Fecha de recepción: 8 de marzo de 2021
Fecha de evaluación: 1 de junio de 2021
Fecha de aprobación: 1 de julio de 2021

Estructuración de los elementos de la responsabilidad del Estado por el uso indebido de los datos relacionados con el estado de salud. *Análisis dogmático y biojurídico*[*]

Laura Victoria Puentes Trujillo[**]

Para citar este artículo
Puentes, L. (2021). Estructuración de los elementos de la responsabilidad del Estado por el uso indebido de los datos relacionados con el estado de salud. *Análisis dogmático y biojurídico*. *Vía Iuris*, (31), 57-74. https://doi.org/10.37511/viaiuris.n31a3

RESUMEN

Con la pandemia ocasionada por la propagación de la covid-19, los Estados adoptaron múltiples instrumentos que no solo les permitieron controlar la transmisión de la enfermedad sino, además, conocer en tiempo real el estado de salud de las personas. A partir del uso de aplicaciones, el Estado colombiano y las entidades territoriales tuvieron acceso ilimitado a datos personales y sensibles, amparados en la excepción relativa al ejercicio de funciones públicas y a la situación de emergencia sanitaria. En este contexto, a partir de la revisión de un caso específico y la aplicación de un método comparativo con el referente mundial para el tratamiento de datos personales, el presente artículo tiene por objetivo mostrar con base en qué tipo de responsabilidad y de qué forma se articulan los elementos en los casos de tratamiento indebido de los datos personales por parte del Estado. En ese sentido, en el presente escrito se presentan los argumentos de orden legal y teórico que permiten afirmar que si bien las entidades estatales en cumplimiento de sus funciones no requieren de autorización para el tratamiento de los datos personales, no están exentas de cumplir con las demás condiciones legales que aseguren los derechos de *habeas data* y de datos personales.

Para el caso específico de los datos relativos al estado de salud en el contexto de una emergencia sanitaria, cuando las autoridades estatales no informan expresamente cuál es la finalidad con la que tratarán los datos personales y no apliquen las reglas del consentimiento informado, habrá lugar a la atribución de responsabilidad estatal por la afectación relevante a bienes o derechos convencional y constitucionalmente amparados; esto, en la medida en que en estos casos hay una transgresión de derechos directamente relacionados con la personalidad: el derecho de *habeas data* y de datos personales.

DOI: https://doi.org/10.37511/viaiuris.n31a3

Palabras clave
Datos personales, autonomía, responsabilidad del Estado, administración de datos, plataforma digital, emergencia sanitaria.

* Este artículo es uno de los resultados del proyecto de investigación "Autodeterminación Genética y Enhancement ¿tenemos un derecho a mejorarnos genéticamente?" a cargo de la autora de este artículo, como integrante del Grupo de Investigación en Derecho Administrativo de la Universidad Autónoma Latinoamericana de Medellín. (Periodo 2020). Medellín, Colombia.

** Candidata a Doctora en Derecho de la Universidad Externado de Colombia y la Universidad del País Vasco, España. Magíster en Derecho con mención en Derecho Público de la Universidad de Chile. Especialista en Derecho Informático y de las Nuevas Tecnologías de la Universidad Externado de Colombia. Abogada, Universidad del Cauca. Profesora investigadora de la Escuela de Posgrados de la Universidad Autónoma Latinoamericana de Medellín. Medellín, Colombia. Correo electrónico de contacto: laura.puentestr@unaula.edu.co. Orcid: https://orcid.org/0000-0003-1700-166X

Structuring the elements of the State's responsibility for the improper use of data related to the state of health. *Dogmatic and bio-legal análisis*

Laura Victoria Puentes Trujillo

ABSTRACT

With the pandemic caused by the spread of Covid-19, States adopted multiple instruments that not only allowed them to control the transmission of the disease, but also to know in real time the health status of people. Based on the use of applications, the Colombian State and the territorial entities had unlimited access to personal and sensitive data, protected by the exception related to the exercise of public functions and the health emergency.

Taking into account this context, based on the review of a specific case and applying a comparative method with the world benchmark for the processing of personal data, this article aims to show based on what type of responsibility and in what way they articulate their elements, in cases of improper treatment of personal data by the State; In this sense, this document presents the legal and theoretical arguments that allow to affirm that although state entities in compliance with their functions do not require authorization for the processing of personal data, they are not exempt from complying with the Other legal conditions that ensure the rights to privacy, habeas data and personal data.

For the specific case of data related to health status in the context of a health emergency, when state authorities do not expressly inform what is the purpose for which they will process personal data and do not apply the rules of informed consent, there will be room for the attribution of state responsibility for the relevant affectation to goods or rights conventionally and constitutionally protected; this, to the extent that in these cases there is a violation of rights directly related to personality: the right to privacy, habeas data and personal data.

Keywords

Personal data, autonomy, State responsibility, data administration, digital platform, health emergency.

Estruturação dos elementos de responsabilidade do Estado pela utilização indevida de dados relacionados com a saúde. *Análise dogmática e biolegal*

Laura Victoria Puentes Trujillo

RESUMO

Com a pandemia causada pela propagação do Covid-19, os Estados adoptaram múltiplos instrumentos que lhes permitiram não só controlar a transmissão da doença, mas também conhecer em tempo real o estado de saúde das pessoas. Com base na utilização de aplicações, o Estado colombiano e as entidades territoriais tinham acesso ilimitado aos dados pessoais e sensíveis, protegidos pela excepção relativa ao exercício de funções públicas e à situação de emergência sanitária.

Tendo em conta este contexto, com base na análise de um caso específico e aplicando um método comparativo com a referência global para o tratamento de dados pessoais, o objectivo deste artigo é mostrar que tipo de responsabilidade e como se articulam os seus elementos em casos de tratamento incorrecto de dados pessoais pelo Estado; Neste sentido, este documento apresenta os argumentos jurídicos e teóricos que nos permitem afirmar que, embora as entidades estatais no cumprimento das suas funções não necessitem de autorização para o tratamento de dados pessoais, não estão isentas de cumprir as outras condições legais que asseguram os direitos de habeas data e dados pessoais.

No caso específico dos dados relativos ao estado de saúde no contexto de uma emergência sanitária, quando as autoridades estatais não informam expressamente da finalidade para a qual os dados pessoais serão tratados e não aplicam as regras do consentimento informado, haverá lugar à atribuição de responsabilidade estatal pela afectação relevante de bens ou direitos convencional e constitucionalmente protegidos; isto, na medida em que nestes casos haja uma transgressão dos direitos directamente relacionados com a personalidade: o direito a habeas data e a dados pessoais.

Palavras-chave
Dados pessoais, autonomia, responsabilidade do Estado, gestão de dados, plataforma digital, emergência sanitária.

Structurer les éléments de la responsabilité de l'État en cas d'utilisation abusive de données relatives à la santé. *Analyse dogmatique et biolégale*

Laura Victoria Puentes Trujillo

RÉSUMÉ

Avec la pandémie provoquée par la propagation du Covid-19, les États ont adopté de multiples instruments qui leur ont permis non seulement de contrôler la transmission de la maladie mais aussi de connaître en temps réel l'état de santé des personnes. Sur la base de l'utilisation d'applications, l'État colombien et les entités territoriales avaient un accès illimité aux données personnelles et sensibles, protégées par l'exception relative à l'exercice de fonctions publiques et à la situation d'urgence sanitaire.

