Santa Marta
Johanna Orduz

El consentimiento informado: una barrera para el respeto irrestricto al derecho a la protección de datos personales

https://doi.org/10.25058/20112742.n51.11

Luis Bernardo Díaz Gamboa[1]
https://orcid.org/0000-0002-0117-4753
luis.diaz@uptc.edu.co

Cindy Paola Rivera Ramírez[2]
https://orcid.org/0009-0008-6596-611X
abogadacindyrivera@hotmail.com

Universidad Pedagógica y Tecnológica de Colombia

Cómo citar este artículo: Díaz Gamboa, L. B. & Rivera Ramírez, C. (2024). El consentimiento informado: una barrera para el respeto irrestricto al derecho a la protección de datos personales. *Tabula Rasa, 51*, 261-288. https://doi.org/10.25058/20112742.n51.11

Recibido: 18 de enero de 2024 *Aceptado: 28 de mayo de 2024*

Resumen:

El presente artículo presenta una serie de reflexiones respecto la política que regula el tratamiento de datos personales, en especial los datos sensibles relacionados con la *vida íntima, personal, sexual, laboral o familiar de las personas y que están manejados por entidades que prestan servicios de salud.* Colombia es uno de los países de América Latina que se ha sumado a la estrategia de incorporar al ordenamiento jurídico una regulación general de protección de datos personales, sin embargo, el instrumento jurídico resulta ineficaz a la hora de garantizar una política de tratamiento íntegra de la información sensible por cuenta de los operadores en el área de la salud, sin brindar garantías reales en el proceso de recopilación, almacenamiento, uso, actualización y transferencia, convirtiendo el consentimiento informado en una entrega de la intimidad del usuario del servicio de salud como requisito para acceder a un procedimiento médico.

Palabras clave: intimidad; datos personales; consentimiento; información; tratamiento.

[1] Decano de la Facultad de Derecho y Ciencias Políticas de la Universidad Pedagógica y Tecnológica de Colombia.
[2] Abogada, especialista en Derecho Procesal, Derecho Administrativo y Derecho Penal.

Informed Consent: A Barrier to Unrestricted Respect for the Right to Personal Data Protection

Abstract:

This article presents a series of reflections on the policy that regulates the treatment of personal data, especially sensitive data related to intimate, personal, sexual, labor or family life of individuals, which is handled by health service providers. Colombia is one of the Latin American countries that has joined the strategy of bringing a general regulation of personal data protection to the legal system. However, this legal instrument is ineffective when it comes to guaranteeing a policy of full treatment of sensitive information on behalf of health operators, since it fails to provide real guarantees in the process of collection, storage, use, updating and transfer, turning informed consent into a surrender of the health service user's privacy as a requirement for access to medical procedures.

Keywords: privacy; personal data; consent; treatment of information.

O consentimento informado: uma barreira para o respeito irrestrito ao direito à proteção de dados pessoais

Resumo:

O presente artigo apresenta uma série de reflexões sobre a política que regula o tratamento de dados pessoais, em especial os dados sensíveis relacionados com a vida íntima, pessoal, sexual, do trabalho ou familiar das pessoas e que estão administrados por entidades que prestam serviços de saúde. A Colômbia é um dos países da América Latina que aderiram à estratégia de incorporar uma regulação geral de proteção de dados pessoais ao ordenamento jurídico, no entanto, o instrumento jurídico resulta ineficaz na hora de garantir uma política íntegra de tratamento da informação sensível por conta dos operadores na área da saúde, sem oferecer garantias reais no processo de coleta, armazenamento, uso, atualização e transferência, fazendo que o consentimento informado se torne uma entrega da intimidade do usuário ao serviço de saúde como requisito para aceder a um procedimento médico

Palavras-chave: intimidade; dados pessoais; consentimento; informação; tratamento.

Introducción

La información de carácter personal a pesar de que se encuentre registrada en bases de datos, solo le concierne a su titular, por lo que es necesario que exista una regulación normativa que controle y vigile el uso de los mismos, para que de esta manera no se genere una flagrante violación a los derechos humanos.

En Colombia se expide la ley estatutaria 1581 de 2012, con el fin de establecer disposiciones generales sobre el ejercicio del derecho a la protección de datos personales, normativa que enuncia los principios rectores que deben aplicarse

en el tratamiento a todo tipo de datos personales, sin embargo, se echa de menos el diseño de una política especial cimentada en garantías de seguridad y confidencialidad para el tratamiento de datos sensibles por parte de las entidades que prestan servicios en el sector salud.

En este contexto ¿En el ejercicio del derecho humano y fundamental de protección de datos personales, la política de tratamiento de datos sensibles en el sector salud, constituye en términos generales, un sistema efectivo y ofrece garantías de seguridad, confidencialidad e integridad a los titulares del dato?

Para dar respuesta al interrogante planteado se acudió al método cualitativo a partir del estudio y análisis normativo, en contraste con artículos y documentos académicos relacionados con la protección de datos personales.

En desarrollo del presente artículo se efectúan, una serie de reflexiones respecto la intimidad, la dignidad y el honor, condiciones inherentes de todo niño o niña, hombre o mujer que deben ser amparadas y garantizadas por un Estado social de derecho, principalmente y por encima del acelerado ejercicio de las libertades, los intereses económicos o políticos, los avances científicos y el derecho mismo a la información.

Protección de datos personales

La dignidad del ser humano, tiene su cimiento, en el fuero interno de cada ser y en la protección de su esencia, de ahí que la intimidad de las personas este reconocida como derecho fundamental en la declaración universal de los derechos humanos y que este derecho haga parte del conglomerado de garantías fundamentales reconocidas por la Constitución Política colombiana; sin embargo, el carácter intangible de derechos fundamentales como la dignidad y la honra hace que en el desconocimiento, los titulares del derecho expongan la garantía plena del ejercicio del derecho a la intimidad, en consecuencia la disposición de datos debe ser pro tempore y limitarse a los datos estrictamente necesarios (Bautista Avellaneda, 2015).

La disposición de la intimidad de cada ser humano es un asunto que le compete de manera exclusiva a cada individuo, por ende, no puede convertirse bajo ningún pretexto en forma de pago para acceder a bienes y servicios, ya que la intimidad y la dignidad de las personas se encuentra fuera del mercado, razón por la cual comercializar con la intimidad de los seres humanos entraña conductas vulneradoras de derechos.

La categoría de protección de datos en principio no surge como derecho y aun se niega tal naturaleza, pero es necesario resaltar su consolidación actual como derecho fundamental tras protagonizar una historia de éxito al amparo de bases jurídicas en el ámbito supranacional (Rallo Lombarte, 2019).

El constituyente reconoce en nuestro ordenamiento jurídico el derecho a «conocer, actualizar y rectificar las información que se haya reconocido sobre ella en bancos de dato y en archivos de entidades públicas y privadas» (Constitución Política de Colombia, 1991), posteriormente el legislador mediante la ley estatutaria 1266 de 2008 reglamenta el alance y los mecanismos de protección y se conoce como el derecho de *Habeas Data,* advirtiendo que es el mecanismo de protección de los datos financieros, crediticios, comerciales y de servicios que se registra en las bases de datos y archivos de las entidades de naturaleza pública y privada (ley 1266/08)

Luego, se expide la ley 1581 de 2012 con el fin de establecer disposiciones generales sobre el ejercicio del derecho a la protección de datos personales y enuncia los principios rectores que deben aplicarse en el tratamiento a todo tipo de datos personales, como la autoridad administrativa competente para investigar y sancionar a los terceros que incumplan las disposiciones tendientes a proteger los datos y es dicho documento el que se hiérenos a utilizar en el presente artículo.

