PROCEDIMIENTO PARA PROTEGER LOS DATOS PERSONALES EN UNA ENTIDAD PÚBLICA

CAROLINA VÉLEZ RESTREPO

NATALIA PÉREZ MONTOYA

Artículo presentado como requisito de grado para optar título de Abogado

Asesor:

LUÍS CARLOS MARTÍNEZ MESA

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS

FACULTAD DE DERECHO

MEDELLÍN

2018

PROCEDIMIENTO PARA PROTEGER LOS DATOS PERSONALES EN UNA ENTIDAD PÚBLICA

Carolina Vélez Restrepo[1]

Natalia Pérez Montoya[2]

Resumen

El texto es un acercamiento al procedimiento que deben realizar las entidades públicas para la protección de datos personales. Aquí se exponen, como parte introductoria, las definiciones para un mayor entendimiento sobre los datos, sujetos intervinientes en el tratamiento de la información y las dos protecciones que los datos personales tienen a raíz de la Constitución Política de 1991. Igualmente, el Gobierno Nacional por medio de leyes y decretos, afianza el tema e induce al amparo que deben tener. El procedimiento se fundamenta en la implementación y cumplimiento de seis pasos que se deben seguir para la elaboración de esa protección por parte de las entidades públicas. Lo anterior tiene como finalidad el cumplimiento de la ley y el respeto que los titulares de la información deben tener, so pena de incurrir en violaciones legales y una eventual sanción pecuniaria.

Palabras clave: Datos, Entidades Públicas, Habeas Data, Titulares, Bancos de Información.

[1] Aspirante al título de Abogada Universidad Pontificia Bolivariana. Email: carovelezrpo@gmail.com

[2] Aspirante al título de Abogada Universidad Pontificia Bolivariana. Email: natymonto@hotmail.com

Abstract

The text is an approach to the procedure to be performed by public entities for the protection of personal data. Here are presented, as an introduction, the definitions for a better understanding of the data, the subjects involved in the treatment of information, and the two types of protection over personal data resulting from the Political Constitution of 1991. Similarly, the National Government strengthens the issue and encourages the protection by means of laws and decrees. The procedure is based on the implementation and fulfillment of six steps that must be followed for the preparation of this protection by public entities. The foregoing is intended to comply with the law and the respect that the holders of the information must have, under penalty of incurring legal violations as well as a possible financial penalty.

Keywords: Data, Public Entities, Habeas Data, Headlines, Information Banks.

Introducción

El Derecho de Habeas Data es un derecho fundamental, que según la Constitución Política de Colombia es: “el 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” (Constitución Política de Colombia, 2018, Art. 15).

La protección Constitucional del Habeas Data se soporta a su vez en varios pronunciamientos que ha hecho la Corte Constitucional, la cual ha confirmado que este derecho debe tener una especial protección en comparación con los demás derechos; motivo por el cual en los últimos años se han ido creando nuevas normas que facilitan su custodia, llegando a establecer incluso sanciones que permiten lograr el cumplimiento de las disposiciones.

En el ejercicio de la regulación que busca proteger el Derecho de Habeas Data, se estableció que la entidad encargada de su vigilancia sería la Superintendencia de Industria y Comercio, entidad que creó el Registro Nacional de Bases de Datos, mecanismo que logra la protección de los datos personales, ya que en dicha plataforma deben registrarse todos los datos personales a los cuales tienen acceso las personas y entidades obligadas a cumplir con las disposiciones.

Es necesario que para dar cumplimiento a las normas creadas en razón de la protección del Derecho de Habeas Data, se realice un procedimiento en el cual deben estar plasmadas cada una de las disposiciones que se han establecido; por tal motivo se presenta un modelo de procedimiento que va dirigido especialmente a las entidades públicas, pero que también puede llegar a cumplir con las necesidades y expectativas de otro tipo de entidad o persona que lo requiera.

Definición y Protecciones

La información que recae sobre las bases de datos de las entidades sin importar su naturaleza posee una protección especial, es decir, no solo los titulares o personas que brindan esa información se encuentran protegidas por la Constitución Política, sino que también por la Ley 1581 del 2012, la cual regula todo lo relacionado con la información emitida, su distribución y almacenamiento.