Compte tenu de ce contexte, sur la base de l'examen d'un cas concret et en appliquant une méthode comparative avec la référence mondiale en matière de traitement des données à caractère personnel, l'objectif de cet article est de montrer quel type de responsabilité et comment ses éléments s'articulent dans les cas de traitement abusif de données à caractère personnel par l'État ; Dans ce sens, ce document présente les arguments juridiques et théoriques qui nous permettent d'affirmer que, bien que les entités étatiques, dans le respect de leurs fonctions, n'aient pas besoin d'autorisation pour le traitement des données personnelles, elles ne sont pas exemptées de respecter les autres conditions légales qui garantissent les droits aux données d'habeas et aux données personnelles.

Dans le cas spécifique des données relatives à l'état de santé dans le contexte d'une urgence sanitaire, lorsque les autorités de l'État n'informent pas expressément de la finalité du traitement des données personnelles et n'appliquent pas les règles du consentement éclairé, il y aura place pour l'attribution de la responsabilité de l'État pour l'affectation pertinente de biens ou de droits conventionnellement et constitutionnellement protégés ; ceci, dans la mesure où dans ces cas il y a une transgression des droits directement liés à la personnalité : le droit à l'habeas data et aux données personnelles.

Mots-clés

Données personnelles, autonomie, responsabilité de l'État, gestion des données, plateforme numérique, urgence sanitaire.

INTRODUCCIÓN

Con ocasión de la emergencia sanitaria originada en la propagación del coronavirus, uno de los asuntos que ha tomado relevancia en el control y la prevención de la propagación de la enfermedad es el suministro de los datos relacionados con el estado de salud, que van acompañados de otros datos personales o sensibles. Esto significa que los datos del estado de salud no solo están siendo tratados por personal médico, sino que las empresas, los empleadores y el propio Estado tienen acceso a ellos, sin que se tenga claridad acerca de cuáles son los requisitos para que sea legítimo su tratamiento, incluida su circulación, ni cuál es el alcance de la causal que permite a las autoridades su tratamiento sin la autorización del titular.

Teniendo en cuenta, entonces, que el tratamiento de los datos acerca del estado de salud se constituye como un elemento necesario de prevención en situaciones de emergencia sanitaria, en este artículo me ocuparé de analizar, conforme a las reglas vigentes en el ordenamiento colombiano, el tipo de responsabilidad en la que puede incurrir el Estado por el indebido tratamiento de los datos personales y cuáles son los elementos que la estructuran; para ello revisaré el caso de *Medellín me Cuida*. Este caso es relevante por cuanto al inicio de la declaratoria de emergencia económica, social y ecológica[1] Medellín fue una de las ciudades de Colombia destacadas en la contención de la enfermedad mediante el uso del mencionado aplicativo, pero en los meses siguientes fue una de las ciudades que más reportó número de contagiados[2] y obtuvo una ocupación de las Unidades de Cuidados Intensivos (UCI) por encima del 95%.

El caso de *Medellín me Cuida* permite hacer un análisis de la estructuración de los elementos de la responsabilidad del Estado por el uso indebido de datos sensibles, esto es, fijar una línea que nos permita distinguir los eventos en los que es legítimo el uso de tales datos para fines de interés general de aquellos en los que se puede atribuir responsabilidad por el desbordamiento de las prerrogativas estatales de quienes tienen a cargo la ejecución de acciones de contención de la enfermedad en calidad de autoridades sanitarias.

En este sentido, la pregunta con base en la cual se adelantó la investigación es, a partir de los principios aplicables al tratamiento de los datos sensibles, ¿cuáles son los límites razonables para el tratamiento excepcional de los datos de salud por parte de las autoridades estatales, cuyo desconocimiento configure la responsabilidad del Estado?

A manera de hipótesis, la idea que se prueba mediante este artículo es que el tratamiento de datos sensibles —incluidos los datos relativos a la salud— por parte de las entidades estatales tiene los mismos límites legales y constitucionales que el tratamiento de datos por parte de particulares, ya que lo único que la ley excepciona es la necesidad de obtener la autorización por parte del titular. En ese sentido, cuando no se cumplen los criterios legales, el Estado incurre en responsabilidad por afectación de bienes jurídicos constitucional y convencionalmente protegidos, ya que en estos casos se vulneran los derechos a la intimidad, los datos personales y el *habeas data*, estos dos últimos como expresión del principio de autodeterminación informativa.

Para abordar el asunto, empleé el estudio de caso como metodología, apoyado en la revisión teórica y dogmática respecto de los elementos que podrían constituir la responsabilidad por el indebido tratamiento de datos personales. Para ello se empleó la revisión de fuentes oficiales y acudí a la comparación teórica y práctica que permite obtener resultados referentes a cómo se puede garantizar el principio de autonomía informativa.

Para lograr esto, en primer lugar, hice un recuento de las principales disposiciones que rigen en el ordenamiento jurídico colombiano en materia de tratamiento de datos personales, contrastándolas con las directrices que, por ejemplo, ha emitido el European Data Protection Board sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de la COVID-19, teniendo presente que se entiende por este dato aquel relacionado con el estado físico y psicológico, pasado, presente o futuro, de la persona natural. El objetivo de esta primera parte fue conocer las

1 Decreto 417 del 17 de marzo de 2020.

2 Según los datos presentados por el Área Metropolitana del Vallé de Aburrá, solo para la ciudad de Medellín se han reportado al 25 de febrero de 2021 ciento noventa y dos mil quinientos ochenta y un (192.581) casos confirmados, con un porcentaje de ocupación de las Unidades de Cuidados Intensivos de hasta el 92%. https://www.medellin.gov.co/irj/portal/medellin?NavigationTarget=navurl://48b007fc8d7912ef960824275ea1cb7a.

disposiciones legales y constitucionales que son aplicables en el ordenamiento jurídico colombiano.

En segundo lugar, abordé de qué forma se ha entendido que las autoridades pueden tener acceso a estos datos y los conflictos jurídicos que en materia de protección de derechos fundamentales suscita dicho entendimiento. Para ello revisé el caso de *Medellín me Cuida*, con el objetivo de presentar la confrontación entre los principios de autodeterminación informativa y satisfacción del interés general, en los casos de tratamiento de datos personales por parte de las autoridades.

En tercer lugar, hice un análisis desde el bioderecho que permite argumentar en favor de una protección reforzada de los datos relativos a la salud de las personas, que implica, al mismo tiempo, establecer criterios de limitación de las facultades de acceso y circulación de las autoridades aún en situaciones de emergencia sanitaria. El objetivo de esto fue abordar los presupuestos teóricos que el bioderecho y la bioética han construido en el tratamiento de los datos relacionados con el estado de la salud.

Finalmente, idagué por la manera como pueden articularse los aspectos dogmáticos y biojurídicos, para la estructuración de los elementos de la responsabilidad del Estado por el uso indebido de los datos relacionados con el estado de salud en situaciones de pandemia, con el propósito de cumplir con el objetivo central de la investigación.

RESULTADOS Y DISCUSIÓN

El tratamiento de los datos personales: regulación y sanciones en situación de normalidad

En el ordenamiento jurídico colombiano la Ley 1581 de 2012 desarrolla el derecho fundamental de *habeas data*. En esta ley estatutaria se estableció una distinción entre el *dato personal* y el *dato sensible*. Por el primero, según se estipula en el artículo 3, se entiende la información que pueda estar vinculada con una o varias personas naturales. El segundo es definido en el artículo 5 como aquella información que afecta el derecho a la intimidad de la persona y cuyo indebido tratamiento puede generar discriminación; en esta última clasificación se incluyen los datos relativos a la salud.