El derecho autónomo fundamental de protección de datos personales, incluye toda aquella información individual, familiar e íntima que aparece en documentos como, el de identidad, el lugar de nacimiento, el estado civil, edad, lugar de residencia, recorrido académico, historia laboral, o datos de carácter más íntimo como el estado de salud, los rasgos físicos, ideología política, preferencias sexuales, entre otros aspectos que permitan identificar a una persona (Castillo Vázquez, 2007).

Cuando hablemos de dato personal hacemos referencia a las siguientes características:

> i) *Estar referido a aspectos exclusivos y propios de una persona natural, ii) Permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) Su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) Su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.* (Cruz Ramírez, s.f.)

Conocida la noción de datos de carácter personal, es procedente hacer alusión a la categoría de datos personales relativos a la salud y las consecuencias que implican la recolección y su tratamiento. Se ha sostenido la tesis que los datos de salud son merecedores de especial protección por el carácter de datos íntimos y sensibles ya que incide directamente sobre la dignidad y la personalidad de la esfera más íntima y reservada de una persona. (Troncoso Reigada, 2010).

A continuación, se estudiarán de manera específica los datos personales relativos a la salud, en los apartados que regula el Reglamento Europeo de Protección de Datos Personales (RGPD) tratando de ver, al mismo tiempo, como surge en la práctica su utilización como su regulación normativa y doctrinaria.

Así pues, el RGPD adopto una noción amplia de dato personal relativo a la salud, en el art. 4. 15) definiéndose así: «datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud»

Deslindadas las anteriores nociones, procedemos a señalar de manera sucinta las bases jurídicas legitimadoras en el tratamiento de los datos personales en el ámbito de la salud.

Nivel de protección de los datos sensibles: caso comparativo RGPD

Aunque en Colombia se promulgo la ley 1266 de 2008 y1581 de 2012, por medio de las cuales se regula y se establece generalidades del derecho de protección de datos personales, es conveniente realizar un estudio comparativo con los criterios y pautas de la política de tratamiento de datos referidos a la salud, específicamente según lo señalado en el Reglamento Europeo de Protección de Datos Personales (RGPD) particularmente en lo que corresponde con la exigencia del consentimiento explícito e informado del titular del dato, diferente a la dinámica que implica el derecho a la salud.

Con la promulgación de la norma europea, se han incorporado novedades significativas, que trazan un panorama sobre la protección de datos personales, ya que, adiciona nuevos elementos a la cultura de la protección de datos completamente necesarios en el ámbito normativo, especialmente en el modelo del consentimiento como fundamento en la legitimación del tratamiento de los datos (Polo Roca, 2020).

Consentimiento

Al respecto la RGPD determina el alcance que tiene el consentimiento de las personas en el tratamiento de los datos en salud, expresamente define el consentimiento como un derecho fundamental consistente en:

> *Artículo 4 numeral 11 Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*. (Unión Europea, 2016)

Por lo que resulta oportuno empezar diciendo que la principal categoría que nos permite hablar de garantías de protección de datos personales es sin duda el tratamiento de datos en salud basado en el consentimiento informado del interesado (Murillo de la Cueva, 2003).

Por regla general el consentimiento debe ser explícito e informado cuando hace referencia al tratamiento de datos genéticos, biométricos, de salud, o vida sexual de las personas, es decir que necesariamente ha de existir

la declaración o una acción afirmativa de dicha voluntad y la facultad de disponer y decidir libremente sobre las cuestiones propias de su ser, fundamentalmente implica un ejercicio del principio de la autonomía personal (Cantero Martínez, 2005).

El reconocimiento de la autonomía como principio, cobra vigencia justamente cuando las personas debidamente informadas otorgan su consentimiento para que su intimidad y demás aspectos de su condición humana sea objeto de ser tratados por una entidad responsable. Así las cosas, el consentimiento informado para el tratamiento de los datos en salud no puede entenderse como un mero formalismo, sino como el derecho de tener conocimiento de lo que se hace con la información de su vida privada e íntima.

El consentimiento en el derecho de protección de datos personales en el ámbito de la salud resulta ser una condición necesaria para la licitud del tratamiento de los mismos y su legitimidad, ya que no contar con dicha voluntad sería una flagrante violación de derechos y libertades fundamentales.

Teniendo en cuenta lo que se ha dicho anteriormente, el consentimiento informado se compone de dos elementos fundamentales: el consentimiento y el derecho a ser informado (Rodríguez López, 2004).

La autorización para tratar los datos personales en salud podrá darse siempre y cuando la persona haya sido previamente informada sobre el alcance de expresar su consentimiento así de cómo los derechos que puede ejercer con respecto el acceso, rectificación, uso y cancelación de la información.

Es decir que la manifestación del consentimiento de una persona será válido entre otras cosas si el titular del dato fue debidamente informado (Cantero Martínez, 2005).

Derecho a ser informado

El derecho a ser informado, implica la facultad de toda persona a conocer y entender las características y alcance que genera el tratamiento de los datos, al respecto la RGPD regula este aspecto y lo recoge fundamentalmente en su artículo 13, y se consigna expresamente a pesar de su extensión, debido a su importancia:

> a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
>
> b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

El derecho a la información es relevante en la protección de los datos personales, primer lugar, porque constituye el escenario en que se promueve la relación del titular de los datos de carácter personal y el responsable de coger y manipular dicha información. Entonces este derecho sería el punto de partida para el ejercicio de otros derechos ya que es la vía que desarrolla la facultad que tienen las personas de consentir libremente la decisión de disponer de sus datos (Arenas Ramiro, 2006).

En segundo lugar, el derecho a ser informado goza de una estrecha relación con el derecho a otorgar el consentimiento informado, debido a que, la falta de información o la información incorrecta, vicia el consentimiento de la persona, así como sucede en el otorgamiento del consentimiento en la suscripción de un contrato, si hay un error en dicha exteriorización será un contrato nulo (Seoane Rodríguez, 2002).

La importancia de esta relación se evidencia especialmente cuando se exige salvo determinadas excepciones, el consentimiento del titular del dato en salud para el tratamiento de los mismos.

En tercer lugar, la relevancia del derecho a la información se observa estrictamente en su contenido, surge como una garantía para que el titular establezca los parámetros del tratamiento de sus datos, a saber, el derecho de cancelación, rectificación y oposición fundamentalmente.

En efecto, para llevar a cabo estos derechos es necesario tener conocimiento previo de su existencia y, precisamente, la información garantiza que el titular de los datos conozca dichas facultades y cómo ejercerlas (Canales, Blanco & Piñar Mañas, 2005).

