EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y LA RESPONSABILIDAD DE LA ADMINISTRACIÓN PÚBLICA EN EL TRATAMIENTO DE DATOS PERSONALES

En Colombia los principios y preceptos contenidos en la Ley Estatutaria 1581 del 2012 "por la cual se dictan disposiciones generales para la protección de datos personales" le son los aplicables al tratamiento de datos personales que se encuentren en bases de datos y archivos tanto de entidades de derecho privado como de naturaleza pública.

Es por ello que a la luz de la Ley General de Protección de Datos Personales, la administración pública en desarrollo de la función de gestión del Estado, tiene una doble condición. Por un lado, es un sujeto vigilado al ser responsable del tratamiento de los datos personales consignados en sus bases de datos, y por otra parte, como autoridad de vigilancia y control en el tratamiento de datos personales, debe garantizar que en su la recolección, uso y disposición final se dé cumplimiento a los principios, derechos y deberes de los titulares.

A partir de esta doble función que desempeña el Estado, se plantea el análisis de la presente investigación, que busca dilucidar cuál es la responsabilidad de la administración pública cuando hace tratamiento de datos personales y cuál es la eficacia de sus facultades de vigilancia y control a dos años de haber entrado en vigencia la Ley 1581 del 2012.

El primer postulado trae consigo varios retos importantes que se deben abordar cuando las entidades de derecho público actúan como responsables del

tratamiento. Los principales cuestionamientos que surgen están enfocados a aclarar si las entidades de derecho público de los ámbitos nacionales, regionales y locales requieren de autorización para el tratamiento de datos personales. La respuesta positiva conlleva a preguntarse si están obligadas a cumplir con todos y cada uno de los deberes a que obliga la ley o si por el contrario están exceptuados de implementar una política de protección de datos personales, medidas técnicas, humanas y administrativas dentro de sus organizaciones que garanticen el correcto tratamiento de los datos personales, como lo están obligadas las entidades de derecho privado.

Así mismo, es igualmente importante revisar cuáles son las responsabilidades administrativas y disciplinarias que se derivan del tratamiento no autorizado de los datos personales y cuáles sus consecuencias. Tales proposiciones hacen repensar la manera como las entidades recogen, almacenan, tratan y eliminan información personal. Tal actividad, propia de las funciones que realizan, les sugiere el reto de llegar a determinar qué datos poseen, qué uso les están dando y con qué finalidad recolectan y tratan permanentemente información personal de los ciudadanos.

La Ley de Protección de Datos Personales también regula la manera como se deben atender las consultas y los reclamos y garantiza el derecho a conocer, actualizar, rectificar y suprimir la información personal que tiene el ciudadano, así como el alcance y trámite de las peticiones de revocatoria de la autorización. La administración pública debe crear una nueva manera de comunicar internamente y hacia el exterior la información que trata,[230] es decir, debe ajustar los canales de contacto con el titular a fin de garantizar que las áreas de atención de consultas, quejas y reclamos puedan brindar, dentro de los términos que da la ley, respuesta clara, completa y oportuna sobre las solicitudes y peticiones para responder al pleno y efectivo ejercicio del derecho de protección de datos personales.

Por otra parte, cuando el Estado mediante la Superintendencia de Industria y Comercio, y más exactamente por medio de la Delegatura para la Protección de Datos Personales,[231] ejerce las facultades de vigilancia del tratamiento de

230 Samuel Parra y Jorge Campañilla, "El procedimiento Administrativo electrónico y la normatividad de protección de datos de carácter personal" en *Administración electrónica*. Lorenzo Cotino Hueso (Valencia: Tirant Lo Blanch, 2010), 807-818.

231 Artículo 17 de la Ley 1266 del 2008, Artículo 19 de la Ley 1581 del 2012 y Decreto 4886 del 2011.

los datos personales, se hace garante del amparo de un derecho fundamental[232] consagrado en el artículo 15 de la Constitución Política Colombiana, por lo que sus decisiones traen consecuencias relevantes en el ámbito personal, llegando a verse comprometidos no solo el derecho de *habeas data*, sino el mismo derecho a la intimidad.

En este ámbito de aplicación, la vigilancia la ejerce con respecto a las bases de datos en manos de entes de derecho público, sociedades de derecho privado, asociaciones y organizaciones no gubernamentales, que se ubiquen en Colombia o a aquellas entidades –responsables o encargadas– que estando fuera del territorio nacional, les sean aplicables la legislación colombiana en virtud de normas y tratados internacionales.

Adicional al amplio escenario objeto de vigilancia de la Superintendencia de Industria y Comercio, el Estado está obligado a regular materias especiales como el Registro Nacional de Bases de Datos, el tratamiento de datos personales de niños, niñas, adolescentes, las normas corporativas vinculantes, las transferencias de datos a terceros países, las políticas de tratamiento y los protocolos de seguridad en su tratamiento.

Tal escenario plantea muchos cuestionamientos acerca del real ejercicio de la facultad de vigilancia y del amparo del derecho fundamental, por lo que en esta investigación también se busca dilucidar además de cuáles han sido los volúmenes de quejas y denuncias presentadas en los primeros años de creación del ente de vigilancia y desde la entrada en vigencia de la Ley 1581 del 2012.[233] También se buscará conocer cuál ha sido el desarrollo reglamentario de la Ley General de Protección de Datos Personales y si este ha sido completo y suficiente o si por el contrario, se puede indilgar responsabilidad a la administración por omisión y demora en la implementación de políticas completas en esta materia para el país.

Finalmente, del estudio integral de los temas abordados, se logrará tener una visión completa de la responsabilidad del Estado como garante del cumplimiento y del amparo del derecho fundamental a la protección de datos personales.

232 Corte Constitucional, *Sentencia C-748 del 2011*, M. P. Jorge Ignacio Pretelt Chaljub.

233 Superintendencia de Industria y Comercio. I*nformes anuales de gestión de la Delegatura para la Protección de Datos Personales* (Bogotá: Superintendencia de Industria y Comercio, 2012-2013).