En el artículo 4 se señalan ocho principios para el tratamiento de los datos personales, a saber: i) legalidad; ii) finalidad; iii) libertad; iv) veracidad o calidad; v) transparencia; vi) acceso y circulación restringida; vii) seguridad, y viii) confidencialidad. Estos principios son relevantes no solo porque contienen las condiciones fundamentales para el almacenamiento, uso y circulación de los datos personales, sino porque en el ordenamiento jurídico tienen una función interpretativa limitativa, ya que en los casos en los que el derecho fundamental de *habeas data* debe ceder ante otro derecho fundamental o ante el interés general, restringen de manera definitiva las posibilidades del tratamiento y amplían las responsabilidades de quien legitimamente puede usar los datos personales, tal como lo veremos en el caso de *Medellín me cuida*.

En el orden jurídico colombiano la autorización previa e informada es un requisito indispensable para el tratamiento de datos personales. Contrario al criterio que permite el uso —en cualquiera de sus formas— de los datos personales, para el tratamiento de los datos sensibles se fijó una prohibición general, salvo que el titular dé su autorización explícita. Como puede observarse en el primer caso, la autorización es un requisito que legitima la posibilidad de tratar datos personales, en tanto en el caso de los datos sensibles dicha autorización es la condición de habilitación de una excepción legal.

En el artículo 10 de la Ley 1581 de 2012, se dispuso que, entre otros casos, no es necesaria la autorización del titular de los daros cuando se trate de: i) información requerida por las autoridades para el cumplimiento de sus funciones legales o constitucionales o por orden judicial y ii) en los casos de urgencia sanitaria o médica.

La Corte Constitucional, retomando lo considerado en la Sentencia C-1011 de 2008, señaló en la Sentencia C-748 de 2011, que es legítimo el tratamiento de datos personales por parte de las autoridades sin que los titulares den su autorización, cuando en la solicitud de información se indique expresamente en cuál de las funciones legales o constitucionales está amparada la solicitud. Ahora, agrega la Corte que, si bien de acuerdo con lo establecido en el la ley estatutaria es posible el acceso de las autoridades a los datos personales, esto no implica que están exentas de cumplir con los demás criterios previstos en el orden interno; en consecuencia, las

autoridades están obligadas a (i) guardar reserva y usar exclusivamente la información para los fines indicados en la solicitud; (ii) informar el uso que le está dando a tales datos personales; (iii) conservar la información con los parámetros estrictos de seguridad, y (iv) cumplir con las instrucciones que sobre la materia imparta la autoridad de control, en el caso colombiano la Superintendencia de Industria y Comercio (SIC).

En las situaciones de urgencia (médica o sanitaria) la Corte Constitucional, en la sentencia antes referida, consideró que esta excepción no contiene una autorización general e ilimitada; por el contrario, solo podrán tratarse los datos personales sin la autorización respectiva cuando el titular no esté en condiciones de otorgarla o "resulte particularmente problemático gestionarla, dadas las circunstancias de apremio, riesgo o peligro para otros derechos fundamentales, ya sea del titular o de terceras personas".

Como puede observarse, si bien el tratamiento de los datos sensibles está prohibido por regla general, con la excepción a dicha prohibición materialmente no parece haber una distinción sustancial respecto de las exigencias legales para el tratamiento de los datos personales. Esto, en la medida en que en ambos casos es suficiente con la autorización del titular o que estemos en frente de alguna de las excepciones contenidas en el artículo 10 de la Ley 1581, en las cuales también —sin un mayor análisis— se ha entendido que están incluidos los datos sensibles.

Con base en lo anterior, en lo que podríamos llamar *tiempos de normalidad*, el tratamiento de los datos personales y, concretamente, de los datos sensibles relativos al estado de salud de las personas exige la autorización o consentimiento previo del titular. Este requisito es necesario tanto en los escenarios médicos como en aquellos en los que no se lleva a cabo un procedimiento médico. Por su parte, en lo referente al recaudo, uso y circulación de los datos personales por parte de las autoridades estatales, que son requeridos para el cumplimiento de las funciones sanitarias, en principio, la excepción al requisito de la autorización está dada en virtud de las funciones que ejerce la autoridad y no como consecuencia de la imposibilidad del titular de otorgar dicha autorización.

Con base en lo previamente enunciado, con el propósito de verificar qué tan efectivas son las condiciones previstas en la Ley 1581 respecto de otros sistemas normativos, pasaré a revisar las condiciones contenidas en el Reglamento General de Protección de Datos (RGDP), expedido por el Parlamento Europeo y el Consejo.

En dicho reglamento se prevé que son principios los siguientes: i) los datos personales deben ser tratados de forma lícita, leal y transparente, ii) los datos personales deben ser recogidos con fines determinados explícitos y legítimos (limitación de la finalidad [inicial]), iii) los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con el tratamiento, iv) los datos personales deben ser exactos y estar siempre actualizados; v) el tratamiento de los datos personales es limitado en el tiempo, por lo que no se conservarán sino por el periodo que es necesario de acuerdo con su finalidad, y vi) el tratamiento de los datos debe hacerse de manera segura.

El RGDP regula explícitamente el derecho al olvido al establecer las circunstancias que permiten a cualquier interesado solicitar la supresión de sus datos personales. Asimismo, la reglamentación delimita las situaciones en las que la elaboración de perfiles (*Data profiling*) es permitida e impone la obligación de designar delegados de protección de datos en tres casos: i) cuando los datos sean tratados por las autoridades, ii) cuando el tratamiento sea hecho por personas que tengan por objeto tratar datos personales, y iii) cuando las actividades de los tratantes "consistan en el tratamiento a gran escala de categorías especiales de datos".

El RGDP también establece la *responsabilidad proactiva*, mediante la cual se impone el deber, al tratante de los datos personales, de aplicar todas las medidas que sean necesarias para garantizar y probar el tratamiento del dato que se está haciendo conforme con lo señalado en el reglamento general. Para ello, las organizaciones analizan qué tipo de datos tratan, con qué finalidad lo hacen y cuáles son los pasos para tener en cuenta para que sus políticas sean acordes con la normativa.

Tal como lo señala Carlos Romeo Casabona (2019), en el RGPD se ha dado prelación al interés social frente al derecho individual, justificado en el hecho de que el tratamiento de los datos de salud en el ámbito médico contribuye al bienestar de la colectividad. Pero, respecto al tratamiento masivo de datos se mantienen ciertos límites importantes para asegurar la efectividad del derecho. Esta situación implica la

necesidad de un enfoque diferenciado para delimitar el alcance del tratamiento de los datos de la salud en diversos escenarios.

De las reglas aplicables a los Estados que conforman la Unión Europea puede inferirse —en una comparación simple de sus contenidos— que las disposiciones del ordenamiento jurídico colombiano no distan sustancialmente de lo previsto en el RGDP, aunque en este último hay tres elementos distintivos que aseguran en un mayor grado la protección de los derechos de los titulares, en la medida en que aun en los casos de tratamiento de datos por parte de las autoridades existe el deber explícito de designar delegados cuya función es garantizar el cumplimiento de los parámetros fijados en el reglamento.

Esta exigencia permite concluir de una manera clara que las autoridades, aun cuando actúan en virtud de las excepciones al reglamento, solo están exentas de solicitar la autorización para el tratamiento de los datos personales, pero las demás exigencias deben cumplirlas cabalmente, so pena de incurrir en las sanciones a que haya lugar.

Las disposiciones expedidas durante la Declaratoria de Emergencia Económica y Social

En el ordenamiento jurídico colombiano se expidieron algunas disposiciones en las que se fijaron las reglas para el tratamiento de los datos personales recaudados con la finalidad de mitigar o controlar la propagación de la enfermedad causada por la COVID-19. Sobre el asunto, se expidieron dos disposiciones: i) el artículo 8 del Decreto 538 de 2020, mediante el cual se flexibilizó el principio de seguridad previsto en la Ley 1581 de 2012, para permitir el uso de plataformas tecnológicas para las actividades de telesalud. Esta flexibilización estuvo justificada en la protección de principios y derechos de mayor valor constitucional, como la vida y la salud de las personas.