Ahora bien, en casos que el consentimiento sea otorgado por un tercero, bien sea porque el titular del dato sea incapaz para ejercer el derecho, o porque ha sido declarado como tal, o bien por circunstancias ajenas a su voluntad como casos de accidentes, o un trastorno pasajero, entre otras. Para estos supuestos de hechos la RGPD establece que dicha información ha de ser suministrada al titular del dato como garantía del tratamiento de los datos (ver el artículo 14 RGPD).

El derecho de protección de datos personales fundado en el consentimiento informado del titular del dato exige a la par el reconocimiento de garantías en el ejercicio de tratamiento de los datos, a saber, el derecho de acceso, de rectificación y suspensión de dicha información personal.

Por otro lado, el Reglamento dispone que el derecho a ser informado se distingue justo en el momento de la recogida de los datos de carácter personal, en dos supuestos, un primer caso, cuando los datos de carácter personal se recogen

directamente del propio titular y se da la información previa al interesado para obtener su consentimiento; segundo caso, cuando el tratamiento de los datos se realiza sin el consentimiento del titular, la información será suministrada al titular, para que ejerza los derechos de acceso, rectificación y cancelación.

En este sentido el derecho de información hace posible que el titular de los datos, pueda conocer la información que está tratando y ver si éstos corresponden con la realidad presente, para, en caso contrario, cambiarlos y adecuarlos a su beneficio (Lizárraga Bonelli, 2019).

Vicios en el consentimiento

En la actualidad el consentimiento informado reviste de mucha importancia cuando hablamos de mecanismos que garanticen la protección de los datos personales y por ello el responsable del tratamiento de los datos ha de demostrar que el consentimiento obtenido cumple con las exigencias legales requeridas para tal fin, además que sea libre, especifico e inequívoco.

Entonces, el consentimiento informado al tratarse del permiso que emite el titular del dato una vez que le hayan informado debidamente sobre los derechos, consecuencias y demás generalidades que implica el tratamiento de los datos en salud, evidentemente dicha información ha de darse en forma comprensible, utilizando un lenguaje claro al punto de evitar tecnicismos que resulte entendible a cualquier persona (Galán Cortés, 1997).

Por su parte, cuando el otorgamiento del consentimiento se da sin la debida comprensión del alcance de lo autorizando, es un claro ejemplo de error en la prestación del consentimiento que afecta la validez de la autorización obtenida y la legitimidad del tratamiento de los datos (Aparicio Salom, 2009).

Entre tanto el consentimiento tiene una estrecha relación con la finalidad que fueron obtenidos los datos en salud, por lo que previo a la exteriorización de la voluntad de la persona, ha de darse a conocer de manera determinada y exacta la finalidad del recaudo, lo dicho cobra relevancia, en la medida que debe mediar la certeza en el por qué y para serán utilizados sus datos, por lo tanto de darse el caso que estos sean utilizados con otros fines a los destinados, salvo las excepciones previstas en el RGPD el consentimiento expresado no es legítimo.

De igual manera sucede cuando la información que se brindada, no se da a conocer la finalidad de los datos y se obtiene el consentimiento por parte del titular o un tercero, a pesar que se haya dado una finalidad legitima según la disposición legal, dicho consentimiento es Nulo (ver artículo 14 RGPD).

Así las cosas, es clara la intención del RGPD de garantizar al titular de los datos, el derecho a tener un conocimiento claro, completo y certero de todos los aspectos que rodean el tratamiento de los mismos.

Excepciones al consentimiento

El derecho a la protección de datos, se define como la facultad de controlar cada uno de los aspectos que componen la personalidad del individuo, el de los datos de carácter personal; al respecto el ejercicio de este derecho fundamental se visibiliza con mayor intensidad que en el caso de otros derechos (Murillo de la Cueva & Piñar Mañas, 1990).

Hasta aquí hemos dicho que en principio está «prohibido el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad de las personas» salvo que el interesado haya expresado su consentimiento y fines determinados en el tratamiento de los datos, sin embargo la normatividad Europea plantea determinados supuestos de hecho en los cuales es legítimo y licito tratar los datos sin el consentimiento del titular, lo cual merece sin duda estudiar el análisis que establece dicha disposición de exceptuar dicha facultad para la manipulación de los datos (ver artículo 9 RGPD).

Los supuestos categóricos que habilitan el tratamiento de datos personales obviando el consentimiento del titular, están previstos en el RGPD así:

> *c) proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.*
>
> *h) medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social*
>
> *i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitario*
>
> *j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.* (ver artículo 9 RGPD)

La normatividad en mención ha establecido una batería de límites al derecho a consentir bajo la premisa que el derecho de protección de datos personales no es absoluto y que la capacidad de controlar los datos es una facultad legítima en los ordenamientos jurídicos.

Por lo tanto, vamos a recoger las excepciones enunciadas y desde ahora intentar realizar un análisis en el contenido concreto y los límites que se han fijado a la facultad de consentir los datos.

El primer supuesto, hace alusión a la finalidad de proteger el derecho a la integridad o la vida del interesado o un tercero, cuando los profesionales de la salud se encuentran en situaciones en las cuales se discute bienes jurídicos de valor más elevado, gozan de la facultad de manera excepcional de recoger los datos personales para dar la prestación en salud como derecho fundamental.

De aquí que la RGPD dispone que en aquellos casos en los cuales se actué para evitar afectación de otros derechos y libertades fundamentales de toda persona, se facilitara a los profesionales de la salud tratar los datos personales siempre que sea necesario (ver artículo 9 RGPD).

El concepto de interés vital erige en sentido estricto, aquellas situaciones de vida o muerte y en sentido más amplio abarca más supuestos que el citado. En cualquiera de los casos es razonable comprender que apunta a la salvaguarda de un interés vital de las personas no es otra cosa que asistencia sanitaria (Coudert, 2005).

Segundo supuesto. A partir del principio de la finalidad, es relevante afirmar que los datos personales en el ámbito de la salud, tienen por cimiento legitimo el régimen jurídico que habilita la recopilación de la información, sin el consentimiento del titular, en los supuestos que la normatividad menciona, que son aquello relacionados con la «medicina preventiva, laboral, diagnóstico médico, prestación asistencial y sanitario».[3]

Una situación de urgencia, son los casos más puntuales en los cuales profesionales de salud requieren el acceso a los datos personales para cumplir sus funciones relacionadas con las prácticas sanitarias. En consecuencia, la manipulación de los datos en el ámbito de la salud, constituye un fin necesario en el ejercicio propio de la prestación de servicios médicos y con ello un medio para proteger la salud de las personas, Sin embargo, se entiende aquí que la posibilidad de alcanzar esta situación de exceptuar el consentimiento del titular, se justifica únicamente para alcanzar la situación en que, por ejemplo, es posible emitir un diagnóstico determinado y concretar las diferentes opciones de tratamiento asistencial (Sánchez-Caro & Abellán, 2004).

[3] Ver el artículo 9 RGPD en cual dispone «Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad».

De otro lado y desde la perspectiva de la doctrina existe el criterio en el cual la interpretación y alcance de la excepción del consentimiento no solo ha de tenerse en cuenta finalidad de la actuación sanitaria, sino que además ha de realizarse un juicio de proporcionalidad y necesidad según sea el caso en particular (Martín Sánchez, Sánchez-Caro & Abellán-García, 2011).

