LA INCIDENCIA DEL MODELO ESPAÑOL EN EL REGISTRO NACIONAL DE BASES DE DATOS COLOMBIANO COMO HERRAMIENTA DE SUPERVISIÓN Y CONTROL

4

Claudia Bibiana García Vargas

Introducción

El presente trabajo investigativo se centra en el estudio de los requerimientos de información del registro de bases de datos español y los requerimientos de información que se han proyectado para el registro de bases colombiano, y el marco legal dentro del que se han gestado dichos requerimientos dentro de cada país, con el fin de ofrecer una visión general del estado actual de las herramientas de supervisión y control que España ha desarrollado como estrategia de vigilancia en el tratamiento de los datos personales, y cómo ese mecanismo ha influido en el proceso de supervisión y control del tratamiento de datos personales que se ha implementado en Colombia a lo largo de los últimos dos años.

Dado en que en Colombia solo hasta marzo de 2014 se dio a conocer el proyecto de reglamentación e implementación del Registro Nacional de Bases de Datos (RNBD), creado por la Ley 1581 de 2012, o Ley de Protección de Datos Personales, el estudio del RNBD se adelantará como una aproximación al mecanismo de supervisión y control con base en estudios preliminares del proyecto de

decreto y desde las obligaciones planteadas desde la misma Ley de Protección de Datos de Colombia.

En igual sentido, el reto que se plantea en el presente trabajo es determinar si, pese a que Colombia ha tendido hacia la estrategia europea en materia de protección de datos personales (más concretamente, la española), tal proceso, así como la implementación de la herramienta de un registro general o nacional de bases de datos, se adecúa a la realidad colombiana y a los nuevos deberes creados por la Ley 1581 de 2012.

Este cuestionamiento particular no está desligado del debate global, ya que la interacción entre naciones ha generado, a través del comercio y de las nuevas tecnologías, que los procedimientos de supervisión, vigilancia y control puedan llegar a volverse obsoletos antes de tiempo.

Pero más allá del cuestionamiento sobre si la estrategia española es la más adecuada, la implementación en Colombia de medidas concordantes con el desarrollo europeo en materia de protección de datos genera un interés importante para Colombia, dada la ventaja de ser considerado un país con un nivel apropiado en el tratamiento de datos personales, así como la intención del legislador de buscar que Colombia se mantenga en concordancia con estándares internacionales en la materia. En consecuencia, la presente investigación busca dar a conocer el funcionamiento del Registro General de Protección de Datos (RGPD) español y poner de presente los requerimientos y las condiciones en los que se está implementando la puesta en marcha del RNBD colombiano, como herramienta fundamental para el ejercicio de las actividades de supervisión y control otorgadas a la Superintendencia de Industria y Comercio (SIC), como autoridad de protección de datos en Colombia.

El caso español: el Registro General de Protección de Datos (RGPD)

A través del presente capítulo, se busca brindar una breve aproximación a cuáles son los antecedentes de creación del RGPD en España, así como saber quién es la autoridad de protección de datos personales en España y cuál ha sido el desempeño del RGPD en el proceso de supervisión de las bases de datos sujetas a tratamiento, de manera tal que, una vez revisados los asuntos que la componen, se pueda conocer su funcionamiento y vislumbrar cuál ha sido la influencia española

en el proceso de vigilancia y supervisión del tratamiento de datos personales en Colombia.

Antecedentes de la creación del Registro General de Bases de Datos

El modelo de protección de datos en España está fundamentado en el modelo comunitario europeo, el cual, mediante la aprobación el Convenio No. 108 del Consejo de Europa de 1981, sobre la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal, y que cimentó las bases para el ejercicio de este derecho y dio origen a la primera norma europea que marcó las pautas del modelo común de protección de datos.

A través del citado Convenio, se buscó el amparo de los derechos y las libertades fundamentales relativas a la vida privada y a la circulación de los datos personales en los países de la Comunidad Europea de Naciones, dada la facilidad de que la misma información sea tratada de manera automatizada a través de las fronteras locales y mundiales.

La estrategia usada por el Consejo de Europa se basó en que cada país miembro de la Unión Europea (UE) lograse garantizar la protección de los datos personales (físicas o naturales) en su territorio, independientemente de la nacionalidad o del lugar de residencia de las personas. Con esa perspectiva, el Capítulo II del citado convenio sintetizó los principios básicos sobre los cuales se fundamenta el derecho a la protección de los datos personales en los 28 países que constituyen la Comunidad Europea.

Por lo anterior, a la luz del Convenio 108 de 1981, los mencionados principios incluyen: (i) el compromiso de las partes[149]; (ii) el principio de calidad de los

149 Consejo de Europa, *Convenio 108 de 1981*, artículo 4. Compromisos de las Partes.

1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte.

datos[150]; (iii) la categoría de datos especiales[151]; (iv) la seguridad de los datos[152], y (v) el principio de las llamadas *garantías complementarias para la persona concernida*. Fueron, precisamente, estos principios los que sirvieron como derroteros por seguir y como base para el desarrollo, en cada país de la Unión Europea (UE), de los fundamentos para la garantía del derecho a la protección de datos personales.

Posteriormente, con la aprobación de la Directiva 46 de 1995 del Parlamento y del Consejo de 24 de octubre de 1995, conocida como la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se sientan las bases para lograr la coordinación de las legislaciones nacionales aplicables en materia de protección de datos, en pro de garantizar la libre circulación de tales datos entre los Estados miembros de la UE.

A través de la mencionada directiva, se consagraron expresamente los principios, los requisitos procedimentales, la existencia de una autoridad de protección para cada país y la creación un registro de las bases de datos; todos ellos, elementos básicos para que se desarrollaran en cada país los requisitos mínimos para la implementación de un sistema homogéneo y articulado para la adecuada protección de datos personales en la UE.

Inicialmente, estos son los principios que cada legislación debió desarrollar dentro de sus propias legislaciones para garantizar las normas rectoras que rigen el tratamiento de los datos personales en Europa. Sin embargo, tales principios, al ser abordados con la perspectiva actual de cada país, y tomando en cuenta el desarrollo que en el ámbito comunitario se ha tenido frente a los principios que rigen la actividad, hoy día se puede hablar de que los principios del derecho a

150 Ibid., artículo 5: "La calidad de los datos personales objeto de tratamiento automatizado se obtendrán de manera leal y legítimamente; serán adecuados, pertinentes y no excesivos en relación con la finalidad que se hayan registrado; deberán ser exactos y puestos al día, legítimos para las cuales se hayan registrado. Igualmente se conservarán de una forma que permita la identificación de la persona por un periodo máximo de acuerdo con la finalidad".

151 Ibid., artículo 6: "Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales".

152 Ibid., artículo 7: "Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

la protección de datos en Europa son: (i) principio de lealtad; (ii) principio de exactitud; (iii) principio finalista; (iv) principio de pertinencia; (v) principio de utilización no abusiva; (vi) principio del derecho al olvido; (vii) principio de publicidad; (viii) principio de acceso individual; (ix) principio de seguridad, y (x) principio de prohibición de tratamiento automático de datos que revelen el origen racial, las opiniones políticas y las convicciones religiosas o de otro tipo, o los datos relativos a la salud o a la propia vida sexual, a menos que el derecho interno prevea las garantías adecuadas[153].

Por su parte, en España, con la expedición de la Ley Orgánica 15 de 1999 de Protección de Datos, y conocida como la LOPD, se traspusieron en todo ese país los preceptos establecidos por la Directiva 95/46 del Parlamento Europeo y el Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. Pese a existir desde 1999, la LOPD solo fue reglamentada hasta 2007, con la expedición del Real Decreto 1720 del 21 de diciembre del citado año, y en adelante, Reglamento de la LOPD, o RLOPD.

Ahora bien, de acuerdo con los principios traspuestos de la normatividad Europea, la norma española estableció como derrotero en la protección de los datos personales: que estos deben tratarse de manera leal y lícita; que deben recogerse con fines determinados, explícitos y legítimos, y que deben ser adecuados, pertinentes y no excesivos en relación con el ámbito ni los fines para los que se han recogido. Así mismo, estableció que los datos deben ser exactos y mantenerse actualizados, de manera que correspondan con veracidad a la situación actual de su titular.

Los *responsables*[154], por su parte, deben atender a los *interesados*[155] que soliciten el acceso a sus datos personales, los cuales solo deben ser conservados por

153 Elisenda Bru Cuadrada, "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad". *Derecho y Política*. 5 (2007): 78-92.

154 Congreso de los Diputados, *Ley Orgánica 15 de 1999*, "De Protección de Datos de Carácter Personal" (Madrid: *BOE* No. 298, 14 de diciembre de 1999), artículo 3, literal d): Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

155 Ibid., artículo 3, literal e): "Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

el tiempo necesario para que se cumpla la finalidad para la cual fueron recogidos, por lo que deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes al fin con el que se obtuvieron.

En concordancia con lo anterior, la norma impuso el deber de que quien recoja datos personales y haga tratamiento de ellos tiene que adoptar todas las medidas necesarias para garantizar la seguridad de dichos datos e impedir cualquier alteración, pérdida, tratamiento o acceso no autorizado.

La LOPD les reconoce específicamente a los ciudadanos los siguientes derechos en materia de protección de datos:

a. Derecho de información en la recogida de datos.
b. Derecho de consulta al RGPD.
c. Derecho de acceso[156].
d. Derecho de rectificación y cancelación[157].
e. Derecho de oposición[158].

Ahora bien, a partir del artículo 18 de la Directiva 95/46 se creó la obligación de contar con registros generales de las bases de datos personales que sean objeto de tratamiento en el espacio europeo. Dicha obligación está íntimamente ligada con el principio de publicidad en el tratamiento de los datos personales, consagrado, a su vez, en el artículo 21 de la citada Directiva Europea, el cual conminó a los Estados miembros a que la autoridad de control fuera la encargada de llevar el registro de las bases de datos. El ejercicio del derecho de acceso al Registro

156 Ibid., artículo 15: "Derecho de acceso: El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".

157 Ibid., artículo16: "Derecho de rectificación y cancelación.

El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación".

158 Ibid., artículo 34. "El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo".

General de Bases de Datos fue concebido para ser consultado gratuitamente por el Titular de la información y para que permitiera el acceso a la información mínima sobre quienes están adelantando tratamiento de datos personales.

Con el establecimiento del principio de publicidad del derecho comunitario como premisa fundamental del derecho a la protección de datos, la legislación española incorporó el *derecho de consulta*, como un derecho derivado del principio de publicidad, consagrado en el artículo 14 de la LOPD, y en el cual se estableció lo siguiente:

> Artículo 14. Derecho de consulta al registro general de protección de datos.
>
> Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Como se puede observar, con base en el derecho a consulta, se habilita a cualquier persona para conocer, de forma pública y gratuita, la existencia de tratamientos de datos de carácter personal, así como los fines para los cuales fue recogida la información y los responsables de su tratamiento. A través del literal j) del numeral 1º del artículo 37 de la LOPD, se estableció como deber de la Agencia Española de Protección de Datos (AEPD) velar por la publicidad de la existencia de las bases de datos de carácter personal, por lo que se reglamentó como obligación el registrar las bases de datos personales existentes en España.

Con la implementación del RGPD en aplicación del derecho de consulta, se garantizó el derecho de los titulares a conocer la información sobre las bases de datos que existen en España, así como que con ello se facilitó el acceso de los titulares a saber quién posee sus datos personales y cuál es la información de contacto de los responsables y la finalidad de las mismas, para así facilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los titulares.

De acuerdo con lo enunciado, y en concordancia con la LOPD[159], es deber de las personas de derecho público y de las de derecho privado registrar en el RGPD las bases de datos que posean, siempre y cuando estas incluyan datos de carácter personal en soporte sistematizado o manual que los haga susceptibles

159 Ibid., artículo 26.

de tratamiento, con las excepciones previstas por la norma, según la titularidad de quien sea su responsable. Según lo dispuesto por el artículo 39 de la LOPD, son objeto de inscripción en el RGPD:

1. Las bases de datos de las administraciones públicas (titularidad pública).
2. Las bases de datos de personas jurídicas de derecho privado (titularidad privada).
3. Las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable al que presta la LOPD.
4. Los códigos tipo, o códigos de conducta (normas vinculantes), a los cuales se refiere el artículo 32 de la LOPD.

Es importante resaltar que el numeral 2 del artículo 2º del RLOPD estableció las excepciones a la mencionada regla[160], por lo cual esta no será aplicable a los tratamientos de datos referidos a personas jurídicas ni a las bases de datos que se limiten a incorporar la información profesional de las personas físicas que presten sus servicios en ellas, y consistentes en nombres y apellidos, las funciones o los puestos desempeñados, la dirección postal o electrónica, y en los números de fax y de teléfono profesionales.

160 Ibid., El apartado segundo del artículo 2 estableció como excepciones al régimen de protección de datos personales, las siguientes bases de datos:

"A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

Adicionalmente estableció que se regirían por sus disposiciones específicas, y solo por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

Los ficheros regulados por la legislación de régimen electoral.

Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia".

Para las bases de datos de una administración pública, la legislación española contempló que cuando una entidad del Estado o un gobierno autonómico requieran crear, modificar o suprimir una base de datos o un fichero, deben hacerlo expidiendo una norma a propósito, que determine, de manera específica y concreta, su creación, su modificación o su supresión del RGBD. Debido a ello, por disposición legal[161], el contenido de las normas mediante las cuales se crean, se modifican y se suprimen bases de datos de titularidad pública debe, a su vez, incluir datos tales como el tipo de dato o de datos que pretende incorporar o modificar, el nombre de la base de datos y su finalidad.