De igual forma, en el parágrafo segundo del citado artículo 8 se señala:

> *los pacientes podrán enviar la imagen del documento firmado en el que manifiesten el consentimiento informado. Cuando esto no sea posible, el profesional tratante dejará constancia en la historia clínica de la situación, de la información brindada sobre el alcance de la atención y de la aceptación del acto asistencial por parte del paciente, de forma libre, voluntaria y consiente*.

Por su parte, la SIC, en calidad de autoridad en materia de protección de los datos personales, emitió la Circular Externa 01 del 23 de marzo de 2020, dirigida a los operadores de telefonía móvil y a la Asociación de la Industria Móvil de Colombia, mediante la cual autorizó a estas empresas para suministrar a las entidades públicas y al Departamento Administrativo de Planeación "los datos personales necesarios" para controlar la propagación de la enfermedad generada por la covid-19.

Entre otras circulares, la SIC emitió la Circular Externa 008 de 2020 el 18 de agosto de 2020, en la que indicó que, en la aplicación de los protocolos de bioseguridad en el momento de la reactivación económica, los responsables y encargados del tratamiento de los datos personales deben tener en cuenta, entre otros aspectos, los siguientes:

1. Los actos administrativos expedidos por el Ministerio de Salud y Protección Social, en los que se definen los protocolos de bioseguridad, no suspenden el derecho fundamental a la protección de datos personales; en consecuencia, el régimen de protección sigue vigente y es de obligatorio cumplimiento para los tratantes de los datos personales.
1. En la aplicación de los protocolos de bioseguridad solo se pueden recolectar los datos que expresamente señala el Ministerio de Salud y Protección Social que sean "pertinentes y adecuados para la finalidad para la cual son requeridos", de ahí que los responsables y encargados del tratamiento deban estar en capacidad de justificar o explicar la necesidad de recolectar los datos que solicitan a las personas, es decir, de dar cuenta de cuál es la finalidad.
1. Los datos recolectados para dar cumplimiento a los protocolos de bioseguridad solo se podrán almacenar durante el tiempo razonable y necesario para cumplir dichos protocolos. Una vez cumplida la finalidad, el tratante debe suprimir los datos recolectados sin que sus respectivos titulares efectúen alguna solicitud expresa.
1. Para el caso de los datos de salud, su recolección, uso, circulación y tratamiento "debe estar rodeado de especial cuidado y diligencia en su recolección, uso, seguridad o cualquier otra actividad

que se realice con estos. Es de notar que ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles".

De lo previamente indicado, encontramos que en el marco de una emergencia sanitaria no hay una suspensión de las condiciones que permitan asegurar la legalidad del tratamiento de los datos personales y, contrario al entendimiento que sobre el asunto se tuvo, la situación de emergencia impone unos deberes a los responsables y encargados del tratamiento de los datos, cuyo cumplimiento está orientado a que los datos recaudados tengan un uso limitado y exclusivamente relacionado con la atención de la emergencia.

Las directrices impartidas por la SIC están dirigidas a todas las personas que tengan la calidad de responsables o encargados del tratamiento de datos personales, con lo cual no hay duda de que todas las personas, naturales y jurídicas, que deban recaudar datos de salud de otras personas en cumplimiento de los protocolos de bioseguridad, no podrán usar esa información ni los demás datos personales para el desarrollo de las actividades comerciales propias de su objeto social o para el cumplimiento de funciones sanitarias a cargo de las autoridades públicas.

Ahora, teniendo en cuenta lo considerado por la Corte Constitucional en la Sentencia C-748 de 2011, las entidades públicas cuando recaudan, usan o circulan datos personales adquieren la calidad de "responsables", aun en los casos en los que dicho tratamiento se haga en virtud de las excepciones previstas en el artículo 10 de la Ley 1581 de 2012. Esto implica que, de igual manera, los criterios restrictivos de circulación, almacenamiento temporal, suficiencia y concreción en la finalidad también le son aplicables a estas entidades, en la medida de que lo único que se exceptúa es la consecución de la autorización del titular de los datos.

Una aplicación para el uso de datos relativos a la salud

Para mostrar el alcance de las consecuencias jurídicas de lo que se ha presentado previamente, es pertinente revisar el caso de la plataforma Medellín me Cuida, mediante la cual el municipio de Medellín, en calidad de autoridad sanitaria y en cumplimiento de las funciones relacionadas con la prevención y mitigación de la propagación del COVID-19, recaudó y trató datos sensibles (relativos al estado de salud de las personas) y datos personales.

El municipio de Medellín en su página web dispuso dos aplicativos: i) Medellín me Cuida –empresas y ii) Medellín me Cuida – familias. A través de la primera, las empresas debían registrar los datos de sus trabajadores y la información sobre el estado de salud que cada uno de ellos reportaba diariamente. Mediante la segunda, los ciudadanos estaban obligados a registrarse si deseaban movilizarse a sus sitios de trabajo, siempre y cuando estuvieran dentro de las excepciones previstas en el artículo 3 del Decreto 457 de 2021, emitido en el marco de la declaratoria de emergencia económica, social y ecológica.

También se les indicó a todos los servidores públicos de la administración, en sector central y descentralizado, que debían registrarse en Medellín me Cuida – familias. Finalmente, el municipio solicitó a las empresas prestadoras de servicios públicos domiciliarios la base de datos de sus usuarios, en la que se pidió, amparado en lo previsto en el literal a) de la Ley 1581 de 2012 —cumplimiento de función de autoridad administrativa—, el número del contrato de servicios públicos domiciliarios, el número de la instalación y la dirección de residencia del titular de los servicios.

En este contexto, una ciudadana interpuso acción de tutela en contra del Municipio de Medellín, y de acuerdo con los hechos narrados en el escrito su empleador le señaló que por orden de la autoridad municipal era obligatorio registrarse en la plataforma Medellín me Cuida y de no hacerlo no podría reanudar sus labores en el sector productivo y podría ser sancionada por las autoridades policivas.

La accionante señaló que al ingresar a la plataforma se encontró con que le solicitaban el número de teléfono, la profesión y la dirección, además de que al "revisar la política de tratamiento de datos", se le informa que los mismos serán tratados conforme con la finalidad prevista en el Decreto 1096 de 2018, expedido por el Alcalde de Medellín, situación a partir de la cual considera que, además de que se le está solicitando información adicional a la requerida, no tiene la opción de limitar el tratamiento de sus datos personales, lo que significa que de no dar la autorización la aplicación no permite completar el registro.

El Juzgado 45 Penal Municipal con Funciones de Control de Garantías amparó los derechos a la intimidad, *habeas data* y al trabajo, argumentando

que no era clara la finalidad con base en la cual el municipio de Medellín solicitaba el suministro de los datos personales. Así mismo, ordenó a la entidad territorial que permitiera a la ciudadana el registro en la base de datos de Medellín me Cuida-Personas suministrando únicamente los datos de identificación personal y laboral necesarios, así como aquellos que atañen a su condición médica, pues estos guardan relación directa con la finalidad legítima de este ente municipal tendiente a mitigar el contagio general.

La entidad territorial apeló el fallo de primera instancia y en la sustentación del recurso argumentó que la información solicitada tenía por finalidad caracterizar a las personas que comenzaran a laborar a partir del día 27 de abril y evitar que las personas que no estaban exentas del aislamiento obligatorio lo incumplieran, para impedir la propagación de la COVID-19. También agregó que es cierto que los datos suministrados por los ciudadanos serán tratados conforme con lo ordenado en la Ley 1581 de 2012, sus decretos reglamentarios y el Decreto 1096 de 2018, sin que sea cierto que los datos suministrados sean públicos, de conformidad con señalado en el numeral 60 de los términos y condiciones de uso de la plataforma.