Tercer supuesto. Tratamiento necesario sin consentimiento del titular de los datos, por razones de interés público en el ámbito de la salud pública, está sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de los individuos. Desde esta perspectiva se entiende por salud pública «todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad» (Unión Europea, 2008)..

Ahora bien, la norma indica las condiciones y situaciones en que es licito en tratamiento de datos realizados por un profesional de la salud cuando representa de manera específica y necesaria determinados intereses como son «la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios» (ver artículo 9 RGPD).

El tratamiento de datos relacionados con la salud refleja una doble perspectiva, por un lado, la salud erige un bien individual intrínseco a cada individuo que se protege de manera personal, pero a la vez desarrolla un matiz colectivo en cuya protección están implicados los poderes públicos que corresponden a un Estado Social de Derecho (Troncoso Reigada, 2018).

De esta manera y para mayor interpretación de las previsiones legales, la pandemia mundial ocasionada por el virus (SAR-CoV-2) conocido como *covid-19*, fue una situación necesaria relativa a salvaguardar la salud pública, de ahí que adquiera la naturaleza de bien jurídico colectivo objeto de protección, cuya tutela se sustenta en el interés social existente en el ambiente de la seguridad sanitaria (Serrano Pérez, 2020).

Por ello el responsable del tratamiento ha de tener especial cuidado con las exigencias del principio de minimización de datos, es decir, tratar los datos que resulten adecuados, pertinentes y no excesivos en relación con los fines perseguidos (Troncoso Reigada, 2018)

En concreto, se habla de categorías especiales de tratamiento de datos, cuando se emplean para «fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos».

Por lo cual la excepción del consentimiento, se rige por los principios de seguridad y finalidad, debido a que las causales para su tratamiento están taxativamente señaladas en el artículo 9 literal I, además, que el encargado o el responsable de realizar el respectivo tratamiento de los datos, ha de ser una persona determinada y legitimada para tal fin, actuando con la premisa de proteger los intereses y los derechos del titular del dato (Troncoso Reigada, 2018)

Una de las novedades en el tratamiento de datos relacionados con la salud es precisamente la minimización en el tratamiento, de ahí que el profesional que efectúe el tratamiento, debe recibir dichos datos de manera anonimizada o con seudónimo, de manera que la identidad solo esté accesible para el médico que ha solicitado el tratamiento de datos (ver artículo 89 RGPD).

El derecho al olvido

De la misma manera que el derecho a prestar o no el consentimiento implica un instrumento *a priori* de control y protección de los datos personales, los derechos de acceso, cancelación y rectificación lo son *a posteriori,* permiten ejercer dominio y control en la información (Garriga Domínguez, 2000).

El reglamento reconoce el derecho de suspensión o derecho de olvido como aquella facultad que ostenta el titular del dato a obtener sin dilación indebida, la supresión del tratamiento los datos de carácter personales, bajo el cumplimiento de ciertas condiciones (art.17) ídem a saber:

> *a) cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;*
>
> *b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;*
>
> *c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;*
>
> *d) los datos personales hayan sido tratados ilícitamente;*
>
> e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
>
> f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

La importancia del derecho de supresión reside en que es un instrumento de defensa para el cumplimiento efectivo del principio de la finalidad, en el sentido que supone que el consentimiento o los datos entregados y tratados, solo podrán

usarse de acuerdo a una finalidad específica y concreta, entonces, es procedente la supresión de los datos que ya no sean necesarios para la realización de la misma, o bien porque pasado el tiempo el titular del dato disponga retirar su consentimiento u oponerse al tratamiento, especialmente en caso que los datos han sido tratados de manera ilícita.

En este sentido vemos que el derecho al olvido constituye una relación con el principio del consentimiento, pues la persona, al ejercitar este derecho manifiesta que estos no deben encontrarse registrados en una base de datos y decide revocar el consentimiento (García Amez, 2010).

Por otra parte, y en relación con los datos personales en el ámbito de la salud, el reglamento establece que el derecho de suspensión no se aplica cuando el tratamiento de los datos sea necesario por razones de interés público en el ámbito de la salud pública o por fines de investigación científica, en la medida que el ejercicio del derecho de supresión haga imposible u obstaculice gravemente el logro o los fines del tratamiento (art.17)

A este punto pareciera que está en duda la efectividad del derecho al olvido, refugiándose en la excepción de la necesidad del tratamiento por razones de interés público, salud pública y por fines de investigación científica, sin embargo, se reconoce el derecho de la supresión de los datos personales aun con tal finalidad, cuando implica vulneración del principio de la dignidad humana, el honor, la intimidad (protección de datos personales) el titular puede ejercer sus derechos y solicitar la eliminación de cualquier información que afecte su imagen como fotografías o aquellos datos relativos a la vida privada (Murillo de la Cueva, 2003).

El derecho al olvido, no es absoluto, se limita su aplicación al entrar en colisión con otros, como el interés público o la salud pública, caso en los cual es necesario realizar una ponderación de interés, para determinar la prevalencia del mismo y sus beneficios (Villanueva, 2003).

Política de tratamiento de datos sensibles en el régimen de salud colombiano

El derecho fundamental a la protección de datos personales (ver articulo 15 Constitución Política de Colombia) es uno de los más importantes en la actual sociedad, el marco jurídico colombiano está conformado por la Constitución Política de Colombia de 1991, la Ley Estatutaria 1581 de 2012 (LEPDP) «por la cual se dictan disposiciones generales para la protección de datos personales»[4] y en el Decreto 1377 de 2013. Este régimen regula de manera general la categoría de los

[4] La presente ley tiene por objeto *desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15* de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

datos personales incluyendo el ámbito de la salud, a la luz de esta normativa LEPDP, se entiende por dato personal, «cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables» (art. 3., lit. c), los principios que se establecen son el de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad (art. 4.), sobre los derechos de los titulares de ser o no informado, oposición, acceso, rectificación, y cancelación están regulados en el Decreto 1377 de 2013.

En Colombia se prohíbe el tratamiento de los datos personales sensibles salvo que el tratamiento sea necesario y en determinados supuestos, como son: aquellos que cuenten con autorización explícita del titular, cuando se tenga por finalidad salvaguardar la vida del titular, así mismo en los casos de miembros o personas que pertenezcan a organismos sin ánimo de lucro y el tratamiento sea efectuado por razones políticas, filosóficas, religiosas o sindicales, con la autorización del Titular y en el curso de actividades legítimas, de igual forma podrá ser objeto de tratamiento los datos sensibles para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial y por ultimo cuando sea para fines históricos, estadísticos o científicos (art. 6)

Además, se contempla como medio de control y se reconoce a favor del titular, el derecho a estar informado de forma explícita y previa, el objeto y finalidad del tratamiento, para que de esta manera extienda su consentimiento (art. 6.) (ver Decreto Nacional 1377 de 2013).

Como se ha dicho anteriormente, la normatividad vigente únicamente permite el tratamiento de datos sensibles cuando concurran alguna de las circunstancias allí previstas, por consiguiente, debemos referirnos a la noción de datos sensibles, como aquella información relacionada directamente con la intimidad del Titular, que al ser divulgada o manipulada se discrimine, bien sea por razón al origen racial o étnico, orientación política, o por convicciones religiosas o filosóficas, o por pertenecer a sindicatos u organizaciones sociales no gubernamentales, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (art. 5.)