La administración pública como responsable del tratamiento de datos personales

Consideraciones básicas

El derecho de *habeas data* o derecho a la protección de datos personales está constitucionalmente reconocido en el artículo 15 de la Carta Política colombiana como un derecho fundamental que busca garantizar al titular del derecho, la posibilidad de determinar a quién entrega su información y qué información da a conocer. Es un derecho que desde antes de la Constitución Política de 1991, se había consolidado jurisprudencialmente por medio de las sentencias de unificación SU-082 de 1995 y SU-089 de 1995,[234] como un derecho propio del individuo, denominado derecho a la autodeterminación informativa o informática.[235]

El ámbito de aplicación de la Ley General de Protección de Datos Personales o Ley Estatutaria 1581 del 2012[236]está circunscrito al tratamiento de datos personales que hagan tanto personas jurídicas de naturaleza pública como el que realicen las asociaciones y demás sociedades de derecho privado.[237]

Las entidades públicas como órganos mediante los cuales la administración pública cumple la función de satisfacer de forma directa e inmediata las necesidades colectivas de los asociados y los fines del Estado son las encargadas de recoger, usar, administrar y guardar datos personales de sus asociados, en principio para el ejercicio de sus funciones públicas. Es por ello que con la entrada en vigencia de la Ley 1581 del 2012, el tratamiento de datos personales por parte de las entidades de derecho público, debió someterse a una revisión integral a la luz

234 Corte Constitucional. M. P. Jorge Arango Mejía.

235 "Debe tenerse en cuenta que la denominación habeas data no ha sido la única utilizada por la jurisprudencia para identificar las facultades del sujeto concernido respecto de las bases de datos. Así, durante el desarrollo del concepto en las decisiones de la Corte se han usado las expresiones de 'autodeterminación informática' o 'autodeterminación informativa'. En todo caso, estas tres definiciones refieren a la misma realidad jurídica, por lo que no ofrecen mayores dificultades en su uso alternativo. Sin embargo, ante la necesidad de contar con una descripción uniforme y habida cuenta del uso extendido del término en el ámbito del derecho constitucional colombiano, esta sentencia utilizará el vocablo habeas data con el fin de nombrar el derecho que tienen todas las personas a ejercer las facultades de conocimiento, actualización y rectificación de la información personal contenida en bases de datos". Corte Constitucional, *Sentencia C-1011 del 2008*, M. P. Jaime Córdova Triviño.

236 La Ley 1581 del 2012 fue sancionada el 17 de octubre del 2012 y publicada en el *Diario Oficial* No. 48.587 de 18 de octubre del 2012. El artículo 28 estableció un régimen de transición.

237 Artículo 2 de la Ley 1581 del 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" (Bogotá: *Diario Oficial* No. 48587 de octubre 18 del 2012).

de la nueva norma para ajustarse a ella y garantizar el pleno y efectivo cumplimiento de los deberes consagrados en el derecho de *habeas data*.

Si bien el ámbito de aplicación señalado en el artículo 2 de la Ley 1581 del 2012 excluyó el uso de la citada norma en el tratamiento que se haga de las bases de datos y archivos 1) de uso estrictamente doméstico y de aquellas que contengan información con finalidades de 2) seguridad y defensa del Estado, el lavado de activos y financiamiento del terrorismo, 3) inteligencia y contrainteligencia, 4) información periodística y otros contenidos editoriales y 5) bases de datos reguladas por la Ley 79 de 1993,[238] no las excluyó de la aplicación de los principios que la ley estableció como directriz fundamental de la actividad de tratamiento de datos personales.

En consecuencia, si bien los organismos del Estado que realizan tareas de vigilancia y control de las actividades antes señaladas no están sometidos a los procedimientos para el ejercicio del derechos de *habeas data*, sí deben realizar sus funciones respetando los principios de legalidad, finalidad, libertad, veracidad o calidad del dato; transparencia, acceso y circulación restringida, seguridad y confidencialidad en el tratamiento de datos personales.[239]

El eje fundamental del derecho de *habeas data* se centra en la autorización que brinda el titular del derecho a quien pretende recoger el dato. El concepto legal es autorización que debe ser previa, expresa e informada,[240] es decir, que para que se entienda que fue otorgado de acuerdo con la ley, se debe avisar al titular de la información[241] con qué finalidad se recaba, quién es el responsable[242] de la información, cuáles son los canales o medios de contacto con el responsable para ejercer sus derechos y, en caso de que el dato personal por recoger esté clasificado

238 "Por la cual se regula la realización de censos de población y vivienda en todo el territorio nacional".

239 El artículo 4 de la Ley 1581 definió estos principios de manera coherente con el desarrollo jurisprudencial que se venía dando en Colombia desde la Constitución Política de 1991, así como de manera armónica con los principios del derecho a la protección de datos personales de la Directiva del Consejo de Europa No. 46 de 1995, conocida como la Directiva 95/46/CE y la Resolución 45/95 de la Organización de Naciones Unidas (ONU).

240 Literal a) del artículo 3 de la Ley 1581 del 2012.

241 "Artículo 3. Definiciones: para efectos de la presente ley, se entiende por: f) Titular: persona natural cuyos datos personales sean objeto de tratamiento.

242 Es quien decide sobre el uso de la base de datos y quien se hace responsable de los datos allí depositados.

como dato sensible,[243] –es decir, que el titular puede llegar a ser discriminado y/o verse afectada en su intimidad–, el responsable de recoger el dato está obligado a informar sobre el carácter facultativo de su respuesta, o sea que el titular puede o no entregar su información si así lo desea.

El artículo 10 de la Ley 1581 del 2012 estableció los casos en que no es necesaria la autorización del titular para realizar el tratamiento de los datos, de la siguiente manera:

1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
2. Datos de naturaleza pública.
3. Casos de urgencias médica o sanitaria.
4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
5. Datos relacionados con el registro civil de las personas.
   Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley. (Subrayado fuera de texto)

Respecto del último párrafo del artículo citado, la Corte Constitucional indicó que:

> […] Una lectura de la norma permite interpretar que lo que busca el legislador estatutario es que en los casos taxativos permitidos por el artículo 10, en los que no es necesario el consentimiento del titular, el uso del dato también debe sujetarse a todos los principios y limitaciones consagrados en la ley. Por el contrario, jamás podría interpretarse como una autorización abierta para que se acceda a datos personales sin consentimiento del titular.[244]

El artículo 2.2.2.25.1.3 del Decreto 1074 del 2015 "Decreto Único del Sector Comercio, Industria y Turismo" define dato público de la siguiente manera:

243 Los datos personales fueron clasificados en Colombia en 1) dato personal de carácter público; 2) dato personal semiprivado, 3) dato personal privado y 4) dato personal privado sensible. Este último se entiende como " […] aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tal como aquel que revele el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos". Artículo 5 de la Ley 1581 del 2012.

244 Corte Constitucional, *Sentencia C-748 del 2011*, M. P. Jorge Ignacio Pretelt Chaljub

> "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. (Subraya fuera de texto).

De acuerdo con lo expuesto, cuando los datos personales que se están recolectando son de naturaleza pública, como por ejemplo los relativos al estado civil de las personas, a su profesión u oficio, a la calidad de comerciante o de servidor público, no se requiere autorización del titular para ser tratados, aunque quien los recoge y trata no está exento de cumplir a cabalidad tanto con los principios que rigen la actividad, así como con las demás obligaciones que les impone la ley.