La AEPD definió el contenido mínimo[162] que debe tener el RGPD según los requisitos establecidos en el artículo 20 de la Directiva 95/46 del CE, los cuales son:

> Artículo 20. Contenido de la notificación.
>
> 1. Los Estados miembros determinarán la información que debe figurar en la notificación, que será como mínimo:
>
> a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante;
>
> b) el o los objetivos del tratamiento;
>
> c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento;
>
> d) los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos;
>
> e) las transferencias de datos previstas a países terceros;
>
> f) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 resultan adecuadas para garantizar la seguridad del tratamiento.
>
> 2. Los Estados miembros precisarán los procedimientos por los que se notificarán a la autoridad de control las modificaciones que afecten a la información contemplada en el apartado 1.

161 Ibid., artículo 20 y artículo 54 de su Real Decreto 1720 de 2007.

162 Mediante la Resolución del 1 de septiembre de 2006, modificada por la Resolución del 3 de noviembre de 2008, la AEPD adoptó el contenido del formulario de registro de las bases de datos personales, el cual debe ser diligenciado e incluido dentro del RGPD.

Por último, es importante resaltar que el control de las bases de datos es responsabilidad de la AEPD, si bien la norma deja a discreción de cada gobierno autonómico decidir sobre implementa o no agencias autonómicas de protección de datos, las cuales llevarán, en exclusiva, el control de las bases de datos públicas. El registro y la vigilancia del cumplimiento de las normas especiales y de los registros de las bases de titularidad privada están exclusivamente en manos de la AEPD.

El ente de control: la AEPD

Al abordar el proceso de implementación y divulgación de los derechos y los deberes que traía consigo la Directiva de Protección de Datos, es importante resaltar cómo, con la perspectiva del derecho comunitario, con el artículo 28 de dicha Directiva, se abrió paso a la creación de entes de control y vigilancia de la protección de datos de carácter nacional; para el caso español, la AEPD.

Dentro de las funciones otorgadas a estos órganos nacionales se encuentran articular las políticas emitidas por el Consejo Europeo e implementar medidas para el desarrollo concordante entre las premisas en la protección de datos, medidas que permitieron el amparo, en el contexto del derecho interno, del sistema de tratamiento de la Comunidad Europea de Naciones.

Como ya se enunció, la Directiva 95/46 estableció en su artículo 28 la creación de las autoridades públicas independientes, cuya función principal es vigilar la aplicación, en el territorio de cada Estado miembro, de las disposiciones adoptadas por ellos en la aplicación de la citada directiva.

A cargo de dicho órgano, también está la función de ejercer como órgano consultivo en materia de elaboración de medidas reglamentarias relativas a la protección de derechos y libertades de las personas y el tratamiento que se dé a los datos personales.

La Directiva estableció que la autoridad de control debía hallarse investida de facultades de investigación, acceso a los datos objeto de tratamiento y a la posibilidad de recoger toda la información que se requiera para el cumplimiento de sus funciones de control. Así mismo, les otorgó a las autoridades de protección de datos personales de cada país la potestad de amonestar o emitir advertencias u órdenes de bloqueo, supresión o destrucción de datos personales, y les dio la

potestad, incluso, de decretar la prohibición del tratamiento provisional o definitivo de datos personales.

La creación y la existencia de la agencia española se dieron de conformidad con lo dispuesto en el artículo 34.2 y en la disposición final primera de la Ley Orgánica 5/1992, del 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y conocida como LORTAD.

Posteriormente, por medio del Real Decreto 428/1993, del 26 de marzo, se aprobó el Estatuto de la Agencia Española de Protección de Datos, el cual estableció que la AEPD es un ente de derecho público con personalidad jurídica propia y plena capacidad, y que actúa con independencia de las administraciones públicas en el ejercicio de sus funciones, naturaleza que también fue recogida por el artículo 35 de la LOPD, el cual, a su vez, estableció:

> Artículo 35. Naturaleza y régimen jurídico.
>
> 1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

Con la entrada en vigencia de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal, o LOPD, a la AEPD le fueron asignadas funciones, la principal de las cuales es la comprobación de la legalidad de los tratamientos de datos personales. Sin embargo, dicha función no es la única de la AEPD: de acuerdo con el artículo 37 de la LOPD, la citada entidad es el ente encargado de:

> a. Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
>
> b. Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
>
> c. Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d. Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e. Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f. Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g. Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h. Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i. Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j. Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k. Redactar una memoria anual y remitirla al Ministerio de Justicia.

l. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

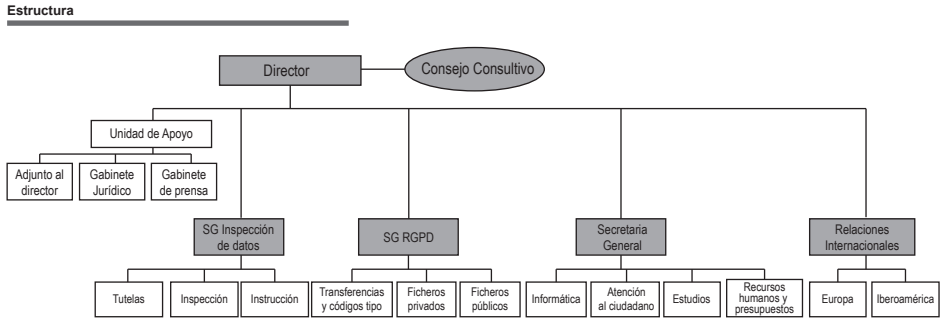
m. Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n. Cuantas otras le sean atribuidas por normas legales o reglamentarias.

El proceso de vigilancia

La estructura funcional de la AEPD comprende un director general, un Consejo Consultivo, una Unidad de Apoyo, una Secretaría General y una Oficina Internacional; y como ejes del desarrollo de las actividades de vigilancia, la Subdirección General del Registro General de Protección de Datos y la Subdirección General de Inspección de Datos, tal como se muestra en la figura 1.

Figura 1. Estructura de la AEPD



Fuente: Agencia Española de Protección de Datos

Para el caso materia de estudio, es importante tener presente dos áreas: (i) la *Subdirección General del Registro de Protección de Datos* y (ii) la *Subdirección General de Inspección de Datos.*

La primera es la encargada de adelantar los trámites propios del estudio de expedientes sobre inscripción de tratamientos notificados, autorización de transferencias internacionales de datos e inscripción de códigos tipo. Dichas funciones son desarrolladas de acuerdo con el principio de publicidad de los tratamientos de datos personales. Expresamente, esta subdirección desarrolla las siguientes funciones:

1. Adelantar trámites relativos a expedientes generados por solicitudes de creación, modificación y supresión de bases de datos de titularidad privada.
2. Tramitar las autorizaciones de transferencia internacional de datos.
3. Hacer las inscripciones de códigos tipo (códigos de conducta).
4. Determinar el contenido de las inscripciones.

5. Aprobar las disposiciones que crean bases de datos de titularidad pública.
6. Vigilar y apoyar el cumplimiento del procedimiento de inscripción y notificación previa al registro de las bases de datos.

Por su parte, la Subdirección General de Inspección de Datos adelanta los procedimientos de comprobación de la legalidad del tratamiento de las bases de datos; o sea, es la entidad encargada de adelantar investigaciones administrativas frente a la posible vulneración del derecho a la protección de datos personales de los titulares. En ejercicio de las facultades otorgadas a la AEPD, dicha dependencia tiene la potestad de adelantar procedimientos de auditoría y de inspección (exámenes de soportes y equipos, sistemas de transmisión y auditoría informática) procedimientos sancionadores e imponer infracciones administrativas. Finalmente, es la encargada de elaborar y adelantar planes con una finalidad educativa y preventiva.

Mediante el Real Decreto 1720/2007, se aprobó el reglamento de desarrollo de la LOPD y se establecieron dos procedimientos mediante los cuales la agencia desarrolla su función de vigilancia y sanción.

El primer procedimiento por el cual se adelantan las reclamaciones frente al ejercicio de los derechos de acceso, rectificación, cancelación y oposición, denominados derechos ARCO, es el procedimiento de instrucción, el cual tiene establecidas unas etapas, a saber:

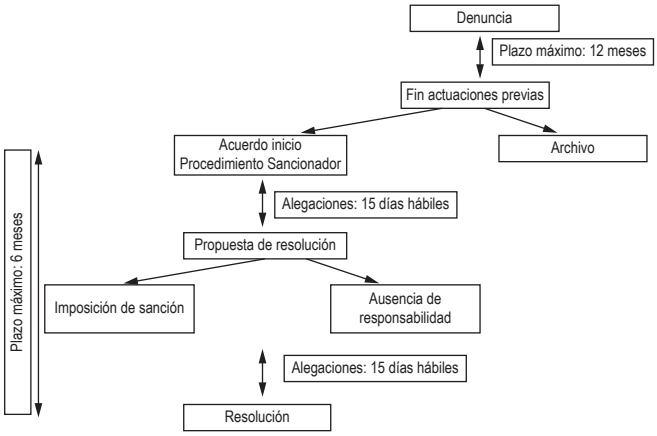
1. El proceso da inicio mediante la realización de la respectiva reclamación por parte del afectado ante la Agencia de Protección de Datos, la cual tiene un plazo de 15 días para trasladar al responsable del fichero los respectivos alegatos. Posteriormente se abre a período probatorio y se adelanta la práctica de inspección o pruebas solicitadas o que determine el ente como pertinentes.
2. Una vez finalizada esta etapa se realiza la audiencia del responsable y el afectado, para finalizar con la respectiva resolución, la cual será de público conocimiento, salvo que se enmarque dentro de las excepciones establecidas en la ley. El plazo máximo de tramitación es de 6 meses.

Por otra parte, el Título IX del RLOPD incluye el procedimiento sancionador, mediante el cual la AEPD ejerce la potestad atribuida por el artículo 37 de la LOPD, desarrollada, a su vez, por el Título VII de la misma ley. El procedimiento establecido es el siguiente (figura 2):

1. Se puede iniciar el proceso con la realización de actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. Esta etapa se realiza de oficio por la AEPD o por denuncia hecha por el afectado o por quien conozca la existencia de un hecho presuntamente ilícito. En esta fase del procedimiento se pedirán todas las pruebas que se estimen pertinentes y podrá durar hasta doce (12) meses, pero una vez finalizada, sin que se haya dictado y notificado acuerdo de inicio de procedimiento sancionador, operará el fenómeno de la caducidad de las actuaciones previas.
2. Una vez finalizada la primera etapa, el Director de la AEPD dictará resolución de archivo, en caso de que no haya mérito para sancionar. En caso contrario, el mismo Director de la AEPD dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, cumplido el plazo de traslado al investigado o responsable, deberá fallarse a más tardar dentro de los seis (6) meses siguientes.

La decisión final, resultado de la investigación puede ser: la imposición de una sanción o la declaratoria de ausencia de responsabilidad.

Figura 2. Procedimiento sancionador de la AEPD



Fuente: Noticias Jurídicas[163]

163 Víctor Roselló Mallol, "Artículos doctrinales: Marketing y protección de datos (VII): El procedimiento sancionador de la AEPD" en *Noticias Jurídicas*. 2010 [acceso 20 de octubre de 2012]. http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4520-marketing-y-proteccion-de-datos-vii:-el-procedimiento-sancionador-de-la-aepd/

El régimen sancionatorio establece que las infracciones pueden ser: (i) infracciones *leves*, y que serán sancionadas con multa de 601,01 a 60 101,21 euros; (ii) infracciones *graves*, que serán sancionadas con multa de 60 101,21 a 300 506,05 euros y, por último, (iii) las infracciones *muy graves*, que pueden ser sancionadas con multa de 300 506,05 a 601 012,10 euros.

Adicionalmente, cuando la infracción sea muy grave, el uso o la cesión ilícitos de los datos de carácter personal impida gravemente o atente, de igual modo, contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad, el director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, ordenar el cese en el uso o la cesión ilícitos de los datos.

Cuando el responsable que sea investigado siguiendo el procedimiento sancionador sea una administración pública, el director de la AEPD podrá ordenar la imposición de medidas correctoras, e, incluso, ordenar la apertura de investigación disciplinaria contra el responsable de la actuación, si así lo ameritara el caso.

Requisitos mínimos de información para solicitar en el proceso de registro

Para que los entes públicos puedan crear bases de datos, deben hacerlo mediante la expedición de normas de orden ministerial o resoluciones emitidas por el titular de la entidad que pretende crearlas. Se deberá adjuntar copia del diario oficial del día en el cual fue publicada la norma; en caso de que el diario se encuentre disponible vía internet, bastará con el número de identificación y la fecha del diario.

La notificación de la existencia de las bases de datos ante la AEPD tiene un plazo de 30 días, contados a partir de la publicación de la norma o el acuerdo que la creó en el diario oficial correspondiente. La información que se solicita en el proceso de registro está enfocada a reportar el nombre de la base de datos, la finalidad y la oficina de contacto ante la cual los ciudadanos pueden ejercer sus derechos A.R.C.O (Acceso, Rectificación, Cancelación y Oposición).

Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero para todos los efectos, tal como lo expresa el artículo 134 del RLOPD.

A partir de marzo de 2012, la AEPD puso en funcionamiento una herramienta adicional, denominada *Dispone*, para agilizar el proceso de creación, modificación y supresión de bases de datos de titularidad pública. La nueva herramienta les simplifica a las administraciones públicas su adaptación a la normativa de protección de datos, en la medida en que facilita el requisito de elaboración y generación de las disposiciones generales o de los acuerdos que deben ser publicados en el diario oficial, o de las regulaciones que las modifiquen o las supriman.

Por otra parte, las personas jurídicas de derecho privado que pretendan crear y tratar bases de datos personales deben notificar previamente a la AEPD la voluntad de crearlas, y especificar la información que se proyecte mostrar en ellas. La solicitud de creación y la inscripción en el registro de las bases de datos deben contener la información establecida en el artículo 54 del RLOPD.