La doctrina en su lugar, considera, que los datos sensibles, es toda aquella información que incide en la privacidad y las convicciones personales, que a la vez constituye un riesgo para prácticas discriminatorias frente al resto de las libertades (Losano, Pérez Luño & Guerrero Mateus, 1989).

De otro lado, los datos sentibles constituyen el verdadero ejercicio del derecho de protección de datos personales desde dos aspectos, desde un criterio formal, representa aquellos datos que requieren una serie de requisitos reforzados para que limiten su libre adquisición y circulación. Ahora desde un criterio material, su afectación interfiere directamente la esfera íntima subjetiva e íntima fundamental de los derechos y libertades de las personas (Toniatti, 1991).

Hasta aquí hemos dicho que la protección legislativa, para cierta categoría de datos deviene de la propia naturaleza del derecho fundamental de protección de datos personales, pero una protección aun mayor se efectúa en el tratamiento de dichos datos.

Principios rectores de los datos personales

El contenido esencial del derecho fundamental de protección de datos deriva de los principios y características que tiene el tratamiento de los mismos, lo cual es de forzoso cumplimiento porque al desconocerse genera como consecuencia vulneración al propio derecho (Piñar Mañas, 2005).

Así las cosas, los principios que pueden dirigirse a la configuración del derecho están previstos en LEPDP, aunque de manera específica son cuatro los que apuntan a su regulación: autorización, finalidad, veracidad y confidencialidad, dejando claro que ser efectivos es necesario el reconocimiento y tutela de los derechos de acceso, rectificación, cancelación y oposición.

Principio de autorización

Deslindadas las nociones anteriores, resulta relevante concentrarnos en el tratamiento de Datos Personales acorde a las previsiones de la normatividad vigente, y para el efecto daremos paso a uno de los principios que es inherente a la protección de datos, la respectiva autorización previa, expresa e informada del Titular.

En materia de protección de datos, los principios tienen la intención de determinar conceptualmente la forma más eficaz de proteger a las personas, que ellas salvaguarden su libertad, el dominio y el poder de decisión sobre los datos personales (Rebollo Delgado & Serrano Pérez, 2008).

Al respecto la autorización previa e informada del titular es requisito *sine qua non* para el tratamiento de los datos personales (art. 9), en la doctrina se conoce como consentimiento informado, visto como el proceso mediante el cual se garantiza que, después de haber recibido y comprendido toda la información necesaria y pertinente, el sujeto voluntariamente manifiesta su deseo. (Moreno Sánchez & Cano Valle, 2004). Mediante dicha expresión de voluntad otorgan su autorización por medio de un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta a fin de constatar de forma inequívoca que sin el consentimiento del titular los datos nunca hubieran sido capturados y almacenados en medios electrónicos o físicos (SIC, 2020).

En consecuencia, toda actividad relacionada con el tratamiento de datos, tendrá que ser realizada con la autorización otorgada por el Titular, salvo los casos excepcionales que señala la ley, previo a informar de manera sucinta y completa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;

c) Los derechos que le asisten como Titular;

d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Ahora el dato personal objeto de tratamiento ha de ser veraz, completo, exacto, actualizado, comprobable y comprensible (SIC, 2014).

Un elemento fundamental del consentimiento informado es garantizar la confidencialidad y reserva de la información tratada, por lo que los sujetos que intervienen o reciban la información, mediante ese acto de confianza, le asiste el deber de conservar en secreto todos los aspectos y circunstancias ajenas que solo le interesan al titular del dato, y más aún cuando se trata de información sensible.

Desde esta perspectiva, el legislador estableció los casos en los cuales es posible adelantar el tratamiento de los datos sin el consentimiento del titular, advirtiendo que quien acceda a la información está comprometido a cumplir con los principios y disposiciones contenidas para el tratamiento de los datos, tales supuestos son:

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.

Para lo cual, vemos que los supuestos que trata los numeral c) y d) hacen referencia a los datos sensibles, pues están relacionados con el origen racial, salud, sexual e íntimo de las personas, que al manipular dicha información se afectaría la intimidad, el buen nombre y la privacidad y demás prerrogativas que cobija el derecho de protección de datos personales.

En este sentido, cobra validez el principio de la finalidad, es decir que el tratamiento de los datos podrá realizarse exclusivamente en los casos en que sea absolutamente necesario para los fines de una investigación concreta o en casos de urgencia médica (Rebollo Delgado & Serrano Pérez, 1998).

Principio de finalidad

La prerrogativa que establece la normatividad y aplicable a los tratamientos, es el de la limitación a la finalidad, caso en los cual, los datos personales serán recogidos para los fines determinados de manera explícita y legítima y no serán tratados con otros fines. Significa, por tanto, que el tratamiento no necesitará una base jurídica distinta que la que permitió la obtención de los datos si los va a destinar en la investigación científica o para la urgencia médica. (Recuero Linares, 2019).

En desarrollo del principio de finalidad, la recolección de datos ha de limitarse a aquellos datos personales pertinentes y adecuados para la finalidad del tratamiento o requeridos conforme a la normatividad vigente (art. 4, Decreto 1377, 2013).

Justamente, en los casos que el consentimiento no es requerido para llevar a cabo el tratamiento de los datos, el principio de la finalidad cobra importancia, pues para el titular de los datos se convierte en la principal garantía, para que el tratamiento se desarrollare con el pleno respeto de sus derechos fundamentales, en la medida que la persona conozca que va a pasar con sus datos, para que van a ser empleados de forma concreta, será el seguro para que la información sea utilizada en el ámbito para el cual se recolecto.

En resumen, los requisitos que exige la normativa para que la finalidad sea acorde a la Ley, bastara que deba ser necesaria, determinada y explícita, además que los datos no se pueden dar una finalidad distinta a la razón por la cual fueron recolectados, que para el tema que nos ocupa, el ámbito concreto, es la de proteger la salud de las personas y en situaciones que se lleve a cabo investigaciones científicas (Remolina Angarita, 2013).

En caso que se manipule o utilice los datos con otro fin distinto al autorizado, y en caso que no se otorgue dicho consentimiento y el tratamiento se destine por razones no previstas en la ley, al titular del dato le asiste la facultad de ejercer el derecho de supresión de la información, acudir ante la autoridad de vigilancia que corresponde a la SIC, para que se adelante las investigaciones pertinentes y sancione al responsable, por incumplimiento en las funciones que le asigna la ley.

Así mismo, y desarrollo del principio de finalidad, el titular del dato tiene el derecho de solicitar en cualquier momento ante el responsable del tratamiento de los datos, se le informe sobre el uso dado a sus datos y la razón por la cual se están tratando los mismos, también en ejercicio de este derecho podrá conocer actualizar o rectificar la información que reposa en las bases de datos (art. 8, Ley 1581 de 2012).

