técnicos por parte de la sociedad **CODENSA** para garantizar el adecuado cumplimiento de las disposiciones de la Ley 1581 de 2012, sino que dentro de su actuar no previó el deber de diligencia suficiente para adoptar las medidas necesarias para otorgar seguridad a los registros, evitando publicaciones en la red social twitter que permitieran la consulta, el uso o el acceso no autorizado de la información de la señora [REDACTED].

Bajo dicho entendido, es claro para este Despacho que **CODENSA**, en su condición de Responsable del Tratamiento debía asegurar la información para evitar su divulgación, pues el hecho de tener implementado políticas de Tratamiento de la información y controles internos de seguridad no impidió que en su práctica fuera la misma sociedad quien divulgara y circulara sin ningún tipo de restricción los datos personales de la denunciante.

En consecuencia, este Despacho encuentra que la investigada incumplió con el deber contemplado en el literal d) del artículo 17 de la Ley 1581 de 2012, el cual contempla que los Responsables de la información deberán conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, razón por la cual se impondrá la correspondiente sanción.

NOVENO: Imposición y graduación de la sanción

9.1 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:

9.1.1 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.

Para el caso que nos ocupa, hay que partir del hecho de que la investigada no demostró contar con autorización de la denunciante para divulgar su información a través de la red social twitter, pues pese a que para el Tratamiento de los datos personales para efectos de la prestación del servicio de energía no se requiera la autorización del Titular, si es necesarios cumplir con dicho requisito cuando la información es tratada con una finalidad de naturaleza distinta a la prestación del servicio público, es por ello que al haber divulgado la información personal de la señora [REDACTED] vulneró su derecho de *habeas data* puesto que dicho Tratamiento fue realizado sin el consentimiento previo, expreso e informado de la misma.

Aunado a lo anterior, y teniendo en cuenta que la sociedad investigada no contaba con la autorización previa Expresa e informada de la Titular para la divulgación de sus datos personales, se encuentra que la sociedad **CODENSA** no conservo la información bajo las condiciones de

seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, toda vez que a través de la red social Twitter dispuso al alcance de terceros los datos personales de la denunciante poniendo en riesgo la intimidad dela misma y violando claramente su derecho de *habeas data*.

En virtud de lo anterior, este Despacho impondrá una multa equivalente a trescientos cincuenta (350) salarios mínimos legales mensuales vigentes por el incumplimiento de los deberes establecidos en los literales b) y d) del artículo 17, en concordancia con los literales c), f) y g) del artículo 4 y el artículo 9 de la Ley 1581 de 2012, sanción que resulta proporcional a la naturaleza de la infracción.

9.1.2 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 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.

En mérito de lo expuesto este Despacho,

RESUELVE

ARTÍCULO PRIMERO: Imponer una sanción pecuniaria a la sociedad **CODENSA S.A. E.S.P.** identificada con el Nit. 830.037.248, de **DOSCIENTOS CUARENTA Y UN MILLONES TRESCIENTOS NUEVE MIL DOSCIENTOS CINCUENTA PESOS M/cte.** (\$241.309.250.00), equivalente a trescientos (350) salarios mínimos legales mensuales vigentes, por el incumplimiento de los deberes establecidos en los literales b) y d) del artículo 17, en concordancia con los literales c), f) y g) del artículo 4 y el artículo 9 de la Ley 1581 de 2012, por los hechos descritos en la parte motiva de esta providencia.

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: Notificar personalmente el contenido de la presente resolución a la sociedad **CODENSA S.A. E.S.P.** identificada con el Nit. 830.037.248, 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 TERCERO: Comuníquese el contenido de la presente resolución a la señora [REDACTED], identificado con la cedula de ciudadanía No [REDACTED].

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D. C.,

13 DIC 2016

El Director de Investigación de Protección de Datos Personales,


CARLOS ENRIQUE SALAZAR MUÑOZ

NOTIFICACIÓN

Investigada:

Entidad: CODENSA S.A. E.S.P.
Representante Legal
para asunto judiciales :
Identificación: [REDACTED]
NIT 830.037.248
Correo electrónico: bernardo.gomez@enel.com.co
Dirección: Carrera 11 N° 82-76 Piso 8
Ciudad: Bogotá, D.C.

COMUNICACIÓN

Denunciante:

Señora: [REDACTED]
Identificación: [REDACTED]
Dirección: [REDACTED]
Dirección de correo electrónico: [REDACTED]
Ciudad: Bogotá, D.C.