Los campos de información para diligenciar en los formularios de solicitud de inscripción de la base de datos son los siguientes (tabla 1):

Tabla 1. Requisitos mínimos de información

Requisitos de información mínimos para personas jurídicas de derecho público	Requisitos de información mínimos para personas jurídicas de derecho privado
1. Finalidad y usos de la base de datos. 2. Personas o colectivos sobre los que se pretenda obtener datos de carácter personal, o resulten obligados a suministrarlos. 3. Procedimiento de recolección de los datos de carácter personal. 4. Estructura básica de la base de datos y de la descripción de los tipos de datos de carácter personal incluidos en esta.	1. Responsable de la base de datos. 2. Identificación de la base de datos, de sus finalidades y de los usos previstos. 3. Sistema de tratamiento empleado en su organización. 4. El colectivo de personas sobre el que se obtienen los datos. 5. El procedimiento y la procedencia de los datos y las categorías de datos.

Requisitos de información mínimos para personas jurídicas de derecho público	Requisitos de información mínimos para personas jurídicas de derecho privado
5. Cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a terceros países. 6. Órganos de las administraciones responsables de la base de datos. 7. Servicios o unidades ante los que pueden ejercitar los derechos de acceso, rectificación, cancelación y oposición. 8. Medidas de seguridad con indicación del nivel básico, medio o alto exigible. 9. En las disposiciones que se dicten para la supresión de bases de datos, se establecerá el destino de estos, o, en su caso, las previsiones que se adopten para su destrucción.	6. El servicio o la unidad de acceso ante el cual el titular ejerce los derechos. 7. La indicación del nivel de medidas de seguridad básico, medio o alto exigible. 8. La identificación del encargado del tratamiento donde se encuentre ubicada la base de datos. 9. Los destinatarios de cesiones. 10. Transferencias internacionales de datos.

Fuente: Elaboración de la autora.

Están obligadas a registrarse todas las personas públicas o privadas que tengan y traten bases de datos personales, a excepción de las bases de datos propias del ejercicio de la actividad doméstica del individuo, las creadas y sometidas a normas de materias clasificadas y las bases de datos para investigación terrorista y formas graves de delincuencia organizada.

Son responsables de los ficheros o de las bases de datos, y de su tratamiento, la entidad, la persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales. Responde por el cumplimiento de las obligaciones propias de la ley de protección de datos personales el representante legal de estas, o, cuando haya de por medio un mandato expreso, el funcionario a quien se haya delegado para su representación.

Cada empresa debe registrar sus datos de identificación y validar la información en el sistema de la AEPD. Posteriormente a ello, el proceso de registro de una base de datos se inicia diligenciando un formulario electrónico de notificaciones telemáticas, denominado NOTA, el cual puede ser presentado en formulario de papel, mediante Internet, firmado con certificado digital.

El proceso de incorporación y registro de cada base de datos genera un código de registro, el cual permite identificar cada base de datos por el responsable de información que inscriba, y así facilita el proceso de modificación y supresión de las bases, de manera independiente.

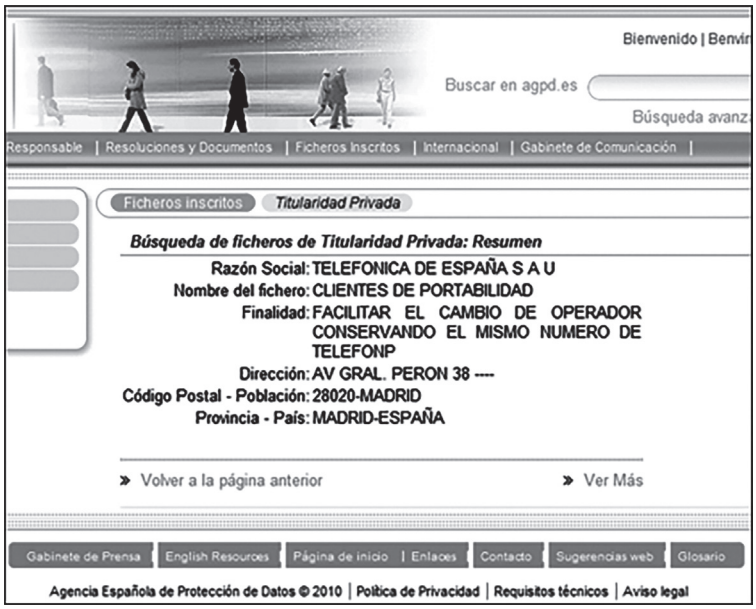
El cargue de base de datos queda vinculado por el responsable de la información, y si este decide entregar a un tercero su tratamiento, el encargado no queda obligado a registrar nuevamente la base de datos. En tal caso, el responsable de la información debe actualizar el formulario indicando quién adelantará el tratamiento de la información en su nombre y bajo su responsabilidad.

Para el manejo de las bases de datos por parte de cada responsable, la AEPD ha creado una guía de seguridad, en la cual se establecen las medidas de seguridad que cobijan el sistema de información, los soportes y los equipos empleados en el tratamiento, las personas que intervienen en el proceso y los locales donde se contenga la información y se haga el tratamiento.

En el proceso de actualización y de supresión de registro de bases de datos solo es necesario ingresar al sistema con la clave de acceso del responsable de la información y diligenciar el formulario de actualización o supresión, el cual solicitará el código del registro de la base de datos, para proceder a registrarlo en el sistema.

Al momento de, simplemente, querer consultar el RGPD, su ingreso no requiere código de ingreso. El acceso al público es libre y gratuito, y permite la búsqueda por nombre de responsable o número de identificación fiscal (NIF). Como consultante del sistema, la información que se puede visualizar se limita al nombre del responsable, el NIF (siempre y cuando no sea una persona natural), el nombre de la base, su finalidad y los datos de contacto, para acceder al ejercicio de los derechos de acceso, rectificación, cancelación y oposición (figura 3).

Figura 3. Información consulta general.



Fuente: AEPG

Por último, dentro de la estrategia de supervisión y regulación del tratamiento de datos personales, la Directiva 95/46 en su considerando 26 habla de la importancia que tiene, en el tratamiento de información en sectores especializados la creación e implementación de códigos de conducta o normas que permitan ajustar la garantía efectiva del derecho a la protección de datos personales frente al desarrollo propio de la actividad. Dicho mecanismo fue traspuesto a la legislación española mediante el capítulo V de la LOPD. Con dichas normas de conducta, los Estados miembros y la Comisión Europea, buscaron contribuir, según las características de cada sector, a la correcta aplicación de normas nacionales y la garantía del citado derecho. Estos mecanismos de autocontrol abren un nuevo camino en el procedimiento de protección de datos.

El contexto tan amplio y dinámico que Internet permite hoy es el escenario perfecto para vulneraciones de todo tipo. Por ello, los mencionados modos de autorregulación, que, normalmente, han tendido a realizarse en el sector privado, son mecanismos de autocontrol que han llegado a ser considerados buenas herramientas con el fin de establecer una serie de reglas, condiciones de organización,

políticas de tratamiento y la implementación de normas especiales de seguridad y sellos o certificaciones altamente llamativas para las organizaciones[164].

En el artículo 27, capítulo V de la Directiva 95/46, se incluyeron los códigos de conducta como elementos útiles para brindar orientaciones en el tratamiento de la información, de acuerdo con las particularidades que pudieran presentarse en los diferentes sectores y ámbitos de la sociedad que trataran información personal. El artículo en mención expone:

> Artículo 27. Códigos de conducta.
>
> 1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.
>
> 2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.
>
> Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.
>
> 3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

164 Mónica Vilasau Solana, "Intimidad y datos personales en internet" en Miguel Pequera Poch (Coordinador). *Principios del derecho en la sociedad de la información. Derecho y nuevas tecnologías* (Barcelona: Editorial UOC, 2005), 152-215.

Al analizar el artículo, y en busca del sentido más amplio de la existencia de este tipo de compilaciones, se encuentra cómo lo que se pretende con la creación de códigos tipo es simplificar todo el proceso adecuación a la norma de sectores específicos, con requerimientos especiales (o, sencillamente, propios) que tratan datos de naturaleza personal.

Dicho en otras palabras, los códigos de conducta, o códigos tipo, buscan facilitar la adecuación a la norma incluyendo criterios de autorregulación sectorial. En España, con el desarrollo que hizo el RLOPD del artículo 32 de la LOPD, se establecieron parámetros para adecuar los tratamientos de datos específicos de sectores o industrias al cumplimiento de la LOPD.

El artículo 71 del RLOPD instauró que los códigos tipo tendrán el carácter de códigos deontológicos[165], o de buena práctica profesional, y serán vinculantes para quienes se adhieran a ellos. Así mismo, tendrán carácter de voluntarios, y su contenido podrá versar sobre la totalidad o sobre apartes del tratamiento de datos en un sector, pero deben versar sobre la totalidad del tratamiento de datos personales que una empresa realice.

Teniendo en cuenta que el objetivo de los códigos tipo es adaptar la LOPD a las peculiaridades de cada sector, se parte de la base de que la mayoría de empresas pertenecientes a un gremio, un colegio profesional, una asociación empresarial o un sector muy específico de actividad tendrán las mismas necesidades y obligaciones en materia de protección de datos en cuanto a tipos de ficheros por registrar en el RGPD de la AEPD, y medidas de seguridad por aplicar para protegerlos.

Pese a que la adhesión a ellos es voluntaria, los códigos tipo son de carácter vinculante, por lo cual los firmantes están obligados a cumplir las exigencias que recoja el documento, las cuales pueden, en algunos casos, superar a las estrictamente legales. Los códigos tipo deben ser redactados en términos claros y accesibles, que faciliten su comprensión y su aplicación. Los promotores de los códigos tipo pueden fijar revisiones (generalmente, anuales) de su cumplimiento. Pero todo ello, teniendo de presente que los códigos tipo deben ser evaluados y aprobados para su registro por la AEPD.

Las administraciones públicas y las corporaciones de derecho público también podrán adoptar códigos tipo, según lo establecido en las normas que les sean

165 f. Ciencia o tratado de los deberes. *Diccionario de la Lengua Española*. Real Academia Española. Versión 2010.

aplicables. Los contenidos de información que deben tener los códigos de conducta son los establecidos en el artículo 73 del RLOPD, el cual obliga a lo siguiente:

> Artículo 73. Contenido.
>
> 1. Los códigos tipo deberán estar redactados en términos claros y accesibles.
>
> 2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:
>
> a. La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
>
> b. Las previsiones específicas para la aplicación de los principios de protección de datos.
>
> c. El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.
>
> d. El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
>
> e. La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.
>
> f. Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.
>
> g. Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.
>
> [...]

El procedimiento que se prevea en el código de conducta deberá incluir el procedimiento para su inscripción en el RGPD, por lo cual la inscripción se iniciará siempre por expresa solicitud de la entidad, del órgano o de la asociación promotora del código tipo.

Con el fin de garantizar el cumplimiento de lo establecido por la LOPD, los códigos tipo deben incluir procedimientos de supervisión propios, para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, así como establecer un régimen sancionador adecuado y eficaz.

Para que los códigos tipo puedan ser considerados como tales para los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, deben ser depositados e inscritos en el RGPD de la AEPD, sin perjuicio de su inscripción, cuando corresponda, en los registros que fueran creados por las comunidades autónomas, según lo dispuesto en el apartado 2 del artículo 41 de la LOPD.

Finalmente, una vez inscritos, la AEPD da publicidad a los códigos tipo; preferentemente, a través de medios informáticos o telemáticos. Sin embargo, una vez revisadas las publicaciones que sobre códigos tipo registra la AEPD, se encuentra que el volumen de participación a través de dicho mecanismo es muy baja, pues solo se registra la publicación de doce códigos tipo en la página web de la entidad y la de un solo registro en los registros autonómicos de protección de datos que lo han incluido, a su vez, en el RGPD.

Por no ser una norma de obligatorio cumplimiento, en el proceso de registro de bases de datos la AEPD no ha incorporado certificaciones ni sellos de cumplimiento de la norma de protección de datos.

El Registro Nacional de Protección de Datos (RNBD). El caso colombiano

Con la entrada en vigencia de la Ley 1581 del 17 de octubre de 2012, o Ley de Protección de Datos Personales, y una vez finalizado el plazo de transición de 6 meses que otorgó la citada norma para adelantar las adecuaciones y su puesta en marcha, tanto las entidades de derecho público como los entes de derecho privado se vieron avocados a adelantar ajustes dentro de sus organizaciones, así como frente a las personas de quienes poseían y trataban datos de carácter personal.

En dicho proceso de adecuación, los responsables de tratamiento[166], además de crear las propias políticas de tratamiento de la información, de acuerdo

166 Congreso de la República de Colombia. *Ley 1581 de 2012*, Por la cual se dictan disposiciones generales para la protección de datos personales (Bogotá: *Diario Oficial*, No. 48.587, 2012), literal e) del artículo 3: "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".

con los principios que rigen la actividad[167], debieron implementar, como los encargados del tratamiento[168], protocolos para recolectar la autorización previa e informada por parte de los titulares[169], así como la creación de procedimientos que garanticen la confidencialidad y la seguridad en el proceso de recolección, tratamiento, trasmisión y transferencia, y hasta de eliminación, de los datos personales custodiados y de cualquier operación hecha sobre los datos personales. Adicionalmente, debieron implementarse canales de atención a los titulares o a las áreas de atención de consultas y reclamos, para garantizar el ejercicio de los derechos de los titulares.