El derecho a la protección de datos personales se concreta en el derecho de las personas a controlar sus propios datos, por ello es fundamental que el titular de la información conozca la finalidad específica que justifica su uso y el tratamiento destinado a sus datos, ya que al no tener control sobre la información está en riesgo de vulneración el derecho (Remolina Angarita, 2013)

Principio de veracidad

Los datos personales sometidos a tratamiento han de ser veraces, completos, exactos, actualizados, comprobables y comprensibles, y en supuestos que estén parciales, incompletos, fraccionados o que induzcan a error, no podrán ser tratados y en caso que se desarrolle el mismo, este será ilícito (SIC, 2020).

En este sentido, la ley 1581 concede al titular el derecho de acceder a sus propios datos, e impone al responsable del tratamiento de los datos, la obligación de rectificar la información que previamente le han suministrado, cuando tenga razones para pensar que los datos no son del todo correctos, sin embargo, cuando resulte que la información no es correcta, le asiste la obligación de destruirlos inmediatamente e informar al titular.

Este principio es en sí un instrumento de protección de los datos, ya que busca que los datos objeto de tratamiento sean pertinentes, adecuados y no excesivos en relación con la finalidad determinada, expresada y autorizada (Davara Rodríguez, 2018).

De este modo, a los responsables y encargados del tratamiento de los datos les asiste el deber de garantizar el principio de veracidad de los datos, y en caso de incumplimiento acarreará las sanciones contempladas en la ley y de competencia de la SIC.

Principio de confidencialidad

El derecho de confidencialidad, implica que ideologías, datos e información de tipo personal e íntimo son de carácter reservado, son suministrados bajo estrictos parámetros de autorización y el expreso consentimiento del titular, en especial es una garantía para que las personas no pierdan el poder de disposición y control de su propia información (Londoño Toro, 1987).

La ley 1581 de 2012, estableció que el principio de confidencialidad es el deber que le asiste a todas las personas que intervengan en el tratamiento de datos personales, de garantizar la reserva de la información, inclusive después que finalice el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando la ley lo autoriza, entonces, desde la óptica de las obligaciones que se derivan para los terceros responsables en el tratamiento de los datos, surge el derecho de *acceso, de rectificación y cancelación* (art.4)

Se entiende por derecho de acceso, a la facultad que tiene el titular a pedir y obtener de forma gratuita información sobre sus datos personales sometidos a tratamiento, al menos una vez cada 30 días o cada vez que existan modificaciones sustanciales al tratamiento de los datos que amerita una consulta (art. 21, Decreto 1377, 2013).

El derecho de acceso, también es visto como método de comprobación de la exactitud y licitud del tratamiento, así como la posibilidad de conocer el sistema que subyace al tratamiento (Rebollo Delgado & Serrano Pérez, 1998)

Significa que el acceso a la información está restringido a terceros ajenos no autorizados, salvo la información pública, así mismo se prohíbe su circulación por internet u otros medios de divulgación o comunicación masiva, excepto en los casos que señale la ley, al respecto la Ley 1581 de 2012 dispone que «Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley».

Ahora bien, el derecho de rectificación, consiste en la potestad que tiene el titular para exigir al responsable del tratamiento que cumpla con las exigencias del principio de veracidad, adoptando las medidas necesarias para corregir los errores o subsanar la información incompleta y así el tratamiento sea reflejo cierto de su expresa voluntad (Davara Rodríguez, 2017).

Aunque la legislación actual (ver artículo 22 del Decreto 1377 del 2013) reconoce el derecho de rectificación de los datos, no se desarrolla un apartado específico frente al tratamiento de los datos en general y en especialmente lo referido a la categoría especial de los datos, para que de esta manera se enuncien las obligaciones enfocadas al cumplimiento de dicho principio.

Sin embargo, la doctrina ha dicho que el principio de calidad es una garantía visible en la práctica, puesto que establece restricciones en la utilización de los datos, los cuales solo pueden ser destinados para las finalidades «determinadas, explícitas y legítimas» autorizadas por el titular o por mandato de la ley, no pudiendo darse una finalidad distinta para aquellas que fue recogida (Troncoso Reigada, 2010).

Por lo tanto, la rectificación es un derecho personalísimo que solo le asiste interés al titular del dato ya que su ejercicio plantea una serie de principios que refieren a la privacidad, el honor, la dignidad e intimidad de las personas, el cual se ejerce mediante una solicitud expresa y clara motivada en la corrección, modificación o complemento de datos objeto de tratamiento, la relevancia de este derecho de rectificación reside en su efecto o resultado, que no es otro que el de «reducir una cosa a la exactitud que debe tener» (Carrillo López, 1988).

El derecho de cancelación, de conformidad con el texto normativo, significa que previa solicitud del titular de los datos personales sometidos a tratamiento, estos pueden ser eliminados cuando sean utilizados para fines distintos al propósito del tratamiento, o cuando no se respeten los principios, derechos,

garantías constitucionales o legales y como requisito de procedencia, la SIC haya determinado algún grado de incumplimiento por parte del responsable o encargado del tratamiento (art.8)

Al respecto, la ley estatutaria no regula de manera clara y especifica el derecho de supresión de los datos y en consecuencia delego SIC, la determinación de régimen de responsabilidad por violación directa a la Constitución y la Ley en el tratamiento de los datos, lo que cual es dable concluir que dicha regulación solo se someterán las organizaciones comerciales, que son las puede vigilar la Superintendencia (Burgos Suárez, 2019).

La supresión de los datos también se conoce como *derecho al olvido,* conforme al cual, el titular tiene la posibilidad de solicitar la desaparición de aquellos datos negativos (*no queridos, perjudiciales, socialmente reprobados o desfavorables*) de los sistemas de registro, es un derecho a la caducidad del dato negativo (Tafoya Hernández & Cruz Ramos, 2014).

Políticas de tratamiento de datos personales

El Decreto 1377 de 2013, dispone en el artículo 13, los lineamientos necesarios y obligatorios para el cumplimiento de los principios y las obligaciones de todos aquellos encargados o responsables del tratamiento de datos personales.

En este sentido, dicha política se aplicará a todas y cada una de las bases de datos que sean objeto de tratamiento *recolección, almacenamiento, uso, circulación y supresión* de datos de carácter personal (SIC, 2020).

La política de tratamiento de los datos personales, se constituye con el fin que, la sociedad en general conozca y tenga a su disposición la información sobre el tratamiento, los fines del mismo, así como el contenido de sus derechos, la forma que pueden ejercerlos y así se proteja el derecho constitucional que tienen todas las personas a conocer, actualizar, rectificar y suprimir sus datos personales.

Al respeto, la normatividad dispone que toda política de tratamiento de datos personales, ha de constar en medio físico o electrónico, con un lenguaje claro y sencillo, de conocimiento a los titulares del dato, donde incluye la siguiente información:

1. *Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable.*
2. *Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.*
3. *Derechos que le asisten como Titular.*
4. *Persona o área 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.

5. *Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.*
6. *Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.*
7. *Cualquier cambio sustancial en las políticas de tratamiento, en los términos descritos en el artículo 5° del presente decreto, deberá ser comunicado oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas* (ver artículo 13 del Decreto 1377 del 2013).

Es de destacar que el articulado señala de forma taxativamente los deberes, obligaciones y condiciones exigibles al responsable y encargado del tratamiento de los datos, en especial la de desarrollar una política de tratamiento de los datos, acorde a los derechos y garantías constitucionales y legales so pena de sancionado por la SIC.

