PROTECDATA
COLOMBIA

PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR SALUD

Previo a realizar análisis respecto del deber legal que corresponde a las empresas del sector salud de aplicar el marco legal en Protección de Datos Personales, es necesario señalar el sustento legal vigente en la materia.

En Colombia, el sustento legal para el tratamiento de datos personales se encuentra en el Artículo 15 Constitución Política de 1991, en el que se reconoció por primera vez el derecho de *habeas data*. Precepto constitucional que fue desarrollado en principio en la Ley Estatutaria 1266 de 2008 y sus decretos reglamentarios (Decreto 1727 de 2009 y Decreto 2952 de 2010), orientada únicamente a la protección de los datos comerciales y financieros, se trata de una norma de carácter sectorial que no enmarca de manera integral y general la protección de datos.

Posteriormente, ante la necesidad de fijar reglas de protección, medios de control y una regulación concreta para el manejo y tratamiento de las bases o bancos de datos, así como los mecanismos para que los derechos planteados en la Constitución Política gocen de plenas garantías, se expide la Ley 1581 de 2012, mediante la cual se regula el derecho fundamental de *habeas data* con la finalidad de proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones como recolección, almacenamiento, uso y tratamiento por parte de entidades de naturaleza pública y/o privada. Esta Ley fue parcialmente reglamentada parcialmente mediante Decreto 1377 de 2013 y Decreto 886 de 2014.

Es importante señalar que del citado marco normativo se deriva el deber legal de las entidades tanto públicas, como privadas de fijar unas políticas claras que den cumplimiento a las directrices planteadas en la norma respecto al uso de los datos personales contenidos en sus sistemas de información para garantizar su tratamiento. Además, deben definir los fines y medios esenciales para el manejo de los datos de los usuarios o titulares, por cuanto los deberes que se le atribuyen corresponden a los principios de la administración de datos, al derecho a la intimidad y *habeas data* del titular del dato personal.

Pues bien, a la luz de la ley 1581 de 2012, en el caso concreto de las empresas del sector salud es imperativo remitirse al artículo 5 de la Ley 1581 de 2012, dado el carácter de los datos que almacenan en sus bases de datos relativos a la salud, considerados en la ley en una categoría especial, como sensibles. Dicho artículo señala que los datos sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, esto es, aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos **a la salud**, a la vida sexual y los datos biométricos.

De acuerdo con la definición que trae el artículo 5 de la ley 1581 de 2012, *"se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación*", es claro que dentro de estos se incluyen los relativos a la salud, por lo tanto, hacen parte de éstos: las historias clínicas, los exámenes de laboratorio y todos los datos relacionados con

la salud de un individuo, lo que implica de acuerdo con la norma una obligatoria protección por parte de las entidades responsables y los sujetos que tengan relación con dichos datos.

De la lectura del artículo 5 en comento, se deriva la obligatoriedad que trae el ordenamiento jurídico de obtener consentimiento previo, expreso e informado del titular para realizar tratamiento de éstos datos aplicando las restricciones y facultades que indica la ley para el efecto, tal como lo establece el artículo 6 de la Ley 1581 de 2012 desarrollado por el artículo 6 del Decreto 1377 de 2013, el cual prevé:

> ***"Artículo 6°. Tratamiento de datos sensibles.*** *Se prohíbe el Tratamiento de datos sensibles, excepto cuando:*
>
> *a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;*
>
> *b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;*
>
> *c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;*
>
> *d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;*
>
> *e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares."*

En el caso especifico de la historia clínica se trata de información relacionada con la salud que corresponde a la intimidad de la persona, por lo que, en la recolección, almacenamiento y tratamiento se debe garantizar además del carácter reservado, los derechos del titular de los datos que contengan éstos expedientes. Es entonces, un deber legal del Responsable del tratamiento aplicar políticas y prácticas que garanticen los principios fundamentales de la protección de datos personales en la historia clínica o expediente médico.

De modo que, el deber de cuidado en el tratamiento de los datos sensibles al interior de una empresa del sector salud corresponde a la gerencia y los profesionales que tengan acceso a éstas bases de datos en el desarrollo del servicio que prestan, siendo de obligatorio cumplimiento la implementación del marco legal en protección de datos personales para el amparo efectivo de la información relativa a salud que está siendo almacenada. Así las cosas, el responsable deberá designar un Oficial de Protección de Datos que cumpla con las funciones establecidas en la norma que entre otras cosas incluye la coordinación de la adecuada aplicación de la ley dentro de su organización.

Asimismo, por tratarse de derechos fundamentales que deben ser garantizados por el Responsable, es necesario y de obligatorio cumplimiento la solicitud de autorización de que trata el artículo 9° de la Ley 1581 de 2012, siendo entonces un deber de los Responsables del Tratamiento de datos personales el establecer unos mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 de del Decreto 1377 de 2013. Para ello, el artículo 7 del Decreto 1377 de 2013, faculta a los responsables para que a través de medios técnicos que faciliten al Titular su manifestación automatizada se obtenga dicha autorización, que podrá efectuarse: (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

Dichas autorizaciones deben contar con el lleno de los requisitos establecidos en la ley, que, para el efecto, el artículo 5 del Decreto Reglamentario 1377 de 2013, señala la obligación de quien recoge los datos personales de informar al titular las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento. Adicionalmente, como se había mencionado el artículo 7 de la misma norma señala que la autorización debe obtenerse mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

Pues bien, una vez analizado el deber legal de implementar el marco legal en protección de datos en las empresas cuya actividad económica corresponde al sector salud, es importante precisar que, si bien es cierto, mediante Resolución Ministerial 1995 de 1999 se establecen directrices para el manejo de la historia clínica, esto es, respecto a su diligenciamiento, administración, conservación, custodia y confidencialidad conforme a los parámetros del Ministerio de Salud y del Archivo General de la Nación en lo concerniente a los aspectos archivísticos contemplados en la Ley 80 de 1989, ello correspondió a la necesidad de establecer un mecanismo legal que amparara la reserva de un documento privado, obligatorio, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en la atención de una persona. Lo anterior, en razón a falta de regulación en la materia que para el año 1999 no existía.

Como se había mencionado la reglamentación en materia de habeas data en Colombia inicio con la expedición de la Ley 1266 de 2008, posteriormente se reguló integralmente mediante Ley 1581 de 2012 y sus decretos reglamentarios. Es claro entonces que para el año 1999 no existía un marco legal en la materia, fueron años de pronunciamientos jurisprudenciales que derivaron finalmente en la reglamentación de la protección de datos en Colombia.

Así las cosas, de acuerdo con el artículo 2 de la Ley 1581 de 2012, las empresas del sector salud están obligadas a dar aplicación al marco legal en protección de datos por no encontrarse dentro de las excepciones que contempla el ordenamiento jurídico vigente, veamos:

> *Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.*
>
> *La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en*

territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;

f) A las bases de datos y archivos regulados por la Ley 79 de 1993. (Resaltos fuera de texto)

Para concluir, nótese que la ley no exime de su ámbito de aplicación las bases de datos del sector salud, las excepciones contempladas en el citado artículo 2 son taxativas no admiten interpretación alguna donde pueda inferirse que las mismas están exentas de cumplir con la obligación de implementar el marco legal en protección de datos.