Pero, quizás, lo primero que debieron adelantar los responsables del tratamiento fue un inventario de las bases de datos que tenían dentro de cada organización, la finalidad para la cual eran usadas estas, y si finalmente, dentro de su actividad, ellas debían seguir siendo un elemento importante de la organización, pues otro deber que les impuso la Ley General de Protección de Datos Personales fue registrar las bases de datos en el RNBD.

El artículo 25 de la Ley 1581 de 2012 definió el Registro Nacional de Bases de Datos como "el directorio público de las bases de datos sujetas a Tratamiento en el país", e impuso el deber a los responsables del tratamiento de información de registrar en él las bases de datos sujetas a control, según el ámbito de aplicación de la ley.

En el trámite que surtió la Ley 1581 de 2012 en el Congreso de la República (entonces Proyecto de Ley Estatutaria No. 46 de 2010 de la Cámara de Representantes), el artículo 25 fue aprobado en primera vuelta por el mencionado órgano el 19 de octubre de 2010, por mayoría absoluta, pero su texto fue adicionado de la siguiente manera:

> Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incum-

167 Congreso de la República de Colombia, *Ley 1581 de 2012*, artículo 4: "Principio de Legalidad en materia de tratamiento de datos, principio de finalidad, principio libertad, principio de veracidad o calidad del dato, principio de transparencia, principio de acceso o circulación restringida, principio de seguridad y confidencialidad".

168 Ibid., artículo 3, literal d): "Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento".

169 Ibid., Literal f): "Titular: Persona natural cuyos datos personales sean objeto de Tratamiento".

> plimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.

A su vez, dicho texto fue incorporado al texto que se sometería a consideración ante el Senado de la República, cuyo Proyecto de Ley Estatutaria era el No. 184 de 2010, y fue aprobado en segundo debate, por lo que el texto definitivo y objeto de control constitucional previo fue el siguiente:

> Artículo 25. Definición. El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.
>
> El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.
>
> Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.
>
> **Parágrafo.** El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.

Analizado el tema por la Corte Constitucional, en Sentencia C-748 de 2011, mediante la cual se adelantó el control de constitucionalidad de la Ley Estatutaria 1581 de 2012, el máximo órgano constitucional hizo especial énfasis en que el RNBD operaría como el directorio público de las bases de datos sujetas a tratamiento que operan en el país, y sería administrado por la SIC, ente de vigilancia y garante del cumplimiento de los preceptos de la citada norma y máxima autoridad de protección de datos en Colombia, tal como lo contempló en el artículo 19 de la citada ley, y el cual ordenó la creación, dentro de la citada superintendencia, de la Delegatura para la Protección de Datos Personales, como más adelante se estudiará.

Las funciones principales que la Corte Constitucional le atribuyó a ese registro fueron tres; a saber:

1. Permitir que todos los ciudadanos sepan cuáles son las bases de datos que funcionan en el país.
2. Dotar a la SIC de una herramienta mediante la cual tenga el control preciso sobre las bases de datos que se tienen en el país, en la medida en que, a través de tal herramienta, se pueda establecer por medio de quién y cómo se trata la información en el territorio colombiano.
3. Permitir al ente de control y vigilancia conocer sobre las políticas de tratamiento de la información que tienen los responsables y los encargados del tratamiento de datos personales, y las cuales deben, como mínimo, contener los deberes que exige la ley, según los principios del derecho a la protección de datos personales. Ello, no solo con el fin de verificar su cumplimiento, sino, además, brindar la posibilidad al ente de control (dada la obligatoriedad de disponer de una política de tratamiento y registrarlas) de verificar el cumplimiento de dichas políticas, y en caso de llegarse a determinar la inobservancia de tal obligación, poder proceder a la imposición de las sanciones correspondientes.

La Corte Constitucional, consciente de la trascendencia y la importancia en el proceso de adecuación, cumplimiento y vigilancia de tal deber legal frente a la pertinencia de la existencia de un RNBD, como herramienta que facilitaría el ejercicio del derecho de hábeas data, manifestó lo siguiente:

> En el marco internacional se observa que esta clase de registros tienen por objeto permitir que todas las personas, como una forma de materializar su derecho al habeas data, puedan **conocer** con exactitud qué bases de datos hacen tratamiento sobre sus datos personales y de esa forma ejercitar todo el plexo de derechos que se derivan del habeas data: actualización, rectificación, oposición, supresión, etc. En consecuencia, ha de entenderse que el registro al que se refiere el precepto en revisión no busca llevar simplemente un registro público de bases de datos, como parecería deducirse de su texto, sino el permitir a cualquier ciudadano establecer con exactitud quiénes son los responsables y encargados del tratamiento de sus datos, como otra forma de materializar el principio de transparencia que guía la administración de las bases de datos. En otros términos, el objetivo de la centralización de esta clase de información por parte de un órgano del Estado, es facilitar el ejercicio de uno de los ámbitos esenciales del habeas data: conocer quién está haciendo tratamiento de datos personales, a fin de que pueda existir un control efectivo de éstos por su titular**,** hecho que explica por qué dicho registro es abierto a la consulta del público en general. En ese orden

> ideas, la inscripción en él se **debe imponer** como una obligación tanto para las bases públicas como privadas, pues este es un instrumento que permitirá que el Estado efectivamente garantice que el titular del dato pueda tener un control efectivo sobre sus datos personales. Es decir, es ésta otra forma que en un instrumento puede ayudar a materializar el ejercicio de un derecho fundamental como lo es el habeas data.

Como ya se expuso, con el mencionado registro se busca, además de cumplir con la obligación legal de difundir y dar publicidad a la existencia de bases de datos de carácter personal, tener una herramienta de verificación y control del cumplimiento del derecho a la protección de datos personales y de protección del titular de estos, dentro del proceso de supervisión que adelanta la SIC en la materia, como autoridad en Colombia, en virtud de las funciones asignadas por el artículo 19 de la Ley 1581 de 2012.

En el presente capítulo, se busca dar a conocer los antecedentes y creación legal del RNBD en Colombia, así como el proyecto de decreto sobre los requisitos para la implementación que adelantó la SIC, como herramienta fundamental para ejercer las funciones de vigilancia y control del tratamiento de datos personales.

Antecedentes legales y jurisprudenciales del derecho a la protección de datos personales, como precedente para la existencia y creación del RNBD

Desde cuando se promulgó la Constitución Política de Colombia, en 1991, y hasta antes de la expedición de la Ley 1581 de 2012, el desarrollo legal y jurisprudencial del derecho a la protección de datos en Colombia estuvo vinculado a la protección de la información de carácter financiero, crediticio y comercial de las personas tanto naturales como jurídicas, como medidas para contener y regular la actividad de *bureaus* privados o centrales de riesgo[170] que recogían, administraban y poseían bases de datos con este tipo de información en Colombia. Dichas organizaciones surgen durante la década de 1980, sin la existencia de una reglamentación especial para la administración y el tratamiento de la información crediticia, financiera y comercial de las personas.

170 Las centrales de riesgo son bases de datos administradas por personas jurídicas de derecho privado que agremian sociedades del sistema financiero (Asobancaria) o empresas dedicadas a la prestación de servicios para el cálculo del riesgo financiero y crediticio (Experian Colombia S. A.), conocidas como burós, cuyos productos comerciales se enfocan en brindar información financiera y crediticia y determinar un *score*, o puntuación de las personas vinculadas a través de bancos, establecimientos de comercio a productos financieros de financiamiento y comercial.

En Colombia, el reconocimiento del derecho a la protección de datos personales está fundamentado en el artículo 15, Título II, "De los Derechos, las Garantías y los Deberes" Capítulo I "De los Derechos Fundamentales", de la Constitución Política de 1991, y el cual lo establece en los siguientes términos:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. *De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*
> *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*. [Cursivas fuera del texto].

Como se observa, el citado artículo consagró en un mismo articulado derechos fundamentales, como: (i) el derecho a la intimidad personal y familiar; (ii) el derecho al buen nombre, y (iii) el derecho a la protección de datos personales (pese a que no lo enunció como tal, sí lo definió, y le dio el alcance y la importancia de un derecho fundamental).

Desde 1991 y hasta 2008, el desarrollo del derecho a la autodeterminación informativa, o derecho del hábeas data (acepciones igualmente usadas por la jurisprudencia para referirse a un mismo derecho[171], al cual hoy se le denomina *derecho a la protección de datos personales*), tuvo un desarrollo importante a lo largo de dicho periodo. Fue en esta época cuando, vía jurisprudencia, se marcó el derrotero de lo que sería el ejercicio del derecho a conocer, actualizar y rectificar información que se encontrara reportada en las bases de datos de las centrales de riesgo. Igualmente, fue para esa época cuando se entró a cuestionar y delimitar el ejercicio de la actividad de las centrales de riesgo, en pro de los derechos de los titulares y en búsqueda de un equilibrio entre el riesgo de la actividad crediticia y el derecho de los ciudadanos a conocer, actualizar y rectificar la información personal.

171 Corte Constitucional de Colombia, *Sentencia C-1011 de 2008*, M. P. Jaime Córdova Triviño, "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 el 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".

Durante el mismo periodo, también se vio cómo el desarrollo jurisprudencial del derecho a la protección de datos se dio en dos vertientes: (i) La primera tendencia consideró que la protección de los datos personales estaba ligada al derecho a la intimidad; por ello, en 1992, con la sentencia T-414[172], la Corte Constitucional fundamentó la decisión de eliminar la información financiera negativa de un ciudadano, al ponderar el derecho a la intimidad del artículo 15, sobre el derecho de información del artículo 20 de la Constitución Nacional Colombiana[173]. (ii) Una segunda línea jurisprudencial de interpretación fue la que desarrolló el derecho de *hábeas data*, como un derecho ligado no solo al derecho a la intimidad, sino vinculado directamente con la potestad de autodeterminación informática e informativa, tendencia que fue ampliamente acogida, y llegó a ser la posición jurisprudencialmente dominante en Colombia.

Debido a los múltiples y reiterados pronunciamientos jurisprudenciales que se sucedieron desde entonces, la Honorable Corte profirió dos sentencias de unificación: la SU-082, de 1995, y la SU-089, también de 1995, y en las cuales se expuso la dicotomía que se presentaba al analizar conjuntamente los alcances y los límites de los derechos de los artículos 15 y 20 de la Constitución Política de Colombia. Fue a través de dichas sentencias como la Corte Constitucional dio inicio al concepto del derecho de hábeas data como un derecho autónomo, cuyo núcleo esencial está fundamentado en la *"autodeterminación informática y la libertad en general y en especial la económica*"[174], y hasta incluyó el derecho a la caducidad del dato negativo en materia crediticia, financiera y comercial.

Desde 1993, se buscó la expedición de normatividad referente a la administración de bases de datos de organizaciones vinculadas con entidades financieras y comerciales, pero solo hasta 2008 se logró expedir esa ley, con la cual se buscó

172 Corte Constitucional de Colombia, *Sentencia T-414 de 1992*, M. P. Ciro Angarita Barón.

173 En este pronunciamiento también es importante en el desarrollo jurisprudencial colombiano, pues la Corte Constitucional, teniendo como soporte el hecho de que el dato reportado en la central de riesgo se encontraba soportado en un documento cuya obligación había sido declarada judicialmente extinta, fue la primera vez que el alto tribunal habló de la prescripción legal de la obligación, como fundamento para hablar de la caducidad del dato personal.

174 Corte Constitucional de Colombia, *Sentencia su-082 de 1995*, M. P. Jorge Arango Mejía "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, y se habla de la libertad económica, en especial, porque ésta podría ser vulnerada al restringirse indebidamente en virtud de la circulación de datos que no sean veraces, o que no haya sido autorizada por la persona concernida o por la ley".

regular el ejercicio de la actividad de recolección, manejo, conservación y divulgación de la información comercial de las personas, ante el masivo uso de la acción de tutela para proteger el derecho de hábeas data[175]. Dicho proyecto fue declarado inconstitucional, por vicios de procedimiento[176].

En 2008, con la expedición de la Ley Estatutaria 1266[177], el legislador colombiano, recogiendo lo que por vía jurisprudencial se había desarrollado frente al mencionado derecho, centró su esfuerzo en regular el tratamiento de datos personales de carácter crediticio, comercial y de servicios, y por ello se puede afirmar, como lo señaló la Corte Constitucional en la sentencia C-1011 de 2008 (por la cual se declaró la exequibilidad de la citada ley), que la referida norma corresponde a una regulación parcial del derecho de hábeas data como tal, y "no puede considerarse como un régimen jurídico que regule, en su integridad, el derecho a la protección de datos personales".

La Ley 1266 de 2008 definió quiénes eran los sujetos obligados[178] dentro del tratamiento de los datos personales de carácter financiero, crediticio y comercial, en qué tipos se clasifican los datos personales[179], cuáles son los principios que rigen el derecho[180], y cuáles, los deberes de los obligados, así como cuáles son los derechos de los titulares de la información[181]. Dado el carácter de norma sectorial, el derecho a la protección de los datos personales ha llegado a denominarse *hábeas data financiero*.

175 Eduardo Cifuentes Muñoz, "El Habeas data en Colombia". *Revista Ius et Praxis*. 3 (2007): 81-106.

176 Corte Constitucional de Colombia, *Sentencia C-008 de 1995*, M. P. José Gregorio Hernández Galindo.

177 Congreso de la República de Colombia, *Ley Estatutaria 1266, expedida el 31 de diciembre de 2008*, "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en las bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" (Bogotá: *Diario Oficial* No. 47.219, 31 de diciembre de 2008).

178 Fuente de información, operador de información, usuario de información y titular de información.

179 Dato personal público, semiprivado y privado.

180 Congreso de la República de Colombia, *Ley 1266 de 2008*, artículo 4: "Principio de veracidad o calidad del dato, principio de finalidad, principio de circulación restringida, principio de temporalidad de la información, principio de libertad, principio de interpretación integral de derechos constitucionales, principio de seguridad y principio de confidencialidad".