De acuerdo a lo reglamentado por la SIC, la política de tratamiento de los datos personales ha de contener el conjunto de operaciones y procedimientos que incluyen recolección de datos, su almacenamiento, uso, circulación y/o supresión. Así mismo, el tratamiento ha de realizarse exclusivamente para las finalidades autorizadas por el titular y previstas en la ley (SIC, 2020).

Por último y en aquellos casos que no sea posible comunicar al interesado las políticas de tratamiento de la información, los responsables están obligados a informar de manera oportuna, a través de un *aviso de privacidad*[5], sobre la existencia de dicha política y la forma de disponer de la mismas en el momento de la recolección de los datos personales (art.14)

Autoridad de protección de datos

Con la entrada en vigencia de la ley estatutaria 1581 de 2012, se delegó a la Superintendencia de Industria y Comercio (SIC), una institución de orden nacional, descentralizada que cuenta con personería jurídica y está adscrita a la Rama Ejecutiva, la potestad de vigilar y controlar el tratamiento de los datos personales.

[5] Decreto 1377 del 2013 señala en su artículo 15 lo respectivo a contenido del aviso de privacidad el cual debe contener como minino: 1. Nombre o razón social y datos de contacto del responsable del tratamiento. 2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo. 3. Los derechos que le asisten al titular. 4. Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información. No obstante, lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos. En todo caso, la divulgación del Aviso de Privacidad no eximirá al Responsable de la obligación de dar a conocer a los titulares la política de tratamiento de la información, de conformidad con lo establecido en este decreto.

La SIC cuenta con facultades sancionatorias, como mecanismo de control para combatir el manejo indiscriminado de los datos personales por parte de los encargados del tratamiento, y vigilante del ejercicio efectivo de sus funciones (Remolina Angarita, 2013).

El poder conferido por el legislador a una autoridad administrativa es con el fin de, asegurar la eficacia de los derechos fundamentales de los titulares de la información, contenidos en los procesos de administración de datos personales (Camargo, 2013).

Dicho proceso sancionatorio inicia con la denuncia instaurada por el titular del dato una vez haya agotado la consulta ante el responsable o Encargado del tratamiento, luego procede la notificación al implicado, la presentación de alegatos y finalmente la adopción del fallo, el cual debe estar motivado por los principios que garantizan el ejercicio del debido proceso en sede administrativa (Remolina Angarita, 2013)

Conclusiones

El principal mecanismo de protección de los datos personales es por medio de una regulación normativa, que busque limitar el ámbito de acceso a la información personal estableciendo reglas para quienes tengan acceso a los mismos, evitando de esta forma, que la información de las personas circule libremente y sin control alguno por parte de sus titulares.

Como se ha mencionado anteriormente, que contamos con marco jurídico Constitucional y Legal que se complementando en muchos apartes por el por las disposiciones establecidas por la Unión Europea en materia de protección de datos personales o el derecho a la autodeterminación informática (Remolina Angarita, 2013)

Entre los aportes más relevantes y destacados de la ley 1581 de 2012, es el alcance que se da a la información personal y la importancia del manejo de la misma, como respuesta a la problemática que promueve el acelerado crecimiento en la sociedad, en donde la información se ha convertido en una fuente esencial para el desarrollo de fenómenos económicos, sociales y políticos.

De esta manera, es claro que se requiere una nueva perspectiva para abordar los asuntos relacionados con la intimidad y privacidad de las personas, en lo que aquí se ha propuesto, la importancia de proteger la información personal en el ámbito de la salud

Al reflexionar sobre el tratamiento de los datos personales en el ámbito de la salud, se cuestiona si la regulación existente responde a los retos y desafíos que impone la sociedad de la información, en el sentido de categorizar los derechos de las personas en el ámbito de su información personal, y sea el criterio relevante para adoptar una posición de respeto por la protección de los datos.

La ley estatutaria 1581 de 2012 estableció de manera general el reglamento para el tratamiento de los datos personales, sin embargo, nos permitimos señalar como primera medida que, aunque dicho instrumento resultar ser un medio pertinente a la hora de limitar las facultades que goza el aparato estatal en relación con los derechos y libertades que benefician a todo el conglomerado social, se olvida el legislador en fijar de manera clara, el derrotero a seguir, cuando nos referimos a información sensible de alto valor que quiere conquistar organizaciones o sociedades que imperan en el mundo de la información.

Por consiguiente, ahora, resaltamos los aspectos más relevantes que han legislado otros ordenamientos jurídicos, como el sistema jurídico de Europa que se encuentra en *Reglamento Europeo de Protección de Datos Personales* (RGPD), ya que dicho instrumento califica en una categoría especial a los datos sensibles y por ello confiriere una regulación, tratamiento y protección unitaria. En este aspecto, el Reglamento ha consolidado un concepto amplio de datos relativos a la salud, lo cual permite extender el ámbito de protección de los datos, como respuesta a los supuestos prácticos que acontecen en la realidad, en especial en el contexto hospitalario.

Como punto de partida de todo tratamiento de datos ha de estar fundamentado la autorización del titular, el derecho de protección de datos personales se constituye en la facultad de una persona de controlar lo que sucede con sus datos, y será la capacidad de esa persona lo que le permite expresar su voluntad y así consentir o no el tratamiento, esta figura del consentimiento informado, es la concreción de esa autonomía de la voluntad, en consecuencia se desprenden la configuración del derecho a ser informado de los parámetros que van a rodear al tratamiento de sus datos (art 13)

La norma europea de protección de datos establece una serie de principios y derechos que han de aplicarse como garantías a aquellos datos de especial protección, los datos sensibles, primero que todo advierte que el tratamiento debe respetar los denominados principios de calidad, finalidad, pertinencia y veracidad. Se trata de un conjunto de principios generales que no solo reconocen la necesidad de proteger y asegurar la conservación de la intimidad y el carácter personal e íntimo de los datos que se manipulan en el sector de la salud, sino que también, prevén los riesgos que conlleva el tratamiento de los mismos.

Partiendo de esta premisa, el régimen de protección de los datos cuenta con diferentes aspectos, entre ellos, el principio de ponderación de intereses cuando entra en conflicto derechos de gran relevancia de la condición humana, aquí la búsqueda del equilibrio se concreta entre la *necesidad* de utilizar los datos sensibles para los fines habilitados por la ley que apuntan a proteger el derecho de la salud, y la *necesidad* de proteger la intimidad y el derecho a la protección de datos personales.

Sin embargo, debemos reconocer el esfuerzo normativo con la expedición de la ley 1581 de 2012 y sus decretos reglamentarios, representa un paso importante en el propósito de proteger la información personal de los ciudadanos, por lo que es necesario destacar las funciones administrativas y jurisdiccionales encomendadas a la Superintendencia de Industria y Comercio como la entidad encargada de la protección de los datos personales.

Referencias

Aparicio Salom, J. (2009). *Estudio sobre la ley orgánica de protección de datos de carácter personal*. Aranzadi.

Arenas Ramiro, M. (2006). *El derecho a la protección de datos personales en Europa*. Tirant lo Blanch.