Se debe analizar la importancia de esta regulación a la luz de la Constitución Política de Colombia, toda vez que es allí donde encuentra el fundamento y sin el cual es vago precisar su concepción y proyección dentro del ordenamiento.

La primera protección Constitucional se encuentra en el Título II: “De los derechos, las garantías y los deberes” en el Capítulo I: “De los derechos fundamentales”, el artículo 15, el cual reza lo siguiente:

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley (Constitución Política de Colombia, 2015, Art. 15).

El artículo consagra como derecho fundamental la protección que las personas deben tener frente a la información suministrada y almacenada por los bancos de datos, asemejándolo al derecho de la intimidad personal. Es decir, que se encuentra relacionado con la esfera privada de las personas y requiere una mayor atención.

Los datos personales, es una información "asociada a una persona y que permite su identificación" (Superintendencia de Industria y Comercio, 2018). Puede estar ligados a varias personas o a una determinada, y admiten una clasificación:

Datos Públicos: son los datos personales de carácter público cuando la Ley o la Constitución lo establezcan. Igualmente serán los contenidos en documentos públicos, en lo relativo al estado civil de las personas y en sentencias judiciales ejecutoriadas.

Datos Semiprivados: son los que no tienen característica de datos reservados, ni íntimos, ni públicos. Este tipo de datos pueden ser de conocimiento por la sociedad, por cierto tipo de personas o por el titular mismo.

Datos Privados: son los datos que se encuentran en la esfera íntima del titular, esto es, son datos que solamente le interesan al titular que los proporcionó. Son reservados o íntimos.

Datos Sensibles: son los datos que afectan directamente la intimidad del titular.

Todos esos datos, son suministrados por las personas en sus actividades cotidianas, y por ende amerita una mayor protección al tratarse del ámbito privado de las personas. Es por ello que existen seis principios rectores que son utilizados como pilares, los cuales son:

- Principio de la Finalidad
- Principio de la Circulación Restringida
- Principio de la Temporalidad de la Información
- Principio de la Interpretación Integral de los Derechos Constitucionales
- Principio de la Seguridad
- Principio de la Confidencialidad de la Información Suministrada.

Toda la información contenida debe tener una finalidad legítima reglada a la luz de la Constitución y la Ley. Esto debido al tipo de dato transmitido, ya que, solo los catalogados como públicos pueden circular libremente. Se debe precisar que los otros tipos de datos deben contar con una debida autorización para su divulgación.

Todas las bases de datos deben garantizar la custodia y discreción de la información, so pena de violar lo contenido en la Constitución, relacionado con la libertad y las garantías consagradas.

Estos principios son la base para la protección que tiene como derecho el titular. La adquisición, circulación y el manejo de la información debe tener una trasparencia constitucional y legal, cuya finalidad sea respetar a las personas vinculadas en la circulación y administración de la información.

Posterior a la definición, es necesario inmiscuirnos en el tema y precisar cuáles son los sujetos intervinientes.

El primero de ellos es el titular de la información, éste se encarga de facilitar la información contenida en las bases de datos. Son personas naturales que pueden conocer, actualizar, rectificar y revocar toda la información proporcionada.

El segundo sujeto que interviene es la persona o entidad encargada de administrar los bancos de información. Son conocidos como “Fuente de Información” u “Operador de la Información”. La información ingresa a los bancos de datos por medio de las relaciones de servicios, comerciales u otras, siempre y cuando se tenga una autorización a través de la Ley o del titular.
La segunda protección Constitucional es el derecho fundamental del Habeas Data, según la Corte Constitucional:

El Habeas Data es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales… (Sentencia T – 729 del año 2002).

Éste es un derecho autónomo. Así lo expresó la Corte Constitucional:

…es un derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo (Sentencia T-307 de 1999).

Posee características propias, las cuales ofrecen las defensas necesarias para salvaguardar la información pública o privada que los sujetos puedan brindar.

Al ser un derecho fundamental, fue creado bajo la Constitución Política de 1991 y considerado como inalienable e inherente a la persona humana.

Los derechos fundamentales, se encuentran ligados a los individuos, en tanto éstos emanan de la dignidad de los seres humanos.