181 Ibid., artículos 6-9. Se desarrolla el derecho a conocer, actualizar y rectificar la información personal de los titulares, en mano de quien esté; es decir, fuentes, operadores y usuarios de la información. Igualmente, en el artículo 16 de la citada norma se encuentra regulado el derecho de los titulares a presentar solicitudes de consulta o reclamo.

En 2012, con la promulgación de la Ley Estatutaria 1581, incluida la sanción presidencial de la Ley 1581 del 17 de octubre de 2012, conocida, a su vez, como la Ley de Protección de Datos Personales, "Por medio de las cual se dictan disposiciones generales para la protección de datos personales", se consolidó el marco legal dentro del que se articula toda la política de protección de datos personales, así como los principios rectores de la protección de datos, las definiciones y los conceptos básicos para entender los derechos de los titulares de la información, los deberes de las personas naturales y jurídicas en el tratamiento de la información, las responsabilidades de quien posee una base de datos o un fichero, las funciones y los alcances del ente encargado de ejercer la vigilancia, las condiciones del tratamiento, y los procedimientos para ejercer los derechos, así como el establecimiento de los mecanismos de vigilancia, control y sanción por vulneración de los derechos en Colombia.

El ámbito de aplicación de la Ley está enfocado en los datos personales consignados en una base de datos que los haga susceptibles de tratamiento por parte de entidades de naturaleza pública o privada (ámbito *subjetivo*), ubicada en el territorio nacional colombiano, o cuando al responsable del tratamiento o al encargado del tratamiento no establecido en territorio nacional, le sea aplicable la legislación colombiana en virtud de normas y de tratados internacionales (ámbito *territorial*).

La norma excluyó de su ámbito de aplicación las bases de datos mantenidas en una esfera exclusivamente personal o doméstica; de igual modo, excluyó las que tengan por objeto la seguridad y la defensa nacionales, así como la prevención, la detección, el monitoreo y el control del lavado de activos y el financiamiento del terrorismo; también, las que tengan como fin y contengan información de inteligencia y contrainteligencia, las de información periodística y contenidos editoriales, las reguladas por la Ley 1266 de 2008 (o Ley de Hábeas Data Financiero), así como las reguladas por la Ley 79 de 1993, norma especial que rige lo concerniente a la información del censo poblacional y de estadísticas.

En la sentencia C-748 de 2011[182], mediante la cual se hizo el estudio de constitucionalidad de la Ley 1581 del 17 de octubre de 2012, "Por el cual se

182 Corte Constitucional de Colombia, *Sentencia C-748 de 2012*, M. P. Jorge Ignacio Pretelt Chaljub. Esta sentencia fue proferida el 6 de octubre de 2011, pero solo llegó a ser firmada y publicada por la Corte Constitucional el 25 de julio de 2012.

dictan disposiciones generales para la protección de datos personales", la Corte Constitucional definió el citado derecho como:

> […] aquel que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de la información que sobre él reposa en los mismos, así como la limitación en las posibilidades de divulgación, publicación o cesión de sus datos, de conformidad con los principios que regulan el proceso de administración de datos personales. Este derecho tiene naturaleza autónoma y notas características que lo diferencian de otras garantías con las que, empero, está en permanente relación, como los derechos a la intimidad y a la información.

Así mismo, la citada sentencia dio claras luces sobre el alcance del régimen general del derecho a la protección de datos personales. Mediante este pronunciamiento, determinó el alcance del ejercicio del derecho a la protección de datos de la siguiente manera:

> (i) El derecho de la personas a conocer –acceso– la información que sobre ellas está recogidas en las bases de datos, *lo que conlleva el acceso a las bases de datos donde se encuentra la información*. (ii) el derecho a incluir nuevos datos con el fin de (sic) 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 las bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normatividad. (Cursivas fuera del texto)

Como se observa, la nueva ley consagró como derecho de los titulares de la información ya no solo el derecho a conocer, actualizar, rectificar, sino que incluyó el derecho a incluir y suprimir la información personal, así como a revocar la autorización que se haya otorgado para su tratamiento, por voluntad del titular, siempre y cuando no haya una obligación legal que lo impida, o cuando en el tratamiento no se respeten los principios, los derechos y las garantías constitucionales y legales del caso.

También facultó al titular con la posibilidad de solicitar prueba de la autorización otorgada para el tratamiento, e imponerle al responsable del tratamiento el deber de solicitar previa e informada la autorización al titular, y así obligarlo

a conservar copia de esta, con el fin de poder consultarla posteriormente, sin importar el medio a través de la cual sea recogida.

Por lo anterior, la norma previó, en ejercicio del derecho de acceso a la información, la *gratuidad*; es decir, que el Titular tenga acceso, sin costo alguno, a conocer qué información se encuentra en determinada base de datos. Ese es un elemento de importancia al momento de concebir el desarrollo del RNBD, pues permitirá saber específicamente el nombre de las bases de datos objeto de tratamiento en Colombia y que poseen las entidades de naturaleza pública o privada, responsables de ellas, así como enterarse de la finalidad para la cual fueron creadas, así como los datos de contacto ante los cuales el ciudadano titular de información podrá ejercer los derechos a conocer, actualizar, rectificar, incluir y excluir la información que sobre él repose en las bases de datos.

Consideró la Corte Constitucional que en los países que han implementado algún tipo de reglamentación para proteger datos personales, crear el registro de bases de datos ha sido un instrumento importante en ejercicio del derecho de publicidad, por lo cual el legislador colombiano adoptó la creación de tal registro en el país.

Prosiguió el Alto Tribunal con la sentencia C-748 de 2011, y discernió en su análisis que la administración de datos personales en Colombia está influida por la concepción internacional del derecho, y ante ello, tras un análisis de las normas internacionales sobre la materia, y luego de revisar el modo como se ha abordado el desarrollo normativo del caso, concluye que, según un análisis comparado entre los modelos de protección de datos en el mundo, el modelo colombiano de protección de datos corresponde a un modelo de protección híbrido entre el modelo centralizado europeo y el modelo sectorial norteamericano.

Resalta la Corte Constitucional, en la aludida sentencia, que los países europeos parten de una categoría general de datos personales, y en ella la idea central sobre el tratamiento de datos personales es considerada "*per se,* potencialmente problemático", por lo que cualquier tratamiento debe sujetarse a principios y garantías mínimas comunes, pero susceptibles de ser complementados por regulaciones especiales, según el tipo de datos y los intereses involucrados, sin que se deje de garantizar la aplicación de principios generales de tratamiento y protección de todos los datos personales, ya sea en bases de datos en manos de entidades de derecho público o de derecho privado. De esta manera ha entendido

la Corte la implementación en la Unión Europea de los principios y los derroteros de la Directiva 46/95, que permite garantizar la protección de los datos personales sin restringir el flujo transfronterizo de estos.

Adicionalmente, del modelo europeo resalta la Corte la existencia de una entidad central, autónoma e independiente que supervisa, vigila y controla la instrumentación y el cumplimiento normativo de los parámetros establecidos para proteger datos personales, como entidad especializada "que permite generar memoria y producir conocimiento que son reempleados en el diseño de políticas públicas en la materia".

Del modelo sectorial norteamericano, resalta la Corte que no parte de una categoría común de datos personales y, por lo tanto, no se considera que todos los datos deban estar sometidos a una misma regulación, por lo cual dicha concepción permite promulgar normas sectoriales que desarrollen regulaciones especiales y diferentes para cada tipo de dato personal,

> […] dependiendo de su relación con la intimidad ó privacidad, como se le denomina en el sistema anglosajón, y con la protección de intereses superiores –como la seguridad y la defensa nacional, es decir, la regulación sectorial se basa en una especie de ponderación de intereses que da lugar a reglas diferenciadas según el tipo de dato, que otorga más o menos poderes de intervención a las autoridades.

Según lo expuesto, la Corte ha encontrado en el caso colombiano que con la expedición de la Ley 1581 de 2012, o Ley de Protección de Datos Personales, aplicable a todo tratamiento de los datos personales, y con la existencia de una ley sectorial[183] enfocada en la protección de los datos personales de carácter financiero, crediticio y comercial, el modelo colombiano se puede catalogar como un modelo híbrido entre el modelo europeo y el modelo americano.

La autoridad de control

La SIC es un ente de carácter público creado en 1959, y su función reguladora está centrada en cinco áreas misionales entre las que se encuentra la de ser la autoridad de vigilancia y control en materia de protección de datos personales[184],

183 Congreso de la República de Colombia, *Ley 1266 de 2008*.

184 Protección al consumidor, propiedad industrial, competencia desleal, regulación de cámaras de comercio, reglamentos técnicos y metrología legal.

por lo que es el ente competente para conocer, vigilar y resolver temas de protección al consumidor, propiedad industrial, competencia desleal, regulación de cámaras de comercio, reglamentos técnicos y metrología legal.

Fue a partir de 2008, ante la expedición de la Ley 1266 de 2008, cuando, junto con la Superintendencia Financiera de Colombia (SFC), la SIC asumió funciones en la protección del *derecho de hábeas data financiero*; es decir, la SIC empezó a vigilar y proteger el mencionado derecho frente al tratamiento de los datos personales de las historias crediticias y financieras de los colombianos, que son tratados por establecimientos comerciales del sector real de la economía, mientras que la SFC ejerce dichas funciones cuando la información personal es tratada por entidades del sistema bancario.

La citada ley aportó un régimen de transición que les permitió a las entidades vigiladas adecuarse a la norma; fue transcurridos seis meses después de su entrada en vigencia (o sea, a partir del 1 de julio de 2009) cuando ambas superintendencias entraron a conocer denuncias y a ejercer controles sobre el tema. Entre 2009 y 2011, la SIC desarrolló tales funciones dentro de la Delegatura para la Protección al Consumidor.

Posteriormente, en 2011, mediante la expedición del Decreto 4886, del 23 de diciembre, se reestructuró la planta de personal de la SIC y se incorporó en su organización la Delegatura de Protección de Datos Personales, como ente designado para ejercer las funciones de autoridad de vigilancia y control, para adelantar procesos administrativos y de juez de tutela que amparase y garantizara el derecho a la protección de datos personales.

El carácter autónomo e independiente de la SIC y su naturaleza de organismo técnico con autonomía administrativa son las características determinadoras de que a la entidad se le otorgara la potestad de vigilancia y control en la protección de datos personales.

Las funciones de vigilancia fueron asignadas por el artículo 17 de la Ley 1266 de 2008, en concordancia con el artículo 17 del Decreto 4886 de 2011, y establecieron que la Dirección de Protección de Datos Personales tendría las siguientes funciones:

> Artículo 17. Funciones de la Dirección de Investigación de Protección de Datos Personales. Son funciones de la Dirección de Investigación de Protección de Datos Personales:

1. Ejercer la vigilancia de los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países de la misma naturaleza, en cuanto se refiere a la actividad de administración de datos personales, en los términos de la ley.

   En los casos en que la fuente, usuario u operador de información sea una entidad vigilada por la Superintendencia Financiera de Colombia, esta ejercerá la vigilancia e impondrá las sanciones correspondientes, de conformidad con lo establecido en el artículo 17 de la Ley 1266 de 2008.

2. Ejercer la supervisión de las instrucciones impartidas por la Superintendencia de Industria y Comercio en materia de protección de datos personales.

3. Velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la Ley 1266 de 2008.

4. Tramitar y decidir las investigaciones adelantadas contra los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países de la misma naturaleza.

5. Ordenar la corrección, actualización o retiro de datos personales de una base de datos, cuando así se determine dentro de la investigación.

6. Ordenar la realización de auditorías externas de sistemas para verificar la adecuada aplicación de la ley 1266 de 2008.

7. Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.

8. Resolver los recursos de reposición y las solicitudes de revocatoria directa que sean interpuestos contra los actos que expida.

9. Las demás funciones que le sean asignadas de acuerdo a la naturaleza de la dependencia.

De acuerdo con la asignación de las mencionadas funciones y la creciente divulgación de los derechos de los titulares de información, como ya se dijo, desde 2009 la SIC ha venido ejerciendo funciones de autoridad e incrementando

su ejercicio en la vigilancia y el control de los datos personales y sobre los datos referentes a la historia crediticia y financiera; o, como se diría en España, sobre el tratamiento de datos personales referentes a la solvencia patrimonial y de crédito.

Posteriormente, con la sanción presidencial de la Ley 1581 de 2012, mediante la cual se expidió la Ley de Protección de Datos, le fueron otorgadas a la SIC facultades para ejercer la vigilancia y el control sobre el tratamiento de todos los datos personales registrados en cualesquiera ficheros o bases de datos de personas jurídicas de derecho público o privado, ubicadas en el territorio colombiano, o a las que, no obstante estar fuera del territorio colombiano, les sea aplicable la norma, en virtud de normas y tratados internacionales. Dicho tratamiento debe respetar los principios, los derechos, las garantías y los procedimientos previstos en la ley colombiana.

La norma concedió el plazo de 6 meses, contados a partir de la fecha de su publicación en el *Diario Oficial* (o sea, a partir del 18 de octubre de 2012), para que se incorporara dentro de la estructura de la SIC una delegatura que ejerciese las funciones de autoridad de protección de datos; pero, como se dijo líneas arriba, a partir de enero de 2012, la SIC incluyó dentro de su estructura la nueva delegatura, con el fin de implementar lo que ya se preveía en el entonces proyecto de ley, hoy Ley 1581 de 2012.