Ahora, es importante distinguir que si bien la información del comerciante, servidor público y del profesional, tiene la connotación de datos personales de naturaleza pública, como lo puede ser el teléfono de su oficina o comercio, la dirección laboral, entre otros, la información personal como el correo personal, su teléfono privado y su dirección de residencia son datos de naturaleza privada, por lo que su recolección y uso requieren de su autorización para ser tratados y se está en la obligación de garantizar todos y cada uno de sus derechos. Es entonces importante no confundir la información de un titular que es tratada en virtud de su profesión u oficio, a la que de este se haga en su ámbito privado.

Si bien la norma definió como dato público, aquel que de carácter residual no es semiprivado, privado o sensible, sin dar mayores luces sobre cuáles son estos de manera concreta, sí dio algunos ejemplos de manera no taxativa, señalando que dada 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 legal".

Al realizar el análisis del alcance de lo establecido por la Ley 1581 del 2012 al considerar que los datos públicos "pueden estar contenidos en registros públicos", es necesario resaltar que en tal evento, los datos personales que allí se encuentren consignados en razón a un deber legal de estar incorporados, no se convierten en datos públicos, ya que su naturaleza no cambia. Así lo señaló la Superintendencia de Industria y Comercio en la investigación administrativa

sancionatoria No. 13-249768 realizada sobre la publicación de datos personales sin autorización en los directorios telefónicos de la ciudad de Bucaramanga del año 2013-2014, cuando manifestó que pese a estar los datos personales de los titulares consignados en un directorio telefónico:

> […] la naturaleza del dato, como lo es la dirección y teléfono de contacto de su residencia, no pierde su carácter de dato personal de naturaleza privada, por lo que su tratamiento estará sometido a la autorización que el titular otorgue para la finalidad que haya decidido conferir.

En el caso concreto era aparecer en tales directorios.

En el mismo sentido, los "registros públicos" como los que poseen las Cámaras de Comercio, Sayco y Acinpro, las Secretarías de Tránsito y Transporte, las oficinas de Instrumentos Públicos y las Secretarías de Hacienda, entre otras, –todas entidades de derecho público que en razón de las funciones que desempeñan, poseen datos personales–, no están obligadas a recoger la autorización de los titulares para el tratamiento de los datos personales que ya poseen, siempre y cuando la información que se recoja sea para el ejercicio de las funciones propias y en el ámbito de su competencia. Es decir que, en la medida en que los datos fueron recolectados en ejercicio del deber legal y con una finalidad específica, la administración los usará de acuerdo con esa finalidad, por lo que no podrá cederlos a particulares u otras entidades, salvo que así lo disponga una orden de autoridad competente o lo haga el titular por expresa autorización.

Por otro lado, cuando los datos personales están consignados en "documentos públicos", no se puede considerar que son de naturaleza pública, ya que en muchas de las ocasiones solo el titular está facultado para acceder a él y su publicidad estará sometida las restricciones que la ley haya impuesto. Así lo ha entendido la Corte Constitucional en la Sentencia T-473 de 1992:[245]

> Los funcionarios están autorizados para no permitir el acceso a aquellos documentos cuya consulta o comunicación pueda atentar contra secretos protegidos por ley, tales como los concernientes a la defensa y seguridad nacionales, a investigaciones relacionadas con infracciones de carácter penal, fiscal, aduanero o cambiario así como a los secretos comerciales e industriales. El acceso no es tampoco permitido cuando el contenido de los documentos vulnere el derecho a la intimidad […].

245 M. P. Ciro Angarita Barón.

Por lo que queda claro que pese a que el dato personal esté contenido en un documento público, su acceso estará sometida tanto a la disponibilidad del documento como a que con su divulgación no se vulneren los derechos relativos a la persona como el *habeas data* y la intimidad.

Así mismo, cuando los datos estén contenidos en "sentencias judiciales debidamente ejecutoriadas" no necesariamente deben estar a libre acceso de cualquiera y mucho menos de manera no controlada por medios electrónicos. Así lo comunicó la Superintendencia de Industria y Comercio a la Corte Suprema de Justicia[246] que, en razón de un recurso de casación interpuesto por el investigado, confirmó la condena a prisión por el delito de acceso carnal violento en menor de catorce años. En el fallo, no solo se señalaba el nombre y lugar de residencia de la menor, sino que se hizo pública información propia de los dictámenes médico- forenses. La sentencia en mención fue colgada en el portal web de la entidad pública, lo que favoreció el acceso a los datos de la menor de edad.[247]

Ante la queja presentada por el representante legal de la menor, la Superintendencia de Industria y Comercio solicitó a la relatoría de la Sala Penal de la Corte Suprema de Justicia que de manera inmediata:

> Suprimiera las versiones que publique en Internet de la providencia dictada el 16 de mayo del 2007, dentro del proceso No. 22224 y de todas las publicaciones que se hayan efectuado o se efectúen de la misma, el nombre de la menor YYY, el de sus familiares, así como todos los datos que permitan la identificación de estos.

Esto, por tratarse de información relativa a menores, a la luz del artículo 7 de la Ley 1581 del 2012, que son catalogados como una categoría especial de datos, por lo que salvo los públicos, su tratamiento está proscrito en Colombia.[248] Es de-

246 Radicación 13-262645, Delegatura para la Protección de Datos Personales, Superintendencia de Industria y Comercio.

247 En esa comunicación la Superintendencia de Industria y Comercio señala que: "el denunciante indicó también que en la actualidad su hija tiene quince (15) años y con mucho esfuerzo se ha podido recuperar de las secuelas psicológicas que tales hechos le ocasionaron; sin embargo, al consultar su nombre en el motor de búsqueda Google, su hija encontró que la decisión dictada por la Sala Penal de la Corte Suprema de Justicia, así como el concepto emitido por el Procurador Cuarto Delegado para la Casación Penal eran visibles y de fácil acceso al público".

248 "Artículo 7. Derechos de los niños, niñas y adolescentes. En el tratamiento se asegurará el respeto de los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito el tratamiento de los niños, niñas y adolescentes, salvo aquellos que sean de naturaleza pública. Es tarea del Estado y de las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos

cir, que al momento de tratar la información se haga de tal manera, que se respete el interés superior de los menores.

Cuando el artículo 7 de la Ley 1581 del 2012 consagró expresamente que *"*queda proscrito el tratamiento de datos personales de niños, niñas y adolescentes" también estableció la salvedad por la cual sí podían ser tratados: "aquellos datos que sean de naturaleza pública", por lo que la Corte Constitucional en la Sentencia C-748 del 2011 declaró la exequibilidad de la Ley 1581 del 2012, aduciendo que tal prohibición no era absoluta, ya que de serlo se estaría llegando a negar otros derechos de los menores. Por lo que concluyó que el tratamiento de datos personales de menores de 18 años, siempre y cuando fueran datos de carácter público, a fin de garantizarle a esta población de especial cuidado, derechos como la salud, la educación, la alimentación equilibrada, su nombre y nacionalidad, tener una familia y no ser separados de ella, el cuidado y amor, la educación y la cultura, la recreación y la libre expresión de su opinión, entre otros.