Bautista, Avellaneda, M E (2015). *El derecho a la intimidad y su disponibilidad Pública.* Universidad Católica de Colombia, Colección JUS público N 7.

Burgos Suárez, J. A. (2019). Ni rectificación, ni olvido Una tesis sobre el conflicto de derechos entre el derecho al olvido y el derecho a la información en Colombia. *Escribanía, 17*(1),125-136. https://revistasum.umanizales.edu.co/ojs/index.php/escribania/article/view/3508

Camargo, P. P. (2013). *El habeas data: derecho a la intimidad*. Leyer.

Canales, A., Blanco, M. J. & Piñar Mañas, J. L. (2005). *Protección de datos de carácter personal en Iberoamérica*. Tirant lo Blanch.

Cantero Martínez, J. (2005). *La autonomía del paciente: del consentimiento informado al testamento vital.* Bomarzo.

Carrillo López, M. (1988). El derecho a la información y veracidad informativa. *Revista Española de Derecho Constitucional, 8*(23), 187-206.

Castillo Vázquez, I. C. (2007). *Protección de datos: cuestiones constitucionales y administrativas*. Thomson-Civitas.

Coudert, F. (2005). Tratamiento de datos especialmente protegidos. En C. Almuzara Almaida (coord.). *Estudio práctico sobre la protección de datos de carácter personal* (pp. 301-326). Lex Nova.

Cruz Ramírez, A. (s.f.). *Habeas Data. La protección Constitucional y Jurisprudencial en Colombia.* https://www.scjn.gob.mx/sites/default/files/transparencia/documentos/becarios/028alejandro-cruz-ramirez.pdf

Davara Rodríguez, M. A. (2018). Acerca de la denominada protección de datos. *Actualidad Administrativa, 10.*

Davara Rodríguez, M.A. (2017). El delegado de protección de datos.

Galán Cortés, J. C. (1997). *El consentimiento informado del usuario de los servicios sanitarios*. Colex.

García Amez, J. (2010). La protección de datos del usuario de la sanidad: derecho a la intimidad y asistencia sanitaria. *DS: Derecho y Salud, 20*(1), 43-69.

Garriga Domínguez, A. (2000). Una nueva exigencia de la libertad: La protección de los datos sensibles. *Dereito: Revista xuridica da Universidade de Santiago de Compostela, 9*(2), 49-81. https://dialnet.unirioja.es/servlet/articulo?codigo=173971

Lizárraga Bonelli, E. (2019). Protección de datos y asistencia médica: hacia un nuevo paradigma del consentimiento. *Actualidad del Derecho Sanitario, 270,* 469-472.

Londoño Toro, B. (1987). El derecho a la intimidad, el honor y la propia imagen enfrentado a las nuevas tecnologías informáticas. *Revista Facultad de Derecho y Ciencias Políticas, 77,* 107-146. https://revistas.upb.edu.co/index.php/derecho/article/view/4970

Losano, M. G., Pérez Luño, A. & Guerrero Mateus, M. F. (1989). *Libertad informática y leyes de protección de datos personales*. Centro de Estudios Políticos y Sociales.

Martín Sánchez, I., Sánchez-Caro, J. & Abellán-García, F. (2011). *Libertad de consciencia y medicamento. Una guía práctica*. Comares.

Moreno Sánchez, J. A. & Cano Valle, F. (2004). El consentimiento bajo información ¿un documento o un proceso? En I. Brena Sesma & L. T. Díaz Müller (coords.). *Segundas Jornadas sobre Globalización y Derechos Humanos: bioética y biotecnología* (pp. 29-40).

Murillo de la Cueva, P. L. (2003). Informática y protección de datos personales. *Revista Chilena de Derecho Informático, 2*. https://revistas.uchile.cl/index.php/RCHDI/article/view/10656

Murillo de la Cueva, P. L. & Piñar Mañas, J. L. (1990). *El derecho a la autodeterminación informativa*. Fundación Coloquio Jurídico Europeo.

Piñar Mañas, J. L. (2005). El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. *Asamblea: revista parlamentaria de la Asamblea de Madrid, 13,* 21-46.

Polo Roca, A. (2020). Sociedad de la información, sociedad digital, sociedad de control. *Inguruak, 68,* 50-77.

Rallo Lombarte, A. (2019). El nuevo derecho de protección de datos. *Revista Española de Derecho Constitucional, 116,* 45-74.

Rebollo Delgado, L. & Serrano Pérez, M. M. (2008). *Introducción a la protección de datos*. Dykinson.

Rebollo Delgado, L. (1998). Derechos de la personalidad y datos personales. *Revista de Derecho Político*, *44,* 143-206.

Recuero Linares, M. 2019. Transferencias internacionales de datos genéticos y datos de salud con fines de investigación. *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada, Nº extra,1,* 413-433.

Remolina Angarita, N. (2013). *Tratamiento de datos personales: aproximación internacional y comentarios de la Ley 1581 de 2012*. Legis.

Rodríguez López, P. (2004). *La autonomía del paciente: información, consentimiento y documentación clínica*. Dilex.

Sánchez-Caro, J. & Abellán, F. (2004). *Datos de salud y datos genéticos. Su protección en la Unión Europea y en España*. Comares.

Seoane Rodríguez, J. A. (2002). De la intimidad genética al derecho a la protección de datos genéticos. *Revista de Derecho y Genoma Humano, 17*, 135-175.

Serrano Pérez, M. M. (2020). El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento general de protección de datos y de la Ley de protección de datos personales y garantía de los derechos digitales. *Estudios de Deusto, 68*(2), 257-292. https://revista-estudios.revistas.deusto.es/article/view/1952

Superintendencia de Industria y Comercio (2014). *Políticas de tratamiento de la información personal en la Superintendencia de Industria y Comercio*.

Superintendencia de Industria y Comercio (2020). *Política de tratamiento de datos personales*. https://sedeelectronica.sic.gov.co/sites/default/files/normativa/Política-de-Tratamiento-de-Datos-Personales.pdf

Tafoya Hernández, J. G. & Cruz Ramos. C. G. (2014). Reflexiones en torno al derecho el olvido. *IFDP: Revista del Instituto Federal de Defensa Pública, 18,* 76-105. https://biblioteca.corteidh.or.cr/documento/68375

Toniatti, R. (1991). Libertad informática y derecho a la protección de los datos personales. *Revista Vasca de Administración Pública, 29,* 139.

Troncoso Reigada, A. (2018). Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. *Revista de Derecho y Genoma Humano*, *49,* 187-266.

Troncoso Reigada, A. (2010). *La protección de datos personales, en busca del equilibrio*. Tirant lo Blanch.

Unión Europea (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. *Diario Oficial de la Unión Europea.* https://www.boe.es/doue/2016/119/L00001-00088.pdf

Unión Europea (2016). Reglamento de protección de datos personales de la Unión Europea RPDP, 2016. *Diario Oficial de la Unión Europea.* https://www.boe.es/doue/2016/119/L00001-00088.pdf

Unión Europea (2008). Reglamento (CE) nº 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo. *Agencia Estatal Boletín Oficial del Estado.* https://www.boe.es/buscar/doc.php?id=DOUE-L-2008-82645

Villanueva, E. (2003). *El derecho de la información. Conceptos básicos*. Ciespal.