De acuerdo con la nueva norma, son funciones de la SIC, en materia de protección de datos personales, las siguientes:

> Artículo 21. Funciones. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:
>
> 1. Velar por el cumplimiento de la legislación en materia de protección de datos personales.
>
> 2. Adelantar 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.
>
> 3. Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus

derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.

4. Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementar campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.

5. Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley.

6. Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

7. Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos.

8. Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.

9. Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.

10. Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.

11. Las demás que le sean asignadas por ley.

De acuerdo con las estadísticas de la Delegatura para la Protección de Datos Personales de la SIC, evidencian un tímido crecimiento en el volumen de quejas presentadas entre el periodo comprendido entre septiembre de 2011 y septiembre de 2013, ha sido constante y con tendencia al crecimiento. El ejercicio de las facultades de vigilancia y control por parte de la SIC, respecto a la garantía del derecho del habeas data financiero, se vieron aumentadas en este periodo en un cincuenta por cien (50%). La tabla 1 muestra los niveles de quejas que se han presentado en Colombia ante la promulgación de esta norma.

Tabla 1. Gestión operativa Delegatura Datos Personales

Trámite	Solicitudes		Solicitudes atendidas	
	Ago. 2011 Ago. 2012	Sep. 2012 Sep. 2013	Ago. 2011 Ago. 2012	Sep. 2012 Sep. 2013
Denuncias Habeas Data	2 007	3 510	2 046	3 064

Fuente: Informe de rendición de cuentas 2013, Superintendencia de Industria y Comercio

El ente regulador, además de ordenar la corrección, la actualización o la eliminación de información personal recogida en una base de datos, está facultado para investigar las conductas contrarias a las normas sobre protección de datos personales, con el fin de determinar si procede la aplicación de las sanciones. Por ello, para 2013 se impusieron multas en 230 investigaciones por un valor total de $1 638 millones de pesos.

Dentro de la estrategia implementada por la SIC se incluye implementar un sistema de supervisión basado en riesgo,[185]mediante el cual pueda llegar a hacer un control eficiente, dado el inmenso (y hasta el momento, indeterminado) universo de ficheros o bases de datos para vigilar. Dicho sistema busca aprovechar de manera eficiente la información que se suministre a través del RNBD, para focalizar esfuerzos en la estrategia de vigilancia sobre la información a la que denominó sensible, y a los volúmenes de datos personales con mayor riesgo de verse afectados.

Este sistema de vigilancia se ha denominado Sistema Integrado de Supervisión Inteligente para la Protección de Datos Personales (SISI), a través del cual se pueda llevar a cabo: (i) Un sistema de supervisión basado en riesgos para el ejercicio de las funciones de protección de datos personales a cargo de la Delegatura para la Protección de Datos Personales de la SIC; (ii) unos elementos estratégicos para llevar a cabo el proceso de supervisión, y (iii) una metodología para el desarrollo de futuras guías de supervisión, que se necesitarán a medida que el proceso de

185 La supervisión por riesgos es un concepto nacido del ejercicio de supervisión bancaria durante los años ochenta del siglo xx, entendido como un esfuerzo por parte del supervisor por vigilar, de manera inteligente y prospectiva, un sector en permanente crecimiento y acelerada sofisticación. En tal sentido, la esencia de la supervisión por riesgos parte de la priorización de los objetivos de supervisión, para cubrir aquellas actividades o riesgos de mayor probabilidad de materialización y, a su vez, mayor impacto, dada esa materialización.

supervisión implementado vaya desarrollándose y madurando dentro de la estructura del SISI.

Requerimientos de información y legales para la implementación del RNBD

De acuerdo con la Ley 1581 de 2012, el responsable del tratamiento de una base de datos es la "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"; es decir, será responsable de la información quien tenga a su cargo las decisiones de manejo, finalidad y destino de los datos personales recabados. A su vez, para la Ley 1581 de 2012, el encargado de las bases de datos es la "persona natural o jurídica, que por sí misma o en asocio con otros, realiza el tratamiento de los datos personales por cuenta del responsable del tratamiento", entendido por *encargado* como aquel que maneja, recaba, organiza o manipula la información de las bases de datos, por mandato expreso y según las órdenes dadas por el responsable de la base. Por lo expuesto, la obligación de registrar la base de datos recae sobre el responsable de dicha base, al ser este quien ha decidido su creación, su finalidad, su tratamiento y el uso de los datos allí consignados.

Es optativo del responsable del tratamiento de la base de datos contratar o no a un tercero para que funja de encargado del tratamiento, pues dicha actividad suya propia. En tal caso, es el responsable quien deberá informar y actualizar el RNBD con los datos del encargado.

Según el carácter del responsable del tratamiento, se deberá adelantar el registro de la base de datos, a excepción de las bases de datos señaladas en el artículo 2º de la Ley de Protección de Datos Personales, por lo cual serán objeto de inscripción en el RNBD las bases de Datos cuyo tratamiento, automatizado o manual, sea hecho por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él; en este último caso, siempre y cuando al responsable o al encargado del tratamiento les sea aplicable la legislación colombiana, en virtud de normas y de tratados internacionales.

El proceso de registro debe hacerse de manera independiente por cada una de las bases de datos sujetas a tratamiento, y generarse un código de registro individual, que servirá para identificarlas y poder seguir haciendo actualizaciones sobre ellas.

A su vez, el titular de la información podrá hacer la consulta de las bases de datos que tenga un responsable del tratamiento, así como hallar información sobre la finalidad y los datos de contacto y sobre los canales de atención del responsable o de los encargados del tratamiento, a través de los cuales podrá para ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

El Gobierno Nacional, a través del Ministerio de Comercio, Industria y Turismo, entidad cabeza del sector al que pertenece la SIC, puso en consulta pública, a través de su portal web, desde el viernes 21 de marzo y hasta el martes 8 de abril de 2014, el proyecto de decreto "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, 'por la cual se dictan disposiciones generales para la protección de datos personales' relativo al Registro Nacional de Bases de Datos"[186]. Un proyecto de decreto que a la fecha de elaboración del presente estudio no había sido sancionado.

Ahora bien, en el proyecto de decreto se enuncia la información mínima que se solicitará al momento en el que los responsables de las bases de datos procedan a hacer los registros de las respectivas bases de datos. Dichos requerimientos de información son el resultado de un estudio preliminar dentro de la SIC, donde se busca (además de garantizarle al titular el mayor número de información posible sobre los responsables y los encargados de las bases de datos ante los cuales ejercer su derecho de acceso) recoger información relevante sobre la cantidad de titulares registrados, los tipos de datos que en cada base reposan y las medidas de seguridad que cada responsable aplica en el tratamiento, la custodia y la eliminación de información. Todos ellos son elementos que servirán como fuente principal dentro de un sistema de supervisión basada en riesgos que ha venido construyendo el ente de control.

En el proyecto de decreto se vislumbraron como requisitos mínimos de información que se solicitarán al momento en que se pretenda registrar una base de datos, sin que estos sean impedimento de que se llegue a solicitar más información, los siguientes:

186 Ver anexo 1.

> Artículo 4. Información mínima del Registro Nacional de Bases de Datos. La información mínima que debe contener el Registro Nacional de Bases de Datos es la siguiente:
>
> a. Datos del Responsable del Tratamiento de la Base de Datos;
>
> b. Datos del Encargado del Tratamiento de la Base de Datos;
>
> c. Canales para ejercer derechos;
>
> d. Nombre y finalidad de la Base de Datos;
>
> e. Vigencia de la Base de Datos;
>
> f. Sistema de Tratamiento de la Base de Datos, y
>
> g. Política de Tratamiento de la información.
> **Parágrafo**: La Superintendencia de Industria y Comercio, como autoridad de protección de datos personales y encargada de administrar el Registro Nacional de Bases de Datos, definirá la información adicional que contendrá el mismo.

A continuación se hará un análisis de los requerimientos mínimos propuestos por la SIC en su proyecto de decreto, buscando incluir unos requisitos mínimos de información que se requerirían al momento en que los responsables del tratamiento registren sus bases de datos, así como aquellos requisitos adicionales que, según el esquema de supervisión por riesgo, lleguen a requerirse de acuerdo con los parámetros de seguridad que se lleguen a necesitar en virtud del proceso de supervisión, por riesgos serán solicitados para garantizar información pertinente al proceso de vigilancia del tratamiento de las bases de datos existentes en Colombia.

La información que se propuso registrar está dividida en siete segmentos, los cuales buscan identificar quién es el responsable de la información, con qué finalidad la trata, si lo hace directamente o a través de un encargado, para qué la trata y con qué medidas de seguridad la maneja, así como el tipo y origen del dato, si es objeto de transmisión y a quién se le entrega la base de datos, y si se pretende hacer dicha transferencia a diferentes países.

Validación previa de usuario

De acuerdo con las experiencias registradas en procesos similares de consolidación de bases de datos en Colombia, el proceso de registro implicará el registro de un usuario por cuenta del responsable del tratamiento, quien tendrá una identificación en el sistema y será el único que tenga acceso al sistema del RNBD, para así garantizar, por una parte, que quien accede sea el responsable del proceso y, por otro, evitar el registro indiscriminado y la suplantación de usuarios, así como la incorporación de información falta de veracidad, inexacta y no comprobable.

Por lo anterior, el proceso se iniciará con la solicitud de creación del usuario dentro del aplicativo. Dicho proceso se adelantaría de forma similar a la del sistema de notificación de actos administrativos vía Internet que actualmente funciona en la SIC.

Los medios de recepción de las solicitudes deberán poderse adelantar por medios tanto electrónicos (por el aplicativo o por correo electrónico) como físicos (radicación personal, correo certificado). Sin embargo, tal como lo contempla el artículo 13 del proyecto de decreto del RNBD, el proceso de inscripción de los usuarios no fue incluido en el documento, buscando que la SIC informe posteriormente sobre el proceso mismo de registro y validación de usuarios en el *software* o el programa que se deje a disposición para soportar y adelantar los trámites pertinentes al registro.

Responsable del tratamiento

Una vez creado el usuario en el sistema, la primera información que consignar en el diligenciamiento del RNBD es la identificación del responsable del tratamiento; es decir, la persona natural o jurídica de naturaleza privada o pública que hace el tratamiento de una base de datos personales creada en ejercicio de la actividad económica y como fruto de esta.

Teniendo presente que las bases de datos o los archivos mantenidos en el ámbito netamente personal no están obligadas a ser objeto de registro, y toda vez que las personas naturales que están registrando sus bases lo hacen en virtud de una actividad comercial o profesional o de un oficio que ejercen, la información que registren dentro de los datos de identificación del responsable de la base de datos

debe corresponder a la dirección, el teléfono y el correo electrónico que tengan en virtud de su profesión o su oficio.

La información que se debe registrar en dicho apartado busca identificar al responsable, por lo cual los campos por solicitar son:

1. Nombre completo o razón social; número de identificación tributaria (NIT), en el caso de personas jurídicas, y cédula de ciudadanía o cédula de extranjería, en el caso de personas naturales. También: correo electrónico de contacto, teléfono y dirección de notificación judicial de la empresa, con el fin de poder establecer contacto. Adicionalmente, deberán indicarse el número de matrícula mercantil y el código de la Cámara de Comercio.
2. Actividad económica: de acuerdo con las convenciones establecidas en el Código Industrial Internacional Uniforme (CIIU), mediante el registro de esa casilla, se busca establecer y sectorizar, por la actividad que desarrollan, a los responsables de la información, así como usar esta para, junto con la finalidad de la base de datos que se registra, establecer estrategias y programas de control sobre los vigilados. Adicionalmente, a través del mencionado dato, se podrá empezar a habilitar la implementación del RNBD por sectores, y facilitar así la puesta en marcha del registro.

Los requerimientos legales que conlleva la implementación de este apartado requieren desarrollar el concepto según el cual la finalidad del RNBD es registrar las bases de datos y los archivos que tengan personas naturales y jurídicas de naturaleza pública o privada sobre datos personales que se posean en ejercicio de una actividad económica, profesional o misional del responsable de esta, en concordancia y desarrollo del principio de uso restringido de la información, así como el que se ha denominado *principio de calidad de los datos*, establecido expresamente en la ley, y según el cual

> […] los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido[187].

187 Congreso de la República de Colombia, *Ley 1581 de 2012, o Ley de Protección de Datos Personales*, artículo 4º.

Igualmente, y dada la posibilidad que tendrá el responsable de inscribir a su nombre a un administrador y a un usuario del sistema del RNBD, deberá registrar los datos de identificación y de contacto de estos, para generar accesos personalizados, pero bajo entera responsabilidad del obligado (responsable del tratamiento). En esta parte del proceso, el responsable deberá incluir los datos de la persona natural o jurídica que hará la función de encargado del tratamiento.

De acuerdo con la reglamentación en materia de protección de datos, precisamente, la información que reporte el responsable de las bases de datos que sean personas naturales deben abstenerse de incorporar información personal, como información de contacto, en el proceso de inscripción de las bases de datos que se tengan, pues las personas naturales que están registrando sus bases solo deben hacerlo en virtud de una actividad comercial o profesional o de un oficio que ejercen. Por ello, la información que se registre en calidad de responsable de la base de datos debe corresponder a la dirección, el teléfono y el correo electrónico que se tengan en virtud de una profesión o un oficio.

Canales para ejercer derechos

Los derechos de conocer, actualizar, rectificar, incluir o excluir datos personales, así como de revocar la autorización dada para su tratamiento ante el responsable o el encargado del tratamiento, son la principal garantía del derecho de protección de datos. En el presente apartado se registrarán los datos de contacto ante los cuales el titular puede ejercer los derechos ante las dependencias de la misma entidad, sea persona jurídica o natural, por lo cual se solicita el nombre de la oficina y los datos de contacto de la persona ante la cual podrán acceder los titulares para ejercer sus derechos.