La Corte Constitucional expresó lo siguiente en cuanto a su definición:

Otro de los pilares del Estado social de derecho se encuentra en el concepto de derecho fundamental. Dos notas esenciales de este concepto lo demuestran. En primer lugar su dimensión objetiva, esto es, su trascendencia del ámbito propio de los derechos individuales hacia todo el aparato organizativo del Estado. Más aún, el aparato no tiene sentido si no se entiende como mecanismo encaminado a la realización de los derechos. En segundo lugar, y en correspondencia con lo primero, la existencia de la acción de tutela, la cual fue establecida como mecanismo de protección inmediata de los derechos frente a todas las autoridades públicas y con posibilidad de intervención de la Corte Constitucional para una eventual revisión de las decisiones judiciales, que sirva para unificar criterios de interpretación (Sentencia No. T-406 de 1992).

Igualmente se considera que la calidad de fundamental que poseen algunos derechos incluidos en la Carta Magna, debe reunir tres criterios de identificación. El primer criterio es la “Conexión directa con los principios constitucionales”, el segundo es la “eficacia directa” y el tercer criterio es el “contenido esencial” (Superintendencia de Industria y Comercio, 2018). Sin el cumplimiento de estos criterios, los derechos no tendrían la calidad de fundamental.

El contenido fundamental debe desprenderse de lo establecido en la Constitución, así pues, deben emanar de los principios y valores que garantizan los pilares democráticos de nuestro Estado. Es por lo anterior que su aplicación resulta ser más directa e inmediata.

Como mecanismo de protección de este tipo de derechos, se encuentra la Acción de Tutela. A ésta, acuden las personas a quienes se les vulnere o amenace un derecho fundamental.
La Corte Constitucional expresó sobre esta protección lo siguiente:

La acción de tutela ha sido concebida únicamente para dar solución eficiente a situaciones de hecho creadas por actos u omisiones que implican la transgresión o la amenaza de un derecho fundamental, respecto de las cuales el sistema jurídico no tiene previsto otro mecanismo susceptible de ser invocado ante los jueces a objeto de lograr la protección del derecho. La tutela no puede converger con vías judiciales diversas por cuanto no es un mecanismo que sea factible de elegir según la discrecionalidad del interesado, para esquivar el que de modo específico ha regulado la ley; no se da la concurrencia entre éste y la acción de tutela porque siempre prevalece -con la excepción dicha- la acción ordinaria. La acción de tutela no es, por tanto, un medio alternativo, ni menos adicional o complementario para alcanzar el fin propuesto. Tampoco puede afirmarse que sea el último recurso al alcance del actor, ya que su naturaleza, según la Constitución, es la de único medio de protección, precisamente incorporado a la Carta con el fin de llenar los vacíos que pudiera ofrecer el sistema jurídico para otorgar a las personas una plena protección de sus derechos esenciales (Sentencia C-543 de 1992).

El Habeas Data entonces, permite que los titulares, le exijan a las personas o entidades encargadas que la información encontrada en las bases de datos sea corregida, administrada, adicionada y actualizada solamente bajo el consentimiento de éste. Igualmente cualquier divulgación o publicación sin el consentimiento debido estaría atacando los derechos consagrados en la Carta Política.

En muchas ocasiones los datos entregados pueden ingresar a una cadena de distribución donde su destino sea llegar a un usuario final. La distribución que se realiza deberá seguir con todos los parámetros establecidos por la ley.

Al igual que el titular se encuentra protegido por el derecho fundamental del Habeas Data, existe la Ley Estatutaria de Protección de Datos Personales 1581

de 2012, la cual se encuentra reglamentada parcialmente por el Decreto Nacional 1377 de 2013, debido a que, reglamenta en éste:

…aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales (…) (Presidencia de la República, 2013, p. 1).

Existen unos datos personales que no requieren la protección de la Ley anteriormente descrita. Esto por el tipo de información contenida.

Serán entonces los datos personales que se encuentran conservados en un ámbito exclusivamente doméstico o personal. Igualmente cuando la finalidad sea la Defensa Nacional, el control de delitos como el lavado de activos y el financiamiento del terrorismo. De igual forma los relacionados con información de inteligencia y contrainteligencia, información financiera y crediticia.

Siempre se requerirá tener una autorización previa del titular para que no se viole ningún derecho y se garantice la protección debida. Sin embargo, esta autorización no será necesaria cuando la información sea solicitada por una entidad administrativa o pública, por una orden judicial o cuando esté acreditado o requerido por la Ley.