En consecuencia, el tratamiento de los datos personales de los menores, al margen de su naturaleza, puede ser objeto de tratamiento siempre y cuando el fin que se persiga con él responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto de sus derechos prevalentes.

Tal interpretación fue recogida por el Decreto Reglamentario 1377 del 2013, que estableció que para el tratamiento de datos personales de niños, niñas y adolescentes, excepto cuando se trate de datos de naturaleza pública, deberá cumplirse con los siguientes parámetros y requisitos: 1) que responda y respete el interés superior de los niños, niñas y adolescentes y 2) que se asegure el respeto de sus derechos fundamentales. Cumplidas las anteriores exigencias, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta su madurez, autonomía y capacidad para entender el asunto.

Adicionalmente, el literal f) del artículo 4 de la Ley 1581 del 2012 consagró el principio de circulación restringida en virtud del cual el tratamiento de información está sujeto a los límites de la naturaleza de los datos:

personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta 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 solo a los titulares o terceros autorizados conforme a la presente ley.

Por otra parte, el numeral 4 del artículo 24 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, ya había definido que, a la luz del derecho administrativo tiene **el carácter de reservado** cualquiera información o documento que involucre los "derechos a la privacidad e intimidad de las personas".

Además, el artículo 2 de la Ley 1712 del 2014 o Ley de Transparencia y del Derecho al Acceso a la Información Pública Nacional, estableció como principio de máxima publicidad universal que: "toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada **sino por disposición constitucional o legal** de conformidad con la presente ley" (Resaltado fuera del texto).

En concordancia, el literal c) del artículo 6 de la Ley de Transparencia definió como información pública clasificada:

> Aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares consagrados en el artículo 18 de esta ley.

Expuestas las anteriores consideraciones, es claro que la administración pública, aun en ejercicio de sus funciones, y pese a tener el deber de garantizar el acceso a la información pública que está depositada en sus organizaciones, debe asegurar los derechos de los titulares y el cumplimiento de todos y cada uno de los deberes que la Ley 1581 del 2012 y su Decreto Reglamentario 1377 del 2013 erigieron como principios del derecho a la protección de datos personales o derecho de *habeas data*.

Es claro que los datos ligados a una persona, por estar vinculados al derecho fundamental a la protección de datos personales, salvo los públicos, no pueden ser divulgados por la administración pública o entregados a cualquiera, sino solo por autorización expresa del titular de la información, el que este autorice o por orden legal o norma que así lo disponga.

Por lo anterior, pese a que los datos personales estén en registros públicos, documentos públicos o sentencias judiciales, su divulgación y uso estarán sometidos a los límites que se derivan de la naturaleza misma del dato, a la finalidad para la cual fueron recogidos y el uso para el cual fue autorizado su tratamiento por el titular, por lo que el tratamiento que le den las entidades públicas, –pese a tener el deber legal de incorporar y hacer uso permanente de información relativa a titulares de información–, está delimitado por la finalidad para la cual los requiera y siempre y cuando se cumplan los deberes a los que los somete la Ley de Protección de Datos Personales.

Obligaciones de la administración pública como "responsable de la información" en el tratamiento de datos personales

El concepto de "responsable de la información" tiene su origen en la denominación que el Convenio 108 de 1981[249] y la Directiva No. 46 de 1995 del Consejo de Europa, más conocida como la Directiva 95/46/CE, definieron al "responsable del tratamiento", como una figura autónoma propia del derecho a la protección de datos personales, que "solo o conjuntamente con otros determine los fines y los medios de tratamiento de los datos personales". Los elementos esenciales para distinguir al responsable del tratamiento de otros agentes, es que este determina los fines y los medios del tratamiento de datos personales, así como si entrega su tratamiento a terceros a quienes se les denomina "encargados del tratamiento", para que por orden expresa del primero trate los datos personales, de acuerdo única y exclusivamente con los fines y actividades señaladas por el primero.

En el Dictamen 1/2010 el Grupo del Artículo 29[250] se dijo que:

> El papel primero y primordial del concepto de responsable del tratamiento es determinar quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera los interesados pueden ejercer sus derechos en la práctica.

249 Convenio No. 108 del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

250 Este grupo de trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente en materia de protección de datos y de derecho a la intimidad. Sus tareas se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE.

Por su parte, en Colombia, el literal e) del artículo 3 de la Ley 1581 del 2012 definió al responsable del tratamiento como aquella "(p)ersona 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".

Al respecto la Corte Constitucional, en la Sentencia C-748 del 2011, señaló lo siguiente:

> En el proyecto de ley estatutaria el legislador enlistó en preceptos separados los deberes de los responsables y de los encargados del tratamiento, deberes que, en términos generales, buscan garantizar el pleno ejercicio del derecho al *habeas data* por parte de los titulares, así como los principios de la administración de datos personales.

Los deberes que puso la norma en cabeza del responsable y del encargado del tratamiento buscan que se garantice, prima facie, el ámbito de protección del derecho de *habeas data*, en la medida en que todos los preceptos y principios en los que se fundamenta el derecho a la protección de los datos personales son oponibles a todos los sujetos involucrados en los procesos de recolección, uso, tratamiento y circulación de datos, independientemente de la posición que ocupen para el efecto.

En la Sentencia C-748 del 2011, la Corte Constitucional realizó el estudio de constitucionalidad del proyecto que posteriormente se denominó Ley 1581 del 2012.

La citada sentencia precisó al respecto:

> En relación con el **responsable del tratamiento**, es decir, aquel que define los fines y medios esenciales para el tratamiento del dato, incluidos quienes fungen como fuente y usuario, se establecen deberes que responden a los principios de la administración de datos y a los derechos –intimidad y *habeas data*– del titular del dato personal.
>
> Específicamente se dispone que son deberes de esta parte de la relación:
>
> 1. Solicitar y conservar **la autorización** para el tratamiento del dato –en los términos descritos antes–, lo que se ajusta plenamente al principio de libertad y consentimiento expreso del titular del dato.
>
> 2. Informar al titular sobre la **finalidad** de esa autorización y actuar en consecuencia; por tanto, el responsable no puede conducirse por fuera de los lineamientos de la autorización, lo que significa que, por ejemplo, no puede **suministrar** al encargado del tratamiento más datos de los que fueron objeto de autorización,

> ni puede someterlos a un tratamiento con finalidades diferentes a las informadas […].
>
> 3. Adoptar las medidas para garantizar la seguridad del dato, a efectos de que no se pierda, no se adultere, no se utilice o acceda por fuera de la autorización. Esto es desarrollado en el literal d) en concordancia con el principio de seguridad en la transferencia del dato.