De acuerdo con ello, y tal como lo señala el artículo 7 del proyecto de decreto mediante el cual se busca reglamentar el RNBD, los canales de atención son todos los medios de recepción y atención de peticiones, consultas y reclamos que el responsable y el encargado del tratamiento deben dejar a disposición de los titulares de información (atención personalizada en oficina, sucursal o punto móvil, atención por vía telefónica, portal web, fax, correo electrónico, etc.), con los respectivos datos de contacto por medio de los cuales el titular puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir sus datos personales

contenidos en bases de datos, y a revocar la autorización que hayan otorgado para el tratamiento de dichos datos.

En todos los canales habilitados se debe prever, como mínimo, la posibilidad de que el titular ejerza sus derechos a través del mismo medio por el cual fue recogida su información, y deje constancia de la recepción y del trámite de la respectiva solicitud.

En caso de que el tratamiento de datos esté siendo hecho por un encargado, el responsable registrará la información de contacto del encargado, para que sea este ante quien se adelante el ejercicio de los derechos de conocer, actualizar, rectificar, incluir, excluir datos personales, así como el de revocar la autorización dada para su tratamiento.

Identificación y finalidad de la base de datos, vigencia de la base de datos y estado del registro

Mediante el diligenciamiento de estos apartados, el responsable del tratamiento de la base de datos deberá brindar la información necesaria para establecer el nombre de la base y la finalidad para la cual fue creada, y que deberá incluir la descripción de su uso, además de escoger, de acuerdo con dicho uso, un código de parametrización, preestablecido en el RNBD, que permita determinar la vocación de la base del caso.

Igualmente, en el aún proyecto de decreto queda establecida la incorporación de la información relativa a la vigencia de la base de datos, la cual debe estar relacionada y en cumplimiento de lo establecido en la finalidad de la base.

Además de lo anterior, mediante este apartado del RNBD la autoridad de protección de datos podrá registrar la suspensión de la operación de la base de datos, su cierre temporal, o, incluso, definitivo, como consecuencia de la imposición de sanciones, producto, a su vez, de un proceso de investigación en el cual se determine que el tratamiento de la base de datos ha incumplido las normas vigentes y los derechos de los titulares, según el proyecto de ley. También se podrán registrar las posibles violaciones que se susciten a los códigos de seguridad, y los riesgos en la administración de la información, de acuerdo con las obligaciones establecidas en los artículos 17 y 18 de la Ley 1581 de 2012 a los responsables y a los encargados del tratamiento, respectivamente.

Con el fin reglamentar este apartado de acuerdo con las obligaciones del responsable y las del encargado del tratamiento, específicamente, la SIC deberá definir los tipos de alertas y los tiempos máximos a lo largo de los cuales los responsables y los encargados deben reportar la vulneración de sus sistemas y sus códigos de seguridad en la administración de la información.

Tipos de datos, sistema de tratamiento, ubicación y nivel de seguridad

En este apartado, el responsable señalará qué tipo de dato está tratando cada una de las bases de datos que posee. El formulario de registro permitirá desplegar las opciones generales, como: si tiene datos de la edad de las personas; datos de ubicación y de contacto; datos relativos al estado de salud; datos relativos al sistema de afiliación al sistema general de salud; datos sobre condiciones de pobreza, discapacidad, afiliación a organizaciones sindicales, minorías étnicas, organizaciones sociales o políticas, o datos biométricos. En general, a raíz de la información recolectada se podrá establecer si el tratamiento de datos se hace sobre datos públicos, sobre datos semiprivados, sobre datos privados o sobre datos privados sensibles. Todo ello, con el fin de establecer desde un inicio cuáles bases de datos manejan datos con un mayor nivel del riesgo, dada la tipología del dato, y así poder dejar abiertas en el sistema opciones de mayor control, si se llegan a requerir ante los diferentes tipos de datos y de bases.

En este apartado también se registrará el sistema de tratamiento en el cual el responsable del tratamiento ha consolidado y trata sus bases de datos; es decir, si lo hace mediante algún tipo de sistema operativo, o si, por el contrario, la lleva de manera manual. Dicha información permitirá perfilar el control y las medidas de seguridad que deben cumplir los responsables y los encargados en el tratamiento de los datos personales. A su vez, deberán informar si la base de datos se encuentra en servidores propios, externos o tercerizados, así como las medidas de respaldo con las que cuenta la información.

Una vez se diligencie este apartado, el RNBD arrojará una alerta al responsable, en la cual le advertirá que, de acuerdo con el volumen y el tipo de información, debe tener y mantener unas medidas de seguridad y un nivel de seguridad determinados, tal como lo advierte el artículo 25 de la Ley 1581 de 2012.

Finalmente, en el proceso de reglamentación del RNBD, es importante destacar que la SIC deberá expedir una circular o un instructivo en el cual se defina la seguridad con la que se debe hacer el tratamiento de la información personal depositada en las base de datos por registrar, dependiendo del tipo de dato y del volumen de personas que contenga la base de datos. Para ello, se debe analizar qué tipo de información maneja la base y el volumen o la cantidad de registros que contiene. Dicho protocolo de seguridad se podrá hacer exigible a quienes traten datos personales, y ello permitiría, además de orientar a los obligados sobre las medidas de seguridad que deben tener, usarlo para verificar el nivel de cumplimiento del deber de seguridad que les exige la norma a los obligados.

De acuerdo con lo definido en el proyecto de decreto, en el parágrafo del artículo 11, la SIC impartirá las instrucciones relacionadas con las medidas de seguridad en el tratamiento de datos personales, y solo a partir de ese momento será exigible la inscripción de la respectiva política de tratamiento.

Política de tratamiento de la información

El documento que constituya la política de tratamiento de la información personal que posean y usen los responsables y sus encargados deberá adjuntarse en el proceso de registro de las bases de datos, pues será mediante esta como la SIC verificará en primera instancia si el tratamiento de las bases se está haciendo según procesos preestablecidos y concordantes con los principios de la protección de datos y los deberes exigidos a los responsables.

Dicha política obligará tanto al responsable como al encargado de la base de datos, y deberá tener los requisitos de información mínima exigida por el ente de control. De acuerdo con el artículo 11 del proyecto de decreto que reglamenta el RNBD, la información mínima que debe incluir la política de tratamiento que cada responsable implemente será:

1. Nombre, o denominación social o razón social de la persona natural o jurídica responsable del tratamiento de la base de datos.
2. Nombre y finalidad de la base de datos.
3. Persona o dependencia responsable de la atención de peticiones, consultas y reclamos ante la que el titular de la información puede ejercer sus

derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

4. Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
5. Fecha de entrada en vigencia de la política de tratamiento de la información y periodo de vigencia de la base de datos.
6. Nivel de medidas de seguridad aplicado al tratamiento de la base de datos.

Como se observa, la política de tratamiento recoge la información mínima que debe conocer el titular del dato sobre el uso, la finalidad y el procedimiento que tiene implementado para ser atendido ante dudas o en caso de que requiera presentar un reclamo. Así mismo, busca brindar un nivel de conocimiento sobre las medidas que usa la empresa o la entidad en el tratamiento de la información personal; sin embargo, al no estar definidos por la SIC los protocolos de seguridad que deben cumplir los obligados, estos aún no quedan obligados a registrar la política de tratamiento, tal como se explicó líneas arriba y lo señala el parágrafo del artículo 11 del proyecto de decreto.

Finalmente, el plazo de inscripción señalado por el decreto reglamentario, aún en discusión, es de los seis meses siguientes a la fecha en la cual la SIC habilite el registro, y de dos meses, contados a partir de su creación, para las bases de datos que se creen.

Temas no incluidos en el proyecto de Decreto que busca reglamentar el RNBD

Si bien en el proyecto de decreto que busca reglamentar el registro de bases de datos no fueron incluidos temas como la procedencia del dato (es decir, si el dato se recogió directamente del titular o si fue producto de una cesión o de una trasmisión de la base de datos por parte de otro responsable, así como si dicha cesión se hizo gratuitamente, o si, por el contrario, fue producto de un venta de información), tal información resulta de especial interés al momento en el que la autoridad de protección de datos, en ejercicio de sus facultades de vigilancia, quiera saber sobre el origen del dato.

De acuerdo con lo anterior, otro tema que no quedó regulado en el proyecto de decreto fue lo referente a la cesión de datos; o sea, si la información de la base

de datos personales fue recogida por un responsable y entregada a otra sociedad u otra entidad (otro responsable), y si dicha cesión fue o no autorizada por el titular al momento de consentir su tratamiento.

A través del registro de la procedencia del dato y de la cesión de las bases de datos, se pueden tener elementos de juicio que permitan establecer a la autoridad de vigilancia y control, así como a los titulares, si las bases de datos y las empresas o las entidades a las cuales entregaron su información la han entregado.

Mediante el registro del origen y cesiones de los datos, también se podría establecer la existencia o no de la autorización por parte del titular del dato, pues la autorización, al ser previa e informada, debe haberse otorgado a sabiendas de si su información podía ser cedida o no, por lo que si en el registro se obliga a registrar cualquier cesión o recepción no autorizadas de información, ello podría ser un claro indicativo de un tratamiento no autorizado y, por lo tanto, ilegal. También permitirá establecer cuál fue el medio por el cual el titular de la información otorgó la autorización (papel, medio informático, telemático u otro).

Por último, frente a la obligación legal impuesta en el artículo 27 de la Ley 1581 de 2012, de regular lo referente a las normas corporativas vinculantes y a las transferencias internacionales, se encuentra cómo, además de que, a la fecha de elaboración de la presente investigación, el Gobierno Nacional no ha emitido reglamentación alguna, también, notoriamente, en el proceso de facilitar el acceso a la información por parte de los titulares y de garantizar la efectiva vigilancia por parte de la SIC, no se incluyó dentro del RNBD, como sí lo hacen en otros países, el registro mediante un apartado especial, ni la obligación de registrar la existencia de normas tipo ni normas corporativas vinculantes, ni de las transferencias internacionales de datos.

Considerando que las normas corporativas vinculantes están encaminadas a que una tercera entidad u organismo, distinto del ente de control, certifique la implementación y el cumplimiento, por parte de sociedades y de entidades, de los parámetros exigidos por la regulación de protección de datos del país, resulta importante que se incluyan y se reglamenten las actividades de los entes certificadores que terminarán complementando, al mejor estilo del modelo norteamericano, la labor de control a la regulación del Estado.

Por lo anterior, resulta de especial interés que el Gobierno Nacional determine la manera como adelantará el control sobre dichos entes certificadores, y

si se va a crear un nuevo registro que apoye la supervisión de estos, así como el cumplimiento de normas corporativas vinculantes, o si, por el contrario, serán incluidos dentro del sistema de verificación creado a partir del RNBD.

Como se observa, tanto la Ley 1581 de 2012 como su Decreto Reglamentario No. 1377 de 2013 fueron escuetos y, simplemente, no desarrollaron a profundidad el tema; a cambio, se dejó abierta la posibilidad de que, vía subsiguientes decretos, se reglamentara en su integridad la materia, bajo el derrotero de "siempre y cuando se ajuste a los principios que rigen el tratamiento de los datos personales".

La Corte Constitucional hizo un análisis sobre lo revisado por el Grupo de Trabajo del Artículo 29, el cual señaló cómo las normas corporativas vinculantes se utilizan en el contexto de las transferencias de datos internacionales, como manifestación clara del principio de responsabilidad, en la medida en que son autorregulaciones de conducta que redactan y siguen las organizaciones multinacionales, y que deben contener las medidas para poner en práctica y hacer realizables los principios para la protección de datos, tales como la auditoría, los programas de formación, la red de funcionarios de privacidad y el sistema de tratamiento de quejas, entre otros.

Con la inclusión de normas corporativas vinculantes y de transferencia internacionales con una óptica más liberal y menos ajustada al control del ente de vigilancia, se vislumbra que el legislador pretendió acompañar la política de protección y control del tratamiento de datos personales con la existencia de procedimientos y adaptaciones privadas de la norma general, que, por ser voluntarias, obliguen a quienes se adhieren a ellas a su cumplimiento. Ello no implica el no sometimiento de las empresas y las entidades certificadas de estas prácticas autovinculantes a las estrategias de control de la autoridad de protección de datos personales.

Si bien las tácticas de autorregulación por parte de los responsables del tratamiento de la información se deben ajustar a los principios y los lineamientos desarrollados por la normatividad, se deben reflejar dentro de cada política de privacidad de los particulares, de las empresas y de los profesionales que se hayan adherido a esta. Por ello, el proceso de vigilancia del correcto tratamiento de información personal, si bien podría partir de la premisa de que quienes se allanen a ese código de conducta, emitido por una empresa certificadora, están cumpliendo con los mandatos de la ley, dichas sociedades no pueden quedar por

fuera del control de la autoridad de protección de datos, y se hace necesario que todas y cada una de las normas vinculantes sean sometidas a su aprobación por parte del ente de control y deban cumplir con una reglamentación especial que garantice el cumplimiento de la norma de protección de datos. Sin embargo, por lo que hasta el momento se está desarrollando en Colombia, no se ha determinado la obligatoriedad del registro ni de la aprobación de los códigos de conducta y buenas prácticas dentro del RNBD, lo que implicaría una pérdida del control de la protección de los datos personales y de la misma autoridad de control.

Conclusiones

La política española frente a la protección de los datos personales y la regulación de su tratamiento están determinadas por la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos. El desarrollo y la estrategia de vigilancia fueron implementados en España a través de la LOPD 15 de 1999, y su reglamentación, a través del Real Decreto 1720 de 2007, terminó de ajustar su implementación con el modelo europeo transpuesto, dado el carácter de país miembro del Comunidad Europea de Naciones.