El fallo dictado por el Juzgado Quinto Penal del Circuito de Medellín revocó la decisión proferida por la primera instancia, bajo la consideración de que el derecho de *habeas data* se encuentra garantizado por la Alcaldía de Medellín al establecer que la dirección física en el marco de la emergencia ocasionada por el coronavirus tiene como finalidad realizar los cercos epidemiológicos correspondientes, en el entorno residencial y laboral. En cuanto al dato del celular, la segunda instancia consideró que también era necesario, dado que su finalidad radica en la posibilidad de ponerse en contado con la accionada de la forma más expedita para alertarle en caso de que se encuentre en riesgo de contagio, conforme con el cerco epidemiológico.

Finalmente, respecto del dato relativo a la profesión o actividad de la accionante, consideró el juez de tutela que se trata de un dato público de carácter voluntario, cuya la finalidad no es otra que determinar si la persona que se registra en la plataforma conforme al ejercicio de su actividad productiva tiene mayor riesgo de ser contagiado con el virus o de contagiar a otras personas en el ejercicio de su actividad, en el evento de ser portadora. Por último, se precisa que el único dato sensible solicitado era el del estado de salud, pero que como la ciudadana no diligenció el formulario, no puede predicarse que hubo alguna vulneración del derecho al *habeas data* o a la intimidad.

Las cuestiones que en el caso de la plataforma de Medellín me Cuida resultan importantes para el eventual establecimiento de la responsabilidad extracontractual del Estado por el uso indebido de datos personales y sensibles relativos a la salud durante la pandemia son las siguientes:

En primer lugar, el municipio de Medellín, conforme con las disposiciones legales y las expedidas por el Gobierno Nacional en el marco de la declaratoria del estado de emergencia económica social y ecológica y la declaratoria de emergencia sanitaria tienen funciones relacionadas con la prevención y mitigación de la enfermedad ocasionada por la covid-19.

Con base en esto, puede entenderse que el tratamiento de datos personales (dentro de los cuales están los datos relativos a la salud) debe hacerse con sujeción a los criterios definidos por la Corte Constitucional en la sentencia que declaró la exequibilidad de las excepciones contenidas en el artículo 10 de la Ley 1581. Esto significa que las autoridades tienen los deberes de reserva de la información, uso restringido, información al titular, seguridad y cumplimiento con las instrucciones que imparta la autoridad de control.

En segundo lugar, la finalidad informada por el municipio de Medellín para el tratamiento de los datos personales solicitados fue la contenida en el Decreto 1096 de 2018, expedido por el Alcalde. Según lo señalado en el numeral ii del anexo de dicho decreto se indica que los datos suministrados por los titulares serán incluidos en las bases de datos de la entidad territorial "para llevar a cabo acciones relacionadas con sus funciones legales y su objeto misional, lo que comprende todas sus competencias funcionales", acudiendo con esto a la excepción referente al ejercicio de funciones legales y constitucionales por parte de las autoridades. La aplicación de lo previsto en el Decreto 1096 de 2018 implica que en ninguna de las actividades a cargo del municipio se requiere la autorización de titular de los datos personales.

Como puede observarse, la finalidad informada a los titulares de los datos personales es la que la administración emplea en las situaciones de normalidad

que, en conclusión, permite su tratamiento general sin que se requiera la autorización del titular. Sin embargo, tratándose de la protección de un derecho fundamental, es importante tener en cuenta que era necesario que se indicara de manera expresa y clara que la finalidad era caracterizar a las personas que comenzarían a laborar a partir del día 27 de abril de 2020 para evitar así la propagación de la COVID-19.

De igual forma, es necesario que en estos casos el tratamiento de los datos personales esté limitado solo a la función sanitaria y de prevención a cargo de la autoridad territorial, en la medida en que la función que está ejerciendo la administración es precisamente la prevista en la artículo 44 de la Ley 715 de 2001, relacionada con la vigilancia y el control sanitario en la jurisdicción, respecto de los factores de riesgo para la salud; esto, en concordancia con lo señalado en el artículo 2. 8. 8. 1. 1. 10. del Decreto 780 de 2016.

No son pues legítimas las razones que da el municipio de Medellín en la apelación del fallo de primera instancia proferido por el Juzgado 45 Penal Municipal con Funciones de Control de Garantías, ya que la remisión al Decreto 1096 de 2018 no permite cumplir con el deber de informar una finalidad concreta y deja abierto el tratamiento de datos personales, incluso para su circulación entre las entidades públicas, sin que se garanticen los criterios de seguridad, circulación restringida y temporalidad.

Otro elemento que resulta llamativo es que se le indicó al ciudadano que dar su consentimiento era obligatorio, esto ocurrió: i) a través de la información que se les dio a los empleadores y el deber que se les impuso a estos de registrar a sus empleados en Medellín me Cuidad – empresas, y ii) no permitiendo que la persona natural quedara registrada en la plataforma si no consentía en el tratamiento de los datos personales. La obligatoriedad de aceptar las condiciones para el tratamiento de los datos personales permite hacer un interrogante básico: si no se requería la autorización porque se estaba actuando en calidad de autoridad administrativa, ¿por qué era obligatorio la aceptación que remite al Decreto 1096 de 2018?

La respuesta al anterior interrogante sugiere que la entidad territorial no estaba actuando en virtud de las excepciones contenidas en los literales a) y c) del artículo 10 la Ley 1581 y por ello sí era necesaria la autorización o que hubo un vicio en el consentimiento de quienes dieron la autorización, porque creyeron que la misma era necesaria para transitar y evitar ser sancionados por las autoridades de policía. Esto es, no cabe considerar que existe libre consentimiento cuando hay un desequilibrio de poder entre el titular y el responsable del tratamiento del dato personal, desequilibrio originado en la falsa información dada por la propia administración.

Ahora, teniendo presente que en estos casos efectivamente no se requería la autorización del titular de los datos personales, cuando se solicita esa autorización por medio del uso de información no cierta también puede concluirse que se produce el desequilibrio de poder, en la medida en que con este se viola directamente el principio de autodeterminación informativa, según el cual, es deber de las autoridades informar las condiciones bajo las cuales sus datos serán tratados para que este pueda decidir si los suministra o ejercer un control respecto del responsable de sus datos.

Lo que se quiere destacar es, entonces, que no hubo coherencia ni claridad en el manejo de la excepción contemplada en el literal a) del artículo 10 de la Ley 1581 de 2012, además de que no se cumplieron los presupuestos señalados por la Corte Constitucional, relativos a informar a los titulares el uso que se le está dando a sus datos y cumplir con las instrucciones que imparta la autoridad de control.

También en el manejo que el municipio de Medellín dio a la información recaudada durante el estado de emergencia económica y el estado de emergencia sanitaria se observa que al informar la finalidad que normalmente emplea en el cumplimiento de sus funciones, no hay un uso exclusivo para los *"fines que justificaron la entrega"*, esto es, la finalidad informada no es, como lo concluye la segunda instancia del fallo de tutela, establecer los cercos epidemiológicos correspondientes en el entorno residencial y laboral, y adelantar acciones de prevención de la enfermedad, ya que lo que expresamente se les está diciendo a los usuarios es que los datos podrían usarse para, por ejemplo, la liquidación de impuestos y cualquier otra de las funciones de las entidades territoriales.