Debe entenderse que la autorización que otorga el titular del dato para que se realice el uso de su información ceñido a la finalidad que le fue informada, debe ser guardada como prueba de su otorgamiento en medio físico, magnético o digital, así como que la información recolectada debe ser guardada bajo medidas de seguridad suficientes que minimicen el riesgo de exposición o pérdida.

El artículo 17 de la Ley 1581 del 2012 consagró los deberes de quien haga la recolección y el tratamiento de los datos personales y decida sobre su uso y disposición final, es decir, el responsable de la información, tal como se enuncia a continuación:

> 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:
>
> 1. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de *habeas data.*
>
> 2. Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el titular.
>
> 3. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.
>
> 4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
>
> 5. Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
>
> 6. Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya

suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

7. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

8. Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

9. Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

10. Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

11. 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.

12. Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

13. Informar a solicitud del titular sobre el uso dado a sus datos.

14. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

15. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Si bien los deberes están enlistados en el citado artículo de manera taxativa, también están ligados de manera tal a los principios que regulan la actividad, que su estudio debe realizarse de manera conjunta, ya que la responsabilidad en su cumplimiento solo podrá alcanzarse al garantizar la aplicación de los principios en beneficio y garantía del derecho fundamental de los titulares.

Los deberes fueron establecidos sin distingo entre si el responsable era una persona jurídica de derecho privado o de derecho público, por lo que su

exigibilidad se predicará de todos aquellos que desarrollen el rol de responsable del tratamiento, aunque las consecuencia que acarrea la responsabilidad sí variará dependiendo de la categoría del responsable.

Las personas naturales y de derecho privado que actúen como responsables del tratamiento estarán sujetas al procedimiento establecido en los artículos 22 al 24 del Capítulo 2 de la Ley 1581 del 2012: quienes vulneren el derecho y la situación sea puesta en conocimiento de la autoridad de control, están sometidos a un procedimiento administrativo que desembocará en la expedición de una orden de actualización, rectificación y eliminación de los datos personales.

También, el ente de control, es decir, la Superintendencia de Industria y Comercio por medio de la Delegatura para la Protección de los Datos Personales, podrá iniciar una investigación administrativa de carácter sancionatorio, que podrá finalizar además de una orden de actualización, rectificación y eliminación, con la imposición de una multa personal o institucional hasta de dos mil (2.000) salarios mínimos mensuales legales vigentes. También podrá ordenarse la suspensión de las actividades relacionadas con el tratamiento de los datos hasta por seis (6) meses, el cierre temporal de las operaciones relacionadas con el tratamiento o el cierre definitivo de la actividad por medio de la cual se efectuaba el tratamiento de datos personales de categoría sensible.[251]

Aunque la Ley 1581 del 2012 no estableció el procedimiento para la aplicación de las sanciones contempladas en el artículo 23, este se rige por el Código Contencioso Administrativo y de Procedimiento Administrativo, que define las etapas en las que a los investigados se les garantiza el derecho de defensa y contradicción y de debido proceso.

Así las cosas, la potestad sancionatoria de la administración pública queda sujeta a los principios que limitan su actuación y configuran el derecho sancionador, como el debido proceso, el principio de legalidad, el principio de tipicidad y los criterios de proporcionalidad y razonabilidad. Los dos últimos le permiten al órgano sancionador tener un marco de referencia para la determinación de la sanción, en tanto que dichos criterios deben estar presentes entre la conducta o hecho que se sanciona y la penalidad que pueda imponerse. El artículo 24 de la Ley General de Protección de Datos Personales estableció los criterios de graduación

251 Artículo 23 de la Ley 1581 del 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" (Bogotá: *Diario Oficial* No. 48587 de octubre 18 del 2012).

de las sanciones, teniendo como juicio de valoración, la dimensión del daño o peligro el interés jurídico tutelado, el beneficio económico obtenido por el infractor y la reincidencia de la infracción.

El artículo 23 de la Ley 1581 de 2012 es claro al enunciar cuáles serían las consecuencias de que las personas naturales y privadas efectúen el tratamiento de datos personales sin tener en cuenta las obligaciones que se derivan de su actividad como responsables. Sin embargo, el mismo artículo 23 en su parágrafo introdujo una variable para los responsables del tratamiento que sean personas jurídicas de derecho público:

Las sanciones indicadas en el presente artículo solo aplican para las personas de naturaleza privada. En el evento en que la Superintendencia de Industria y Comercio advierta el 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.

Lo anterior implica que el tratamiento de datos que no se ajuste a lo establecido en la norma será objeto de revisión del órgano de control de la actividad administrativa como la Procuraduría General de la Nación. En efecto, la inobservancia de los deberes y el respeto del derecho de *habeas data* de los titulares, no acarreará la imposición de multas de carácter pecuniario o la suspensión o cierre de la base de datos, sino consecuencias legales según lo establece la Ley 734 del 2002 o Código Único Disciplinario.

Pese a ello, nada dice la norma sobre la facultad de órdenes de actualización, eliminación o rectificación de los datos personales solicitados por los titulares ante el responsable del dato. Una cosa diferente a la imposición de sanciones es la garantía del derecho a conocer, actualizar y rectificar la información. Por eso ante la falta de claridad de la norma, es posible que un titular de información, cuyo dato no se encuentre actualizado en una base de datos en manos de un ente público, esté en capacidad de solicitar la garantía de su derecho fundamental ante la autoridad de control.

Dada la reciente expedición de la norma y la lenta concientización de los titulares sobre el derecho que tienen a que se garantice su *habeas data*, no existe, a la fecha, jurisprudencia que dé pautas sobre la posibilidad de que los titulares puedan exigir al órgano de control la revisión de una decisión o la inobservancia que conduzca a que entidades estatales se nieguen a garantizar el derecho

fundamental. En el estudio de constitucionalidad del proyecto de ley la Corte Constitucional tampoco se pronunció a propósito de este tema, por lo que, siendo la Superintendencia de Industria y Comercio, la autoridad de protección de datos,[252] nada hace pensar que los titulares no puedan solicitar que se haga cumplir su derecho a conocer, actualizar y rectificar los datos personales que de ellos se encuentren en bases de datos de la administración pública.

Si bien la administración pública, actuando como responsable del tratamiento, no puede ser objeto de imposición de multas o sanciones, sí está obligada a aplicar dentro de su organización los deberes que como responsable le impone la ley, por lo que debe, –en los casos en que recoja datos personales diferentes a los que requiere en ejercicio de su función o actividad misional, así como para ceder o entregar a terceros dicha información–, solicitar autorización de los titulares, informando la finalidad de su uso; igualmente, debe guardar la autorización, –como prueba de su otorgamiento en medio físico, magnético o digital–, bajo medidas de seguridad suficientes que minimicen el riesgo de exposición o pérdida.

Aunque estos son los derroteros sobre los cuales se cimienta el tratamiento de datos personales, la norma fue expresa en enumerar en el artículo 17 una serie de deberes predicables y exigibles a los deberes del responsable.