La influencia del modelo de vigilancia y control de España sobre el modelo planteado en Colombia es evidente. Colombia, a través de la estrategia trazada en la Ley 1581 del 17 de octubre de 2012, incorporó en el ordenamiento colombiano fundamentos básicos del modelo europeo, como la creación de un ente de la vigilancia y control, la incorporación de principios propios que regentan la protección de datos personales (como el principio de veracidad o calidad del dato, y los de finalidad, seguridad, circulación restringida), como los más relevantes, así como, la categorización de datos personales cuyo uso pueda generar discriminación o trate información de menores, como datos personales especiales dada su sensibilidad. Así mismo, como influencia del modelo español, la nueva ley colombiana de protección de datos personales estableció la creación de un RNBD, tal como España incorporó el Registro General de Protección de Datos.

La implementación en Colombia del RNBD, de acuerdo con el proyecto de decreto puesto a consideración de la opinión pública en marzo de 2014, abordó

aspectos como: (i) la individualización del responsable y del encargado del tratamiento de la base de datos; (ii) los canales o el medio de contacto para que los titulares de los datos personales ejerzan sus derechos; (iii) la identificación, la finalidad y la vigencia de la base de datos, y el estado del registro de dicha base; (iv) los tipos de dato, el sistema de tratamiento, la ubicación y el nivel de seguridad de la base de datos, y (v) la política de tratamiento de la información. Dicha inclusión es concordante con la propia Ley de Protección de Datos Personales, pero resulta mínima frente a los requerimientos de control del modelo europeo.

Pese a lo anterior, con el proyecto de decreto se deja claro que es obligación de todos los responsables del tratamiento, ya sean personas jurídicas de derecho público o privado, registrar bases de datos. Así mismo, definió los contenidos mínimos, o parámetros generales, que debe contener la política de protección de datos que cada responsable implemente, y obliga al responsable a declarar qué tipo de dato y qué tratamiento les está dando, según la finalidad para la cual fueron recogidos, y esta es la principal herramienta de control del tratamiento, pues cualquier uso diferente del señalado será fácilmente probado y sancionado.

Ahora bien, aunque Colombia estableció la existencia de normas vinculantes que les permitan tanto a los gremios como a las empresas privadas la construcción de sus propias normas que regulen el tratamiento de los datos personales, siempre y cuando se enmarquen dentro de los principios y los lineamientos de la Ley de Protección de Datos Personales, no conminó, como sí lo hizo España, a que dichas normas tipo, o normas autovinculantes, fueran registradas en el RNBD, y dos años después de promulgada la Ley 1581 de 2012, el tema sigue sin regulación.

Al respecto, aunque España tiene incorporada la existencia de códigos tipo o normas de autorregulación de agremiaciones de profesionales, su incorporación en el RGPD no ha sido importante, ni su uso masificado, según las propias página web y las estadísticas de la AEPD.

Se puede concluir que, si bien Colombia ha desarrollado su jurisprudencia y su normatividad garantizando la protección y el ejercicio del derecho de las personas a preservar su información personal y familiar por fuera del ámbito público, y aunque ha basado su modelo de control de protección de los datos personales en el modelo europeo (sobre todo, en el español), la falta de interiorización del derecho por parte de los gremios económicos y la laxitud del titular del dato han llevado a que el modelo estadounidense de normas sectoriales y

de autorregulación, como las certificaciones privadas o las normas corporativas vinculantes para el tratamiento de los datos personales, vayan adquiriendo una mayor importancia.

Esa tendencia norteamericana se halla ampliamente ahincada en Colombia, dada la gran influencia de ese país en el comercio y en las estrategias de desarrollo económico colombianos y suramericanos, y por la demora en el pronunciamiento, por parte del ente de control, sobre estas materias, todo lo cual hace de dichas tácticas de autorregulación una estrategia llamativa de protección de los datos personales; sobre todo, para las grandes empresas y los conglomerados económicos, y así se deja que el titular del dato a merced de las empresas desarrolle normas propias, certificadas por entes de certificación y de auditorías privadas. Tal situación puede llegar a ser reprochable en un modelo que busque, ante todo, la garantía del derecho fundamental, a través de un ente de control estatal.

A título personal, y todavía sin un desarrollo reglamentario en la materia, creo que Colombia fortalecerá la aplicación de normas vinculantes y de estrategias autorregulatorias que dinamicen y faciliten la adecuación de la nueva norma, aunque se pierda rigor en la eficiencia del control del tratamiento de los datos personales, en desarrollo una estrategia hacia el modelo norteamericano.

Para terminar, cabe tener presente que en Colombia, desde hace por lo menos una década, se han venido desarrollando aproximaciones sectoriales en el tratamiento de información personal. Esto, en razón a la influencia de los diferentes gremios de la economía que han venido desarrollando estrategias propias, que faciliten el tratamiento de la información personal de los clientes y de los usuarios. Ello, sumado a la falta de compromiso personal y social en el cuidado de los datos personales, marcará, con seguridad, una diferencia importante respecto a lo pretendido a la hora de buscar la implementación y el desarrollo de la política de protección de datos personales.

La sociedad colombiana, en su gran mayoría, considera que los datos personales son públicos, y el desarrollo normativo hasta antes de la nueva ley (2012) dejó ver que no todos los datos personales tienen una connotación privada, situación que dificulta implementar una cultura de protección de los datos personales, por lo cual una estrategia de imposición de la norma no es suficiente; quizás, lo más importante sea la estrategia de concientización. Así pues, con el ánimo de que la Ley de Protección de Datos Personales cumpla con los objetivos previstos,

es importante que la autoridad de control enfoque sus esfuerzos en la tarea de sensibilización, divulgación y capacitación, tanto de las personas o los titulares de la información como de las empresas, los gremios, las asociaciones y entes públicos, para que conozcan los derechos y los deberes que trajo consigo la nueva ley, pero también, que tienda programas de acompañamiento en el montaje y el desarrollo de las políticas de privacidad y manuales de seguridad para la información de pequeños y medianos empresarios; también, que endurezca el control, de manera focalizada, sobre los gremios. Pero, sin duda, el más importante propósito por cumplirse es que las personas reconozcan en este derecho la importancia que tiene para su vida personal, familiar y social.

Anexos

Que en el ámbito internacional, los países que han implementado la creación de un registro de bases de datos, han conseguido obtener una herramienta de supervisión del cumplimento de los deberes legales a cargo de los responsables del Tratamiento de datos.

Que el Registro Nacional de Bases de Datos permitirá cumplir con la obligación legal de difundir y dar publicidad a la existencia de Bases de Datos de carácter personal y servirá de herramienta de verificación y vigilancia para la efectiva protección del derecho de hábeas data.

DECRETA

CAPÍTULO I. DISPOSICIONES GENERALES

Artículo 1. ***Ámbito de aplicación.*** Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las Bases de Datos cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable o al Encargado del Tratamiento les sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2 de la Ley 1581 de 2012.

Artículo 2. ***Deber de inscribir las Bases de Datos.*** El Responsable del Tratamiento debe inscribir en el Registro Nacional de Bases de Datos, de manera independiente, todas y cada una de las Bases de Datos sujetas a Tratamiento.

Artículo 3. ***Consulta del Registro Nacional de Bases de Datos.*** Los ciudadanos podrán consultar en el Registro Nacional de Bases de Datos, las Bases de Datos que posea un Responsable del Tratamiento, su finalidad y la información de contacto para ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

CAPÍTULO II. EL REGISTRO NACIONAL DE BASES DE DATOS

Artículo 4. ***Información mínima del Registro Nacional de Bases de Datos.*** La información mínima que debe contener el Registro Nacional de Bases de Datos es la siguiente:

a) Datos del Responsable del Tratamiento de la Base de Datos;

b) Datos del Encargado del Tratamiento de la Base de Datos;

c) Canales para ejercer derechos;

d) Nombre y finalidad de la Base de Datos;

e) Vigencia de la Base de Datos;

f) Sistema de Tratamiento de la Base de Datos, y

g) Política de Tratamiento de la información.

Parágrafo: La Superintendencia de Industria y Comercio, como autoridad de protección de datos personales y encargada de administrar el Registro Nacional de Bases de Datos, definirá la información adicional que contendrá el mismo.

Artículo 5. ***Responsable del Tratamiento de la Base de Datos.*** Cuando el Responsable del Tratamiento de la Base de Datos sea una persona jurídica, deberá indicar su denominación o razón social y su número de identificación tributaria. Cuando el Responsable del Tratamiento sea una persona natural, la información que registre dentro de los datos de identificación debe corresponder a aquella considerada como de naturaleza pública, de acuerdo con las normas vigentes.

Artículo 6. ***Encargado del Tratamiento de la Base de Datos.*** Cuando el Encargado del Tratamiento de la Base de Datos sea una persona jurídica, deberá indicar su denominación o razón social completa y su número de identificación tributaria. Cuando el Encargado del Tratamiento sea una persona natural, la información que registre dentro de los datos de identificación debe corresponder a aquella considerada como de naturaleza pública, de acuerdo con las normas vigentes.

Artículo 7. ***Canales para ejercer derechos.*** Son los medios de recepción y atención de peticiones, consultas y reclamos que el Responsable y el Encargado del Tratamiento deben poner a disposición de los Titulares de información, con los datos de contacto respectivos, por medio de los cuales el Titular puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir sus datos personales contenidos en Bases de Datos y revocar la autorización que hayan otorgado para el Tratamiento de los mismos. Estos canales deben prever, por lo menos, la posibilidad de que el Titular ejerza sus derechos a través del mismo medio por el cual fue recogida su información, dejando constancia de la recepción y trámite de la respectiva solicitud.

En los casos en que el Tratamiento de datos lo realice el Encargado, el Responsable registrará la información de contacto del Encargado para que el Titular pueda adelantar ante este el ejercicio de sus derechos.

Artículo 8. ***Nombre y finalidad de la Base de Datos.*** El Responsable del Tratamiento identificará cada una de las Bases de Datos que inscriba, de acuerdo con la finalidad para la cual fueron creadas y deberá describir su objeto y especificar los usos para los cuales se crearon.

Artículo 9. ***Vigencia de la Base de Datos.*** Es el término previsto por el Responsable para el Tratamiento de datos personales, de acuerdo con la finalidad para la cual se creó la Base de Datos. Una vez expirada la vigencia se debe proceder a eliminar la Base de Datos.

Artículo 10. ***Sistema de Tratamiento.*** Los datos personales contenidos en Bases de Datos podrán ser tratados de manera sistematizada o manual. Son Bases de Datos manuales aquellas cuya información se encuentra organizada y almacenada de manera física y Bases de Datos automatizadas aquellas que se almacenan y administran con la ayuda de herramientas informáticas.

DECRETO NÚMERO _____ de 2012 **Hoja Nº. 4 de 5**

Continuación del decreto "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, 'por la cual se dictan disposiciones generales para la protección de datos personales' relativo al Registro Nacional de Bases de Datos."

Artículo 11. ***Política de Tratamiento de información.*** La información mínima que debe contener la Política de protección de datos que cada responsable de Bases de Datos implemente, será la siguiente:

a) Nombre o denominación social o razón social de la persona natural o jurídica Responsable del Tratamiento de la Base de Datos.

b) Nombre y finalidad de la Base de Datos.

c) Persona o dependencia responsable de la atención de peticiones, consultas y reclamos ante la cual el Titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

d) Procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.

e) Fecha de entrada en vigencia de la Política de Tratamiento de la información y período de vigencia de la Base de Datos.

f) Nivel de medidas de seguridad aplicado al Tratamiento de la Base de Datos.

La Superintendencia de Industria y Comercio impartirá las instrucciones relacionadas con las medidas de seguridad en el Tratamiento de datos personales.

Parágrafo: La inscripción de la Política de Tratamiento de información solo será exigible una vez que la Superintendencia de Industria y Comercio imparta las instrucciones relacionadas con las medidas de seguridad en el Tratamiento de datos personales.

CAPÍTULO III. TÉRMINOS Y CONDICIONES DE INSCRIPCIÓN EN EL REGISTRO NACIONAL DE BASES DE DATOS

Artículo 12. ***Plazo de inscripción.*** Los Responsables del Tratamiento deberán adelantar la inscripción de sus Bases de Datos en el Registro Nacional de Bases de Datos dentro de los seis (6) meses siguientes a la fecha en que la Superintendencia de Industria y Comercio habilite el Registro. Las Bases de Datos que se creen con posterioridad a ese plazo, deberán ser inscritas dentro de los dos (2) meses siguientes, contados a partir de su creación.

Artículo 13. ***Inscripción de las Bases de Datos.*** La Superintendencia de Industria y Comercio establecerá el procedimiento de inscripción en el Registro Nacional de Bases de Datos que deberán cumplir los Responsables del Tratamiento, previa validación de su identidad, de acuerdo con lo que para el efecto establezca esa entidad.

Artículo 14. ***Actualización de la información contenida en el Registro Nacional de Bases de Datos.*** Los Responsables del Tratamiento de las Bases de Datos deberán actualizar en el Registro la información inscrita cuando haya cambios sustanciales y deberán reportar el hecho de que la Base de Datos ha sido dada de baja antes de la expiración de su vigencia.

DECRETO NÚMERO _____ de 2012 **Hoja N°.** 5 de 5

Continuación del decreto "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, 'por la cual se dictan disposiciones generales para la protección de datos personales' relativo al Registro Nacional de Bases de Datos."

Artículo 15. ***Vigencia.*** El presente decreto rige a partir de su publicación en el Diario Oficial.

PUBLÍQUESE Y CÚMPLASE
Dado en Bogotá, D.C., a los

EL MINISTRO DE COMERCIO, INDUSTRIA Y TURISMO

SERGIO DÍAZ-GRANADOS GUIDA