En ese sentido, se advierte la necesidad de que, por tratarse de una excepción a la necesidad del consentimiento —mas no de las otras condiciones para el tratamiento de los datos personales— las autoridades estatales deben diseñar finalidades

que sean conformes con cada una de las funciones que legalmente tienen a cargo y no tener una finalidad tan amplia que, en última instancia, permita el tratamiento de los datos personales de manera indistinta y general.

En tercer lugar, en el ejercicio de las funciones legales y administrativas, el municipio de Medellín obtuvo información no solo de los ciudadanos que se registraron en la plataforma Medellín me Cuida, sino de otras entidades públicas y privadas, tales como de los prestadores de servicios públicos domiciliarios y de los empleadores de todos los sectores económicos de la ciudad.

La actividad de contraste de la información obtenida por diferentes medios es relevante en la medida en que el municipio de Medellín no solo tiene la calidad de responsable, sino también de encargado del tratamiento de los datos personales, por lo que la entidad territorial debe cumplir con los deberes contenidos en los artículos 17 y 18 de la Ley 1581 de 2012.

En cuarto lugar, la excepción prevista en el literal c) del artículo 10 de la Ley 1581, relativa a que no se requiere la autorización del titular en los casos de emergencia médica o sanitaria está justificada en el hecho de que no sea posible obtener del titular la autorización, bien sea porque su estado de salud no se lo permite o porque ante la emergencia sanitaria hay un riesgo inminente que hace necesaria la intervención urgente del tratante de los datos personales.

El alcance antes referido permite advertir que si bien para ese momento se estaba ante una pandemia originada en un virus que era desconocido para el estado de la ciencia y que por ello no era fácil determinar cuáles eran los procedimientos que debían seguirse en el caso concreto, esto no impedía que debía obtenerse la respectiva autorización cuando el titular estaba en capacidad de dar su consentimiento o que por el tipo de emergencia sanitaria el riesgo no sea inminente.

Por lo anterior no puede concluirse que la emergencia sanitaria fuera suficiente por sí sola para que las autoridades prescindieran de la necesidad de obtener el consentimiento, porque exigía probar que el riesgo era inminente y por ello necesario el tratamiento de los datos personales sin la autorización. En estos eventos, la finalidad del recaudo, uso y circulación de los datos personales está exclusivamente relacionada con la salvaguarda de un derecho fundamental superior o del interés general, por lo que tampoco se considera que es legítima la finalidad informada por el municipio de Medellín, relativa al cumplimiento de sus funciones legales ordinarias.

Análisis biojurídico: autonomía y consentimiento informado

En el libro *Principles of biomedical ethics* de Beauchamp y Childress (2013), cuya primera edición apareció en 1979 y probablemente el libro de bioética más influyente del mundo, los autores ofrecen un marco deliberativo a partir de la articulación de cuatro principios: i) respeto por la autonomía, ii) no maleficencia, iii) beneficencia y iv) justicia.

Para Beauchamp y Childress (2013) la autonomía en la bioética es entendida como un mandato de moralidad común, cuyo contenido está relacionado con el respeto y la protección de las personas a través de posibilitarles vivir de acuerdo con los puntos de vista basados en sus creencias, visiones y valores particulares.

La autonomía es el principio con base en el cual se protege la libre elección de los sujetos de acuerdo con sus gustos y preferencias. Bajo este entendimiento, para que una persona actúe de manera autónoma, tal como lo señalan Ruth R. Faden & Tom L. Beauchamp (1986), se deben cumplir ciertas condiciones estructurales y de procedimiento. Un agente autónomo es el que tiene la capacidad de actuar de manera racional y al mismo tiempo actuar: i) informado, ii) entendiendo la información, iii) intencionalmente, iv) voluntariamente, v) conscientemente, vi) sin coerción externa y vii) con el derecho de ser subrogado en su decisión en caso de que su autonomía se vea disminuida o perdida.

Así mismo, los autores en estudio añaden que el principio de autonomía contiene dos tipos de obligaciones: una positiva y otra negativa. La positiva significa respetar el derecho que otros tienen de tomar decisiones autónomas, y las órdenes negativas de no interferir, limitar o restringir de ninguna manera las acciones y decisiones de otros.

Sin embargo, estas obligaciones no solo implican permitir o no interferir, ya que, por ejemplo, en el campo clínico o biomédico respetar la autonomía significa que tanto el médico como el científico deben

informar sobre las condiciones del procedimiento al paciente o al sujeto de la experimentación antes de aplicarlo. Del mismo modo, deben asegurarse de que los sujetos/pacientes hayan entendido sustancialmente la información, así como no ejercer ninguna presión para la toma de decisiones. Finalmente, deben garantizar la intencionalidad y la voluntariedad de las personas, así como asegurar que no exista coerción externa que los obligue a decidir o ir en contra de su voluntad.

Las anteriores consideraciones teóricas permiten señalar que tanto las condiciones estructurales y de procedimiento del principio de autonomía, como las obligaciones positivas y negativas que se desprenden de ella, dan paso a la privacidad o a lo que podemos caracterizar en términos de Adinolfi (2007) como la consideración del principio de autodeterminación informativa, con base en la cual puede garantizarse el derecho de *habeas data* y de datos personales. Es decir, este principio se consolida en términos de la tutela efectiva de la personalidad.

El principio de autodeterminación informativa, tal como lo reseña la doctrina italiana, tiene su origen en la separación que en Alemania se hace de este respecto del derecho a la vida privada desarrollado en Estados Unidos. Sus elementos centrales son i) la posibilidad de reconocer la reparación aun en los casos en los que el daño es inmaterial y ii) la autonomía del consentimiento, que permite autorizar, bloquear, oponerse, ratificar, rectificar información acerca de la persona (Adinolfi, 2007, p. 7). La protección de este principio y de los derechos que de este se desprenden (datos personales) se efectúa mediante la tutela de la personalidad.

En igual sentido, desde el punto de vista la filosofía de la responsabilidad extracontractual, el reconocimiento de perjuicios por daño a derechos fundamentales tuvo su origen en el reconocimiento del derecho a la intimidad y a la privacidad. Tal como lo señala George C. Christie (2013), solo hasta el momento que se reconoció el daño por invasión a la intimidad, fue cuando se hizo evidente la necesidad de proteger la tranquilidad emocional de los seres humanos, que genera grandes conflictos con otros derechos, caso en el cual es necesario evaluar si el derecho a la intimidad alcanza primacía presuntiva, respecto del otro derecho en conflicto. En este escenario, en materia de tratamiento de datos sensibles son dos los principios fundamentales que deben tenerse en cuenta: i) la intimidad y privacidad personal y ii) la autodeterminación informativa.

Para el caso del *habeas data*, conforme con la estipulación legal, este derecho fundamental está inescindiblemente relacionado con el derecho a conocer, actualizar y rectificar la información que terceros traten mediante los diferentes bancos de datos, lo que incluye tanto a las entidades públicas como privadas. Tomando en cuenta tal relación, ¿qué se está dañando cuando hay un uso indebido en el tratamiento de los datos sensibles relativos a la salud? La respuesta es simple: el principio de autodeterminación informativa y la intimidad y privacidad personal.

Ahora, la configuración del principio de autonomía ha sido criticada muchas veces; sin embargo, Beauchamp y Childress (2013) intentan demostrar que en una teoría deliberativa debidamente estructurada, el respeto por la autonomía no puede ser excesivamente individualista que lleve a descuidar la naturaleza social de los seres humanos y el impacto de las decisiones y elecciones individuales en los demás. Tampoco debe estar excesivamente centrado en la razón, prescindiendo de las emociones y, finalmente, dicha teoría no puede ser exorbitantemente legalista o jurídica, hasta el punto de otorgar preeminencia a los derechos sobre las prácticas y responsabilidades sociales.