De la lectura integral de tales deberes, salta a la vista el primero y más general, pero a la vez más relevante de los que tienen los responsables: garantizar el pleno y efectivo ejercicio del derecho de *habeas data,* que engloba la totalidad de los postulados y los principios que regulan el derecho a la protección de los datos personales. Si se vulnera alguno de ellos, obviamente se está afectando este. Sin embargo, resulta de vital importancia en la legislación la existencia amplia de tal deber, ya que con el avance de la tecnología y el creciente desarrollo de posibilidades de acceso, uso y disposición de información por medios no tradicionales, así como las complejas formas de relacionarse los titulares de la información,

252 "Artículo 19. Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, por medio de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Parágrafo 1°. El Gobierno nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos. Parágrafo 2°. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 del 2008 se sujetará a lo previsto en dicha norma".

porque se consagra como deber, la garantía plena y el ejercicio efectivo del derecho de *habeas data*. También es importante tal deber, en la medida en que está directamente relacionado con el ejercicio del derecho a presentar peticiones, quejas, consultas y reclamos a los responsables y encargados del tratamiento.

Los artículos 14 y 15 de la Ley 1581 del 2012 consagraron el derecho de los titulares de la información a presentar consultas y reclamos, ya sea a título personal o mediante los causahabientes, ante entidades de derecho privado o público.

Los términos en que deben ser tramitadas y respondidas dichas peticiones es de diez (10) días en caso de que se trate de consultas hábiles, prorrogables hasta por cinco (5) días más, siempre y cuando se le informe al solicitante de dicha prórroga. Por su parte, los reclamos, que versen sobre actualización, corrección y eliminación de los datos consignados en las bases de datos del responsable, así como las solicitudes de revocatoria de la autorización para su tratamiento deben ser atendidas dentro del plazo de quince (15) días hábiles.

El procedimiento de consulta y reclamación está construido de manera armónica con lo establecido en el derecho de petición incluido en el artículo 23 de la Constitución Política de 1991. Por lo que su ejercicio está cimentado en el derecho constitucional fundamental que tiene toda persona a presentar peticiones respetuosas ante las autoridades y a obtener pronta solución, regulado de manera general por el Título II de la Ley 1437 del 2011[253] y de manera especial, en materia de protección de datos personales, por los artículos 14 y 15 de la Ley 1581 del 2012.

Al respecto, mediante sentencia C-748 del 2011, la Corte Constitucional manifestó lo siguiente:

> Esta norma hace una regulación típica del derecho de petición que consagra el artículo 23 de la Constitución, que en el caso en estudio se traduce en el derecho que tienen los titulares del *habeas data* o sus causahabientes para presentar ante los bancos de datos que manejen las autoridades públicas o privadas, peticiones para establecer que (sic) información o datos poseen sobre ellos y los términos para atender las consultas. El artículo 15 por su parte, regula los reclamos que puede efectuar el titular del dato o sus causahabientes al responsable o encargado del tratamiento con el fin de

253 Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Título II - Artículos 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32 y 33 de la Ley 1437 del 2011 declarados inexequibles con efecto diferido hasta el 31 de diciembre del 2014. Corte Constitucional, *Sentencia C-818 del 10 de noviembre del 2011*, M. P. Jorge Ignacio Pretelt Chaljub

corregir, actualizar o suprimir la información contenida en la base de datos o cuando se considere que se ha incumplido con cualquiera de los deberes que le corresponde.

Por lo anterior, es válido señalar que los mecanismos establecidos en los artículos 14 y 15 de la Ley 1581 del 2012, al estar fundamentados en el derecho de petición, son una de las herramientas con las que cuentan los titulares de la información para hacer efectivo su derecho a la protección de los datos personales, en la medida en que pueden presentar solicitudes de información o un reclamo o queja sobre la manera como se está tratando su información personal.

De acuerdo con la lista de deberes de la administración pública como responsable del tratamiento, quizás la más importante sea garantizar que la información que posee en sus bases de datos sea veraz, completa, exacta, actualizada, comprobable y comprensible, ya que este es el núcleo central del derecho de *habeas data*. Por lo que el establecer mecanismos de coordinación dentro de sus dependencias resulta trascendental, no solo para cumplir tal deber, sino para desempeñar su labor a la altura de las exigencias derivadas de poseer una administración que cada vez más se comunica electrónicamente entre sus distintos órganos y con el ciudadano.

La planeación estratégica de la organización para la implementación de la política de tratamiento de datos personales

La existencia de los deberes que debe cumplir la administración pública, como responsable del tratamiento, no solo soporta lo exigido en los artículos 14, 15 y 17 de la Ley 1581 del 2012, sino que para poder cumplir con muchos de ellos, tanto sociedades privadas como entidades públicas debieron realizaron una serie de análisis y diagnósticos que les permitieran establecer qué bases de datos poseían, cuáles datos estaban allí incorporados, cuál era la finalidad de su utilización, si realmente estaban haciendo uso de ellos, establecer si requerían la autorización de los titulares, si contaban con ellas y si poseían dentro de sus organizaciones las medidas de seguridad necesarias para su adecuado tratamiento y seguridad.

El 27 de junio del 2013, con la entrada en vigencia del Decreto Reglamentario 1377 del 2013, los responsables del tratamiento de datos personales tuvieron que implementar nuevas herramientas de tratamiento de la información y un aviso de

privacidad[254] accesible a todos los titulares para que conocieran los mecanismos para hacer efectivos sus derechos.

Con la existencia de una política de tratamiento de la información por cada uno de los responsables de tratamiento, el legislador buscó que los titulares conocieran los responsables, su ubicación y los medios de comunicación a través de los cuales se pudieran contactar con ellos, el tratamiento al que estaban sometidos los datos, así como la finalidad para la que eran tratados. También les permitió aclarar los derechos que les asisten ante el responsable de sus datos personales y los procedimientos establecidos por cada uno de los responsables para que el titular ejerza sus derechos.[255]

Adicionalmente, los artículos 2.2.2.25.3.2 y 2.2.2.25.3.4 del citado Decreto[256] establecieron los parámetros que debían cumplir los avisos de privacidad, como mecanismo más corto y de práctica visualización por parte del responsable para que los titulares conocieran sumariamente la información que reposa en las políticas de tratamiento de datos de los responsables.

Pero sin duda, la obligación que trae consigo una mayor carga para la administración pública es cumplir a cabalidad con el deber de seguridad de la información. Esto implica implementar procedimientos y medidas técnicas y del recurso humano, en la medida en que involucra la capacitación del personal, la creación

254 "Artículo 3. Definiciones. Además delas definiciones establecidas en el artículo 3 de la Ley 1581 del 2012, para efectos del presente decreto se entenderá por: […] 1. Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

255 Artículo 2.2.2.25.3.2 del Decreto 1074 del 2015, que derogó el artículo 13 del Decreto 1377 del 2013.

256 Decreto 1074 del 2015. "Artículo 14. Aviso de Privacidad. En los casos en los que no sea posible poner a disposición del titular las políticas de tratamiento de la información, los responsables deberán informar por medio de un aviso de privacidad al titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales.