Frente al tema de los datos personales de niños, niñas y adolescentes, se tiene una protección especial, al tratarse de menores de edad, la Ley Estatutaria 1581 de 2012 que manifiesta lo siguiente:

Artículo 7°. Derechos de los niños, niñas y adolescentes. En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública… (Congreso de la República, 2012, Art. 7).

Todo tratamiento de la información de un menor está prohibido, salvo cuando se les sea respetado el interés superior y sus derechos fundamentales. Así mismo, se requerirá autorización del representante legal.

Regulación por el Gobierno Nacional

La protección de Datos Personales se encuentra regulada por el Gobierno Nacional mediante la Ley 1581 del año 2012 o igualmente denominada Régimen General de Protección de Datos Personales, cuyo propósito es ordenar y proteger las bases de datos que son susceptibles de tratamiento por parte de las entidades públicas y privadas del país.

Se designó a la Superintendencia de Industria y Comercio para el manejo, protección y recopilación de los Datos Personales bajo la premisa de que se respeten y cumplan los derechos, garantías y principios que se estipulan en el Régimen General de Protección de Datos Personales.

Estas funciones se realizan a través de lo que se denomina “Directorio Público” (Superintendencia de Industria y Comercio, 2018), cuya finalidad es tener la información del número de bases de datos existentes en el país. Este directorio se encuentra en el Registro Nacional de Bases de Datos.

Se debe aclarar que la utilidad y función del “Directorio Público” solamente es cuantitativo, es decir, dentro de éste no se encuentran los datos de las personas que recaen en las bases de datos que tienen las entidades públicas y privadas del país. Solamente será relevante la cantidad de bases de datos que se tienen. El Decreto 886 de 2014, en el artículo quinto, informa cuál es la información que se debe incluir en el Registro Nacional de Bases de Datos.

Artículo 5°. 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:

- Datos de identificación, ubicación y contacto del Responsable del Tratamiento de la base de datos.

- Datos de identificación, ubicación y contacto del o de los Encargados del Tratamiento de la base de datos.

- Canales para que los titulares ejerzan sus derechos.

- Nombre y finalidad de la base de datos.

- Forma de Tratamiento de la base de datos (manual y/o automatizada), y

- Política de Tratamiento de la información… (Presidencia de la República, 2014, Art. 5, p. 2).

Los datos personales deben recaer única y exclusivamente en el tercero que recolecta la información bajo la autorización debidamente obtenida de la persona que aporta el dato personal.

La implementación del Registro Nacional de Bases de Datos en el país es muy importante porque genera conciencia en la sociedad y una responsabilidad por parte del Estado, armónico a su modelo constitucional.

Procedimiento

Toda la normatividad que regula el Derecho de Habeas Data se encarga de establecer de forma general la protección de este derecho, pero no establece una diferencia entre personas de carácter público y privado, por lo que las entidades públicas a pesar de que en el ejercicio de recolección de datos obtengan datos públicos que son considerados por el Decreto 1377 de 2013 como “Los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público” (Presidencia de la República, 2013, p. 2), que a su vez son datos sobre los cuales no se obliga a tener autorización de tratamiento precisamente por su naturaleza; las entidades públicas también obtienen datos personales que requieren autorización de tratamiento y por supuesto protección por parte de ellas, siempre y cuando se encuentren actuando como responsables o encargados de las bases de datos y del tratamiento de estos.

Es claro, que las entidades públicas también deben cumplir con lo establecido en todas las normas que buscan la protección de los datos personales, motivo por el cual se debe establecer un procedimiento para cumplir con las disposiciones. Para dar cumplimiento prescrito existe plena libertad, pero si se quiere realizar de una forma eficaz y eficiente se deben seguir los siguientes pasos:

- **Consecución e identificación de datos personales dentro de la entidad.**

Es posible que dentro de la entidad nunca hubiera existido la preocupación de percatarse por los datos personales que en ella reposan o que ella maneja, debido

que la inquietud de proteger y blindar el Derecho de Habeas Data en el país por parte de los entes encargados sólo se despertó hace unos pocos años, lo que hace necesario cumplir con lo siguiente:

✓ Realizar una inspección de todos los datos personales que se encuentran a disposición de la entidad, para así poder identificar qué clase de bases de datos se emplean con cierta cotidianidad y por último determinar la necesidad de usarlas, ya que de no ser necesarias las bases de datos no habría razón que justifique su utilización, por lo tanto deben ser suprimidas.