Con base en la respuesta a tales críticas es posible, para el caso concreto de la propagación de la COVID-19, hacer un balance entre la decisión individual de no informar el estado de salud a las autoridades, con las consecuencias que ello puede traer para los demás, y la satisfacción de un interés general a cargo del Estado, que le permite a este acceder a tales datos sin que sea necesario el consentimiento del titular.

Este balance sugiere dejar de lado el individualismo absoluto y la omisión en el control de las funciones estatales. En otras palabras, si bien el Estado puede tratar los datos del estado de salud en una situación de emergencia sanitaria sin que el titular consienta en ello, eso no implica que el uso sea irrestricto o ilimitado solo por el hecho de que el tratante es una autoridad.

Es condición para garantizar la legalidad y legitimidad del tratamiento que la autoridad informe de manera clara y contundente cuál es la finalidad del

tratamiento y que, tal como funciona en la comunidad europea, haya un control en la función de salubridad que permita garantizar el cumplimiento de los parámetros fijados en el orden interno. Así, por ejemplo, la circulación de datos personales entre entidades públicas debe restringirse, ya que no es por la calidad de los sujetos que se permite tal circulación, sino por la función pública que ejerce en relación con la prevención de la propagación de la enfermedad.

De otro lado, del principio de autonomía se desprende, entonces, la necesidad de que en situaciones médicas el paciente sea informado de todas las condiciones que incidan en su salud. Pero no es suficiente con que este requisito se cumpla de manera informal, ya que el paciente debe dar su consentimiento informado, sumada al nacimiento de la obligación del médico de guardar secreto profesional.

Tratándose de tratamiento de datos relativos a la salud por fuera del escenario médico, por ejemplo, en los casos de emergencia sanitaria o en ejercicio de las funciones asignadas legalmente a las autoridades, es importante tener en cuenta que por tratarse de datos sensibles su tratamiento debe hacerse con mayores exigencias. Para fundamentar esta idea es relevante tener en cuenta lo afirmado por Carlos Romeo Casabona (2019), respecto de las implicaciones del uso masivo de estos datos, según quien su tratamiento para algún perfilamiento y determinación de protocolos generales afecta las decisiones que cada uno puede tomar respecto de su dato de salud; concretamente, afecta su derecho a consentir de manera informada sobre las múltiples decisiones que se pueden tomar a partir de la obtención de sus datos.

Ahora, sin perder de vista que en la situación de emergencia sanitaria ocasionada por la COVID-19 lo que se trata —de manera principal— son los datos relativos a la salud, lo que corresponde es procurar la obtención de la autorización del tratamiento de datos sensibles y no ampararse en el ejercicio de la función estatal como una forma de eludir este deber. Es importante tener presente que dicha autorización para el caso específico de los datos relativos a la salud debe darse a partir de las consideraciones establecidas por lo que canónicamente se ha entendido por consentimiento informado. Esto, en la medida en que el consentimiento informado es la materialización del principio de autonomía. Por el contrario, cuando no se asegura que el consentimiento del interesado sea dado en forma libre, sin condiciones que coaccionen la libertad de decisión del sujeto necesariamente debe haber consecuencias jurídicas por el indebido tratamiento, tal como lo prevé Romeo Casabona (2019).

Articulación de los aspectos dogmáticos y biojurídicos en la estructuración de los elementos de la responsabilidad del Estado por el uso indebido de los datos relacionados con el estado de salud para el control de la pandemia originada en la COVID-19

Para la estructuración de los elementos de la responsabilidad extracontractual del Estado, teniendo en cuenta los parámetros legales fijados en la Ley 1581 de 2012 y atendiendo a los criterios ofrecidos por el bioderecho, es importante tener presente que cuando no hay claridad respecto de la finalidad del tratamiento de los datos personales y, por el contrario, hay un entendimiento ampliado del alcance de las excepciones a la necesidad del consentimiento que, en el caso de datos relativos a la salud, debe ser cualificado (informado), hay lugar a la atribución de responsabilidad de las autoridades. Por ello, en el presente acápite lo que intentaremos mostrar es cuál es la vía para su estructuración.

Lo primero es decantar la discusión acerca de la responsabilidad objetiva derivada del uso de la tecnología y la responsabilidad por falla en el servicio, tal como lo propone Daniel Peña Valenzuela (2015). En el primer caso, se acude a la prevalencia de los criterios de riesgo permitido, creación de riesgos, aumento de riesgos, principio de confianza y posición de garante con las que se busca el control en el cumplimiento de los estándares de gestión, que se constituyen en los límites de riesgo permitido de las actividades estatales.

En relación con el riesgo permitido, autores como Yesid Reyes (2005) señalan que se entiende por este:

> aquel riesgo que permanece aun con el cumplimiento de las normas de cuidado que deben acompañar la ejecución de toda actividad peligrosa socialmente admitida. Así son requisitos para su configuración, que la actividad resulte beneficiosa frente al riesgo de peligrosidad y que haya "indeterminación de las potenciales víctimas de ese riesgo residual" (p. 95).

En ese sentido, el reproche jurídico que en estos casos se efectúa por el desarrollo de actividades prohibidas o por la ejecución de actividades permitidas sin la observancia de las normas de cuidado previamente establecidas para la minimización del riesgo.

Por su parte, la falla en el servicio ha sido entendida como el incumplimiento de una obligación a cargo del Estado. Este tipo de responsabilidad, a diferencia del derivado del riesgo permitido, constituye un tipo subjetivo, en la medida en que es la actuación irregular de la administración la que, en la mayoría de los casos, genera perjuicios indemnizables a los particulares. Esta responsabilidad tiene su origen en el derecho administrativo francés, que en el ordenamiento jurídico colombiano no se ha alejado de la concepción francesa, ya que uno de los criterios determinantes es la irregularidad o anormalidad en la actuación de las entidades estatales, además del retardo, la ineficiencia o la omisión o ausencia del servicio; todos estos supuestos hacen parte de la responsabilidad por falla del servicio.

Para el caso del tratamiento de los datos personales por parte de las autoridades estatales, encontramos que dicho tratamiento no constituye una actividad que pueda considerarse por sí sola riesgosa, ni siquiera en situación de pandemia. En esa medida, entendemos que lo que se pretendió con la expedición de la Ley 1581 de 2012 no fue establecer los límites del riesgo permitido, sino regular el ejercicio de tres derechos fundamentales como el derecho de *habeas data,* el derecho a la intimidad y el derecho de datos personales. Además, respecto del requisito de la indeterminación de las víctimas por el desarrollo de la actividad peligrosa puede afirmarse que tampoco se cumple con tal condición, ya que estos tres derechos están dentro de la categoría de derechos de la personalidad, tal como se argumentó.

Así, tratándose de un derecho fundamental, la protección del derecho de datos personales y de *habeas data* puede hacerse por cualquiera de los mecanismos previstos en el ordenamiento jurídico, bien sea mediante la reclamación que el titular puede hacer a los responsables y encargados del tratamiento, mediante el ejercicio de la acción de tutela o a través de los medios de control que pueden interponerse ante la SIC para que esta ejerza las facultades sancionatorias que le fueron conferidas.

Ahora, ninguno de estos mecanismos puede considerarse como una forma correctiva o de reparación de los daños patrimoniales o extrapatrimoniales que pueda sufrir una persona cuando el Estado no cumple con los deberes relacionados con la seguridad, limitación de la finalidad, circulación restringida y atención de las recomendaciones de la autoridad en materia de protección de datos personales. Es en este escenario en el que es posible atribuir responsabilidad al Estado por falla en el servicio, esto es, cuando en ejercicio de una función estatal, como lo es la prevención de la propagación de la COVID-19, no cumple con los deberes previstos en la Ley 1581.