Artículo 15. Contenido mínimo del aviso de privacidad. El aviso de privacidad, como mínimo, deberá contener la siguiente información: 1) nombre o razón social y datos de contacto del responsable del tratamiento; 2) el Tratamiento al cual serán sometidos los datos y la finalidad del mismo; 3) los derechos que le asisten al titular; 4) los mecanismos dispuestos por el responsable para que el titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el aviso de privacidad correspondiente. En todos los casos, debe informar al titular cómo acceder o consultar la política de tratamiento de información. No obstante lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos".

En todo caso, la divulgación del aviso de privacidad no eximirá al responsable de la obligación de dar a conocer a los titulares la política de tratamiento de la información, de conformidad con lo establecido en este decreto.

de perfiles y la asignación de funciones claramente establecidas dentro de la organización, que permitan asumir e indilgar responsabilidades en su interior.

Dada la falta de versatilidad organizacional de la administración pública, tanto en la creación y eliminación de cargos, así como en la asignación de roles y responsabilidades, la implementación de una estructura coherente que garantice el ejercicio del derecho a la protección de datos personales, les impone el reto de establecer y consolidar el inventario de bases de datos personales que posea la entidad, para poder fijar prioridades, establecer roles y asignar funciones dentro de su organización, por medio de los cuales pueda dar respuesta a entidades, autoridades de vigilancia y a los propios ciudadanos.

Así mismo, ajustar los manuales de funciones, a fin de establecer responsables y posteriormente demostrar la diligencia o no, ante los entes de vigilancia, que como se dijo, en materia de protección de datos personales le corresponde a la Procuraduría General de la Nación, el estudio del cumplimiento de los deberes como responsables de las diferentes entidades que conforman la administración pública. Ya que de otra forma, toda la responsabilidad recaería sobre los representantes legales de las entidades.

Por otro lado, la puesta en marcha de la política de tratamiento y aviso de privacidad genera la implementación de medidas técnicamente controlables sobre el acceso a la información, ya que no todas las áreas de la administración pública pueden o deben tener acceso a la información personal y a incorporarlas para la actualización, corrección y en caso de que proceda, la eliminación de la información allí depositada. Todo esto requiere del desarrollo, planeación y adquisición de estrategias y herramientas tecnológicas.

Por lo anterior, con la entrada en vigencia de la Ley 1581 del 2012 y sus decretos reglamentarios, la administración pública debe cumplir con todas y cada una de las exigencias que se deriven de la ley. Además, está inmersa en una serie de obligaciones que permitan la adecuación administrativa, tecnológica y la capacitación humana a fin de poder probar que puede actuar como responsable del tratamiento de los datos personales.

Sin embargo, a dos años de haber entrado en vigencia de la Ley General de Protección de Datos Personales, de acuerdo con estudios preliminares realizados por la Dirección Nacional de Planeación (DNP), se encuentra que en el ámbito nacional, los órganos que conforman la Administración Pública, no están

preparados para cumplir con las obligaciones que se derivan de su actividad como responsables del tratamiento, ya que no se han establecido criterios de unificación y de buenas prácticas que garanticen su cumplimiento. Por lo que el reto es grande y las consecuencias inesperadas, ante el desconocimiento de la administración pública de los deberes que le atañen en materia de protección de datos personales.

La administración pública como autoridad de control

El artículo 19 de la Ley 1581 del 2012 estableció que la Superintendencia de Industria y Comercio, por medio de la Delegatura para la Protección de Datos Personales, ejercerá la vigilancia con el fin de garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en esa ley.

La Resolución 4886 del 23 de diciembre del 2011 reestructuró la Superintendencia de Industria y Comercio y le atribuyó funciones de vigilancia y control que empezó a desarrollar formalmente, a través de la Delegatura para la Protección de Datos Personales, por lo que a partir del 2012 esa Superintendencia ha ejercido las funciones legalmente asignadas por las Leyes 1266 del 2008 y 1581 del 2012, como autoridad de protección de datos personales.

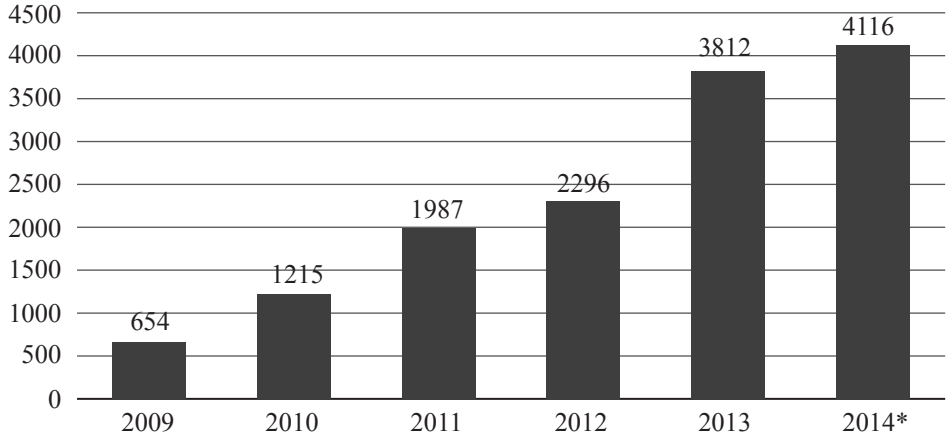
Sin embargo, desde el año 2008, cuando la Ley 1266 del 2008 le otorgó las facultades de vigilancia y control de los operadores, fuentes y usuarios de información de las bases de datos con información financiera, comercial y crediticia, la Superintendencia a través de un grupo de trabajo realizó las primeras investigaciones al respecto.

De acuerdo con esta incipiente inserción dentro de la organización administrativa de la Superintendencia, empiezan a presentarse a partir de enero del 2009 las primeras quejas en materia de *habeas data* financiera.

Si bien el aumento del número de quejas ha sido considerable, sigue siendo un porcentaje relativamente bajo para la totalidad de la población que puede ver vulnerado su derecho de *habeas data*.

Según las estadísticas de la Superintendencia en su informe anual de rendición de cuentas del 2014, el volumen de quejas presentadas ha sido el siguiente:

Figura 1. Volumen de quejas



* Cifras a 22 de octubre del 2014.