✓ Determinar el propósito con el cual se están recolectando los datos personales, esto es porque el titular de la información debe conocer el tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo (Congreso de la República, 2012, Art. 12). Un ejemplo de finalidad puede ser el de brindar seguridad y control de acceso a edificios.

- **Elaboración del Manual de Procedimiento de Tratamiento de Datos Personales.**

La regulación al Derecho de Habeas Data incluye también la protección de los datos personales, la cual debe ser desarrollada de acuerdo a la normatividad que la rige; aun así cada entidad –Responsable y Encargado- se encuentra en plena libertad de establecer las políticas y procedimientos que garanticen la protección de los datos personales que se encuentran a su cargo; frente a este punto se recomienda:

✓ Determinar la información básica pero completa acerca de la protección y desarrollo del Derecho de Habeas Data, la cual estará contenida en la Política de Tratamiento de Datos Personales.

La información seleccionada debe permitirle los entes de control, los terceros y en especial los titulares de la información que se encuentra comprendida en las bases de datos de la entidad, someramente bajo que reglas y condiciones estarán custodiados los datos personales de las personas que brindaron la autorización para su tratamiento.

✓ Clarificar los recursos utilizados para lograr la obtención de los datos personales por parte de la entidad, es decir, se debe exponer cuáles son los medios utilizados por el responsable o encargado del tratamiento de los datos personales, para obtener dicha información. Entre los medios hay una muy común que es la de peticiones, quejas, reclamos y sugerencias (PQRS).

✓ Establecer e implantar los mecanismos y procedimientos por medio de los cuales lo titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización. (Presidencia de la República, 2013, art 13). Un ejemplo de ellos son los canales de comunicación de la entidad encargada o responsable del tratamiento de datos, que pueden ser: correo electrónico, buzón de sugerencias, línea telefónica entre otros.

- **Obtención de autorización por parte de los titulares de los datos personales.**

El responsable de los datos personales, en este caso la entidad pública se encuentra en la obligación obtener una autorización por parte del titular de la información para poder hacer uso de ella; la autorización es el consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales (Congreso de la República, 2012, art. 3).

Vemos que el consentimiento debe cumplir principalmente con tres requisitos para que sea considerado válido, cada requisito tiene una connotación diferente; el hecho de que el consentimiento deba ser previo implica que el titular de la información debe brindar con antelación el permiso para el tratamiento de sus datos.

Cuando la norma indica que la autorización debe ser expresa lo que busca es que la manifestación de voluntad se dé de forma clara y que no se preste para entender cosa distinta; y cuando se hace referencia a que el consentimiento debe ser informado apunta a un deber por parte de la entidad responsable de los datos personales, la cual debe informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada (Presidencia de la República 2013, art. 17).

Para dar cumplimiento a lo establecido, deben seguirse lo siguientes pasos:

✓ Identificar si la información que se va a recolectar o que se ha recolectado requiere una autorización por parte del titular, toda vez que la norma trae ciertas excepciones frente a las cuales el responsable de los datos no requiere autorización por parte del titular para hacer uso de su información. El artículo 10° de la Ley 1581 de 2012, establece:

Artículo 10. Casos en que no es necesaria la autorización.

La autorización del Titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

b) Datos de naturaleza pública;

c) Casos de urgencia médica o sanitaria;

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

e) Datos relacionados con el Registro Civil de las Personas... (Congreso de la República, 2012, art. 10).

✓ Establecer modelos de autorización teniendo en cuenta cada base de datos usada en la entidad. Esto es porque cada banco de datos, como se expresó con anterioridad tiene una finalidad diferente, la cual debe ser dada a conocer al emisor de lo información, ya que este es un derecho consagrado por el Artículo 8° Literal c) de la Ley 1581 de 2012, el cual dispone:

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

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales (…). (Congreso de la República, 2012, (Artículo 8° Literal c).

✓ La entidad debe decidir de qué forma va a conservar prueba, bien sea digital y o escrita de la aprobación dada por el titular de la información.

- **Identificar los riesgos que pueden correr los datos personales usados por la entidad.**

El hecho de tener almacenados datos personales puede generar riesgos, los cuales deben ser evitados con mecanismos y formas que garanticen la seguridad de los mismos. La Ley 1581 del 2012 en su artículo cuarto, en el literal g, establece el principio de seguridad como principio rector de la disposición, el cual implica qué:

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento (Congreso de la República, 2012, Art. 4).

Además de ser consagrado como un principio, la seguridad de los datos personales es un deber del responsable, el cual se encuentra consagrado en el **artículo 17 literal d de la Ley 1581 de 2012,** que establece:

Artículo 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:
(…)

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento (…) (Congreso de la República, 2012, Art. 17, literal d.).

Para acatar lo dispuesto es necesario:

✓ Identificar si a través de las actividades que realice la entidad en el ejercicio común de funcionamiento, se pueden generar riesgos que pongan en peligro los datos de las personales sobre los que la entidad es el responsable o encargado. Además, es necesario analizar la posibilidad de la materialización de los riesgos, incluyendo el impacto que puedan generar.

✓ Crear formas que ayuden a evitar o eliminar los riesgos que pueden correr la información de las personas que otorgaron la autorización de tratamiento a la entidad. Algunas de esas formas o mecanismos pueden ser la adquisición de software que ofrezca formas de protección de los datos personales; otra forma es elegir a una persona que haga parte de la entidad y que se encargue exclusivamente de revisar y verificar constantemente que los bancos de datos se encuentren protegidos en debida forma.

- **Incluir cláusulas de confidencialidad, aviso de privacidad y habeas data en los contratos celebrados por la entidad.**

La protección de datos personales debe ser integral, es decir que debe ser implementada en todos los campos de acción de la entidad, uno de ellos es el de la contratación de la cual puede resultar mucha información que debe ser tratada bajo la normatividad del derecho de habeas data.

Los datos pueden surgir tanto en la celebración de un contrato, como en su ejecución; para blindar de forma eficiente la información derivada de la contratación es necesario pactar las cláusulas de confidencialidad, de aviso de privacidad y de habeas data.

La cláusula de confidencialidad consiste en un acuerdo que busca mantener una información en secreto, con la finalidad de que esa información no pueda llegar a ser utilizada en beneficio de las partes. Las partes involucradas con esta cláusula se comprometen a no revelar los datos que puedan resultar del contrato.

Según el artículo 3° Numeral 1° del Decreto 1377 define el aviso de privacidad como la comunicación dada por el responsable, dirigida al titular de los datos personales, en la cual se da a conocer las políticas de tratamiento de información, incluyendo la finalidad del tratamiento que se pretende dar a los datos personales.

Por último, la cláusula de habeas data es aquella mediante la cual el responsable del tratamiento de los datos personales recibe la autorización por parte del titular de la información, para que sus datos sean manejados por la entidad.

- **Registro de las bases de datos en el RNBD**

El Registro Nacional de Bases de Datos –RNBD- es según la Superintendencia de Industria y Comercio, el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos.

El registro de las bases de datos de una entidad debe realizarse en unos tiempos determinados mediante decretos; esta es una obligación que debe ser cumplida tanto por el responsable como por el encargado de los datos personales.

Con este punto se da por terminado el procedimiento que debe seguir una entidad obligada a dar cumplimiento a la normatividad que se encarga de la protección de datos personales. El procedimiento es una propuesta que se realiza teniendo en cuenta la experiencia en entidades estatales como lo son Plaza Mayor Medellín S.A. y la Sociedad Televisión de Antioquia Limitada –TELEANTIOQUIA-.

El anterior procedimiento abarca de forma simple pero completa todos los requerimientos que se requieren para cumplir con lo dispuesto, pero puede llegar a ser modificado teniendo en cuenta la necesidad y funcionamiento de cada entidad.

Conclusiones

Los datos personales están consagrados en la Constitución Política como un derecho fundamental, los cuales goza de una doble protección. Igualmente se encuentran regulado por el Gobierno Nacional por medio de decretos y leyes.

Los titulares deben autorizar el tratamiento de la información proporcionada a las entidades independiente de su naturaleza. So pena, de que esos Bancos de Datos o terceros incurran en una violación de lo establecido y protegido por la Constitución Política.