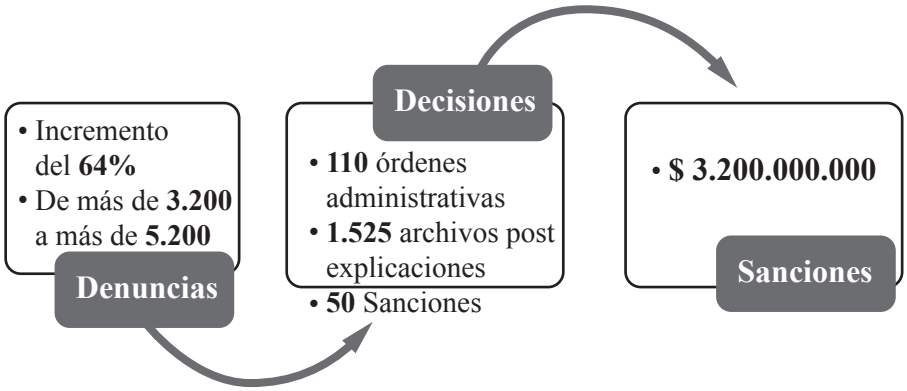
Fuente: Superintendencia de Industria y Comercio. Informe de gestión a octubre del 2014

Como se observa, las quejas presentadas para el 2014 han alcanzado un volumen significativo, lo que implica que cada día más ciudadanos conocen su derecho y que la entidad de control ha visto de manera ascendente cómo se requiere de mayor capacidad organizacional para cubrir la demanda.

En virtud de este volumen, y consciente de la entrada en vigencia de la Ley General de Protección de Datos Personales, el ente de control ha visto un crecimiento del 64 % en el volumen de las quejas presentadas y, por tanto, un aumento en los actos que profiere, tanto en materia de órdenes de actualización, corrección y eliminación de los datos personales, como de investigaciones administrativas sancionatorias, tal como se muestra en el cuadro de rendición de cuentas publicado por la Superintendencia de Industria y Comercio.

Tal volumen de quejas tiene su origen principalmente en discusiones sobre la veracidad de la información incorporada en las bases de datos, la indebida atención de las consultas, quejas y reclamos y, en menor proporción, la falta de autorización para el tratamiento de los datos personales.

Figura 2. Delegatura para la protección de datos personales.



Fuente: Superintendencia de Industria y Comercio

Además de hacer investigaciones de oficio o a petición del interesado otra de las funciones asignada a la autoridad de control, según el artículo 21 de la Ley 1581 del 2012, es promover y divulgar los derechos de los titulares en relación con el tratamiento de sus datos personales. Aunque esta actividad es el eje fundamental para que los ciudadanos conozcan sus derechos también trae implicaciones organizacionales, que obligan al ente de control a encontrar mecanismos eficientes para garantizar la vigilancia del tratamiento de los datos personales.

El reto de la Superintendencia es grande, dados los desafíos tecnológicos derivados del tratamiento de datos con mecanismos sistematizados y que permiten una fácil volatilidad de la información, por lo que los principales guardianes de la información personales son los propios titulares de la información.

Adicionalmente, los retos que le deja planteada la norma, sobre la creación de reglamentación enfocada a la regulación en materia de tratamiento de datos de menores de edad, la transferencia internacional de datos y los procesos de certificación en manos de terceros certificadores, demuestran que en materia de vigilancia y control, la Superintendencia tiene un gran desafío y que Colombia está hasta ahora empezando a comprender el alcance y dimensión del ejercicio del derecho a la protección de datos personales y las consecuencias y responsabilidades que le atañen a la administración pública.

Conclusiones

El ámbito de aplicación de la Ley 1581 del 2012 o Ley General de Protección de Datos Personales, enmarca tanto la actividad que desarrolla la administración pública como responsable del tratamiento de datos personales que posee en razón de las funciones que desempeña, así como las responsabilidades que se derivan de la función de vigilancia y control que en materia de protección de datos personales le asignó la ley.

Esta doble función incluye diferentes responsabilidades y consecuencias, por lo que actuando como responsable del tratamiento, todas y cada una de las entidades nacionales, departamentales y regionales, es decir, las entidades de derecho público están obligadas a cumplir con los deberes que la ley les impuso a quienes traten datos personales y decidan sobre su recolección, uso y disposición final.

Sin embargo, por existir normas que les imponen responsabilidades a las entidades de derecho público, quienes se encarguen del tratamiento que se haga de los datos personales que se recojan, en virtud de una norma, no están obligados a obtener la autorización de los titulares para ejercer su actividad, de acuerdo con los fines propios de la entidad, aunque si están obligados a garantizar todos y cada uno de los derechos con que la ley General de Protección de Datos Personales busca amparar el derecho de *habeas data*.

El cumplimiento de los deberes exigidos a los responsables del tratamiento conlleva una carga; sin embargo, en el caso de las entidades de derecho púbico, el ajuste y cumplimiento de todas y cada una de las obligaciones, significa un esfuerzo y una planeación estratégica dentro cada entidad, ya que se debe depurar y reorganizar la información.

Tal deber implica capacitación humana, gestión administrativa e innovación tecnológica. Todo ello para que los funcionarios puedan desempeñar su función a cabalidad.

Los estudios preliminares realizados por el Departamento Nacional de Planeación, dan cuenta de que las entidades del orden nacional no han implementado eficientemente una estrategia que permita garantizar el cumplimiento de la Ley 1581 del 2012, por lo que pese a estar a dos años de la entrada en vigencia de la ley General de Protección de Datos Personales, la correcta puesta en marcha de los procedimientos que la Ley impone a los responsables del tratamiento, aún es

escueta, pese a la responsabilidad disciplinaria que se desprende del desconocimiento e incumplimiento del régimen de protección de datos personales.

Por otra parte, la administración pública, a través de la Superintendencia de Industria y Comercio, y en especial a través de la Delegatura para la Protección de Datos Personales ejerce la función de autoridad de vigilancia y control, mediante la cual desarrolla dos funcione: hacer investigaciones para ordenar a los responsables del tratamiento que actualicen, corrijan y eliminen los datos personales de las bases de datos que posee y realizar investigaciones administrativas de carácter sancionatorio, de acuerdo con lo establecido por el procedimiento sancionatorio consagrado en los Códigos de Procedimiento Administrativo y de lo Contencioso Administrativo.

El crecimiento permanente del volumen de quejas presentadas, así como la mayor divulgación de la existencia del derecho le implica a la autoridad de control el desarrollo de estrategias más eficientes para ejercer la actividad de vigilancia, así como un crecimiento de sus recursos humanos, por lo que se requiere fortalecer la recientemente creada autoridad de vigilancia.

A dos años de entrada en vigencia de la Ley General Protección de Datos Personales, no se han reglamentado materias como el tratamiento de datos personales de menores de edad, las transferencias internacionales de datos ni la creación de terceras entidades certificadores de buenas prácticas en el tratamiento de datos, por lo que se puede aseverar que, si bien el esfuerzo como autoridad en materia de protección ha sido importante, la autoridad de control como órgano de la administración pública se encuentra aún en una etapa de desarrollo incipiente.