El cumplimiento de las normas que regulan el derecho de habeas data implica realizar varios procesos y procedimientos, para que se logre una efectiva protección por parte de las entidades y personas obligadas a hacerlo; para esto es

necesario analizar el funcionamiento y la necesidad por parte del responsable de los datos personales.

El derecho de habeas data actualmente se encuentra muy protegido por parte de las autoridades encargadas, por ende, quién ponga en riesgo o quien atente contra su seguridad podrá tener consecuencias bastantes considerables, lo que generaría un impacto negativo frente a quién no cumplió con las disposiciones.

Recomendaciones

El Capítulo II Procedimiento y Sanciones, de la Ley 1158 de 2012, establece las consecuencias que pueden llegar a acarrear el hecho de no cumplir con las disposiciones de la ley por parte del responsable y el encargado del tratamiento de los datos personales. En este capítulo se puede evidenciar que las sanciones pueden ser tanto pecuniarias como administrativas, ya que el incumplimiento de la norma puede ocasionar una condena de hasta dos mil (2.000) salarios mínimos mensuales legales vigentes, hasta el cierre temporal de las operaciones relacionadas con el tratamiento de los datos personales.

Es claro que si no se cumple con la disposición las consecuencias serán bastante perjudiciales, en este caso para las entidades estatales, por lo que se recomienda hacer uso del procedimiento aquí planteado con el cual pueden abarcar en su totalidad con lo prescrito en la normatividad correspondiente.

Cabe anotar que el cumplimiento no sólo conlleva a realizar los pasos propuestos, además de estos hay que tener en cuenta los plazos establecidos para inscribir las bases de datos en el RNBD. Los plazos pueden ser consultados en el Decreto 90 de 18 de enero de 2018, expedido por el Ministerio de Comercio Industria y Turismo.

Referencias Bibliográficas

Colombia. Congreso de la República. (2008). *Ley estatutaria 1266 del 2008*. Bogotá: El Congreso.

Colombia. Congreso de la República. (2012). *Ley estatutaria 1581 del 2012*. Bogotá: El Congreso.

Colombia. Congreso de la República. (2014). *Ley 1712 del 2014*. Bogotá: El Congreso.

Colombia. Corte Constitucional. (1992). *Sentencia C 543 de 1992*. M. P. José Gregorio Hernández Galindo.

Colombia. Corte Constitucional. (1992). *Sentencia T 406 de 1992*. M. P. Ciro Angarita Barón.

Colombia. Corte Constitucional. (1999)- *Sentencia T 307 de 1999*. M. P. Eduardo Cifuentes Muñoz.

Colombia. Corte Constitucional. (2002). *Sentencia T 729 de 2002*. M. P. Eduardo Montealegre Lynett.

Colombia. Corte Constitucional. (2008). *Sentencia C 1011 del 2008.* M. P. Jaime Córdoba Triviño.

Colombia. Corte Constitucional. (2011). *Sentencia C 748 del 2011*. M. P. Jorge Ignacio Pretelt.

Colombia. Corte Constitucional. (2014). *Sentencia T 020 de 2014*. M. P. Luis Guillermo Guerrero Pérez.

Colombia. Corte Constitucional. (2014). *Sentencia T 176 de 2014.* M.P. Jorge Ignacio Pretelt Chaljub.

Colombia. Corte Constitucional. (2015). *Sentencia T 167 de 2015*. M. P. Jorge Ignacio Pretelt Chaljub.

Colombia. Presidencia de la República. (2009). *Decreto 1727 del 2009.* Bogotá: La Presidencia.

Colombia. Presidencia de la República. (2013). *Decreto 1377 del 2013*. Bogotá: La Presidencia.

Colombia. Presidencia de la República. (2014). *Decreto 886 del 2014*. Bogotá: La Presidencia.

Colombia. Secretaría General de la Superintendencia de Industria y Comercio. (2013). *Resolución 20752*. Bogotá: Superintendencia de Industria y Comercio.

Colombia. Superintendencia de Industria y Comercio. (2012). *Resolución 76434*. Bogotá: Superintendencia de Industria y Comercio.

Colombia. Superintendencia de Industria y Comercio. (2018.). *Protección de datos personales*. Obtenido de http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Constitución Política de Colombia. (2010). *Artículo 15.* Bogotá: Legis.