Para establecer si es posible atribuir responsabilidad al Estado en estos casos, lo primero que debe tenerse en cuenta es que ha habido una mutación jurisprudencial del concepto de daño. Por ejemplo, de acuerdo con la Corte Suprema de Justicia, al estudiar la posibilidad de daños extrapatrimoniales en la responsabilidad contractual, el daño puede ser entendido como

> una modificación de la realidad que consiste en el desmejoramiento o pérdida de las condiciones en las que se hallaba una persona o cosa por la acción de las fuerzas de la naturaleza o del hombre. Pero desde el punto de vista jurídico, significa la vulneración de un interés tutelado por el ordenamiento legal, a consecuencia de una acción u omisión humana, que repercute en una lesión a bienes como el patrimonio o la integridad personal, y frente al *cual* se impone una reacción a manera de reparación o, al menos, de satisfacción o consuelo cuando no es posible conseguir la desaparición del agravio (nft).

También ha señalado la Corte Suprema de Justicia que

> *en contraposición al daño estrictamente patrimonial, el perjuicio extrapatrimonial no se reduce al tradicional menoscabo moral, pues dentro del conjunto de bienes e intereses jurídicos no patrimoniales que pueden resultar afectados mediante una conducta dolosa o culposa se encuentran comprendidos aquéllos distintos a la aflicción, el dolor, el sufrimiento o la tristeza que padece la víctima*. ***En este contexto, son especies de perjuicio no patrimonial —además del daño moral— el daño a la salud, a la vida de relación, o a bienes jurídicos de especial protección constitucional tales como la libertad, la dignidad, la honra y el buen nombre, que tienen el rango de derechos humanos fundamentales*** (Sentencia SC10297-2014).

Por su parte, la jurisprudencia del Consejo de Estado ha reconocido la tipología de daño por afectación relevante a bienes o derechos convencional y constitucionalmente amparados, señalando que una de las características de este tipo de daños es que se repara principalmente a través de medidas de carácter no pecuniario, ya que se privilegian por excelencia las medidas reparatorias no indemnizatorias.

Sin embargo, el Consejo de Estado en Sentencia 49740 de 2010, Consejera Ponente Marta Nubia Velásquez Rico, señala que

> en casos excepcionales cuya reparación integral, a consideración del juez, no sean suficientes, *pertinentes,* oportunas o posibles podrá otorgarse una indemnización, única y exclusivamente a la víctima directa, mediante el establecimiento de una medida pecuniaria hasta 100 SMLMV, si fuere el caso, siempre y cuando la indemnización no hubiere sido reconocida con fundamento en el daño a la salud. Ese quantum deberá motivarse por el juez y ser proporcional a la intensidad del daño y/o la naturaleza del bien o derecho afectado.

Otra característica de este tipo de daño es que sus efectos se manifiestan en el impedimento de la víctima de gozar y disfrutar de sus derechos constitucionales y convencionales; es decir, desde el punto de vista material, el titular del derecho no puede ejercerlo en las condiciones legales y constitucionales que le fueron reconocidos.

En este contexto, el deber de reparar del Estado nace de la moralización de la reparación en los casos en los que están comprometidos derechos de la personalidad y de la necesidad de la reparación integral cuando en las irregularidades del Estado están comprometidos derechos fundamentales o convencionales.

CONCLUSIONES

La configuración de la responsabilidad del Estado puede darse cuando las autoridades en materia de tratamiento de datos personales no cumplen con los criterios previstos en el orden interno, lo que significa que si bien la situación de pandemia ameritaba que las entidades estatales usaran datos personales para el cumplimiento de la función de prevención y mitigación de la enfermedad, lo que se traduce en que el derecho fundamental individual debe ceder al interés general, no por ello el Estado está habilitado para desconocer los otros criterios que permitan el adecuado tratamiento de los datos en su poder, de tal manera que se entienda que hay una suspensión plena de los derechos a la intimidad personal, de datos personales y de *habeas data*.

Para el caso del tratamiento de los datos relativos a la salud, cuando no hay consentimiento informado se presenta una afectación al derecho de *habeas data* en los casos en los que estos datos son almacenados en bases de datos que no cuenten con los criterios técnicos y jurídicos que aseguren el cumplimiento de los principios y reglas aplicables. También, la ausencia de dicho consentimiento viola el derecho a los datos personales, porque su tratamiento —sin que necesariamente sean almacenados en una base de datos como la de Medellín me Cuida— se efectúa sin el cumplimiento de uno de los criterios que aseguran la autodeterminación informativa: recibir claramente cuál es la finalidad con la que serán tratados los datos por parte de las autoridades y su expresa relación con las funciones estatales que tienen a cargo. Así, por ejemplo, para el caso objeto de estudio en la medida en que no hubo claridad en la información, además de que se señaló que era obligatoria la entrega de la autorización, puede concluirse que hubo violación de este derecho.

Así como se evidencia que no se informó la finalidad específica para el tratamiento de datos sensibles y que requieren, a diferencia del tratamiento de otros datos personales, un consentimiento informado, con el que se garantiza la autonomía de las personas y que estas conozcan las consecuencias que acarrea suministrar esos datos para su tratamiento por parte de las autoridades.

Al ser los derechos a la intimidad, los datos personales y el *habeas data* derechos fundamentales, cuando el Estado no cumple con todos los parámetros legales y constitucionales para asegurar la tutela de cada uno de estos, y dada su relación estrecha con el principio de autodeterminación informativa, hay lugar a hacer un reproche jurídico de responsabilidad por la vía del esquema de afectación a bienes jurídicos de especial protección constitucional, conforme con los criterios vigentes en la jurisprudencia colombiana.

En resumen, el ejercicio de la autonomía por parte del titular de los datos de salud en articulación con la ley estatutaria de protección de datos personales permiten establecer la necesidad de crear para las

entidades públicas el deber de informar al titular sobre la finalidad con la que se usarán sus datos. La falta de información implica una mala praxis. El derecho a la autonomía decisoria es fundamento de la convivencia social, la falta de un consejo ha de considerarse *per se* como un elemento de antijuricidad, que lesiona el derecho de autoderminación informativa del titular con independencia del daño material.

REFERENCIAS

Adinolfi, G. (2007). Autodeterminación informativa consideraciones acerca de un principio general y un derecho fundamental. *Cuestiones constitucionales*, *17*(2), 4-28.

Beauchamp, T. L., & Childress, J. F. (2009). *Principles of biomedical ethics*. Orxford: Oxford University Press.

Christie, G. (2013). La intersección de la responsabilidad extracontractual y el derecho constitucional y los derechos humanos. En C. Bernal Pulido & J. Fabra Zamora (Eds.), *La Filosofía de la responsabilidad civil. Estudios sobre fundamentos filosófico-jurídicos de la responsabilidad civil extracontractual* (pp. 591-608). Bogotá: Universidad Externado de Colombia.

Colombia, Consejo de Estado. Sentencia 49740 (C. P. Marta Nubia Velásquez Rico; 4 de septiembre de 2010).

Colombia, Corte Constitucional. Sentencia C-1011 (M.P. Jaime Córdoba Triviño; 16 de octubre de 2008).

Colombia, Corte Constitucional. Sentencia C-748 (M.P. Jorge Ignacio Pretel Chaljub; 6 de octubre de 2011).

Colombia, Corte Suprema de Justicia. Sentencia SC10297-2014 (M.P. Ariel Salazar Ramírez; 5 de agosto de 2014).

Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*. Oxford: Oxford University Press.

Juzgado 45 Penal Municipal con Funciones de Control de Garantías. Sentencia 103 (J. Yudy Carolina Lozano Muriel; 20 de mayo de 2020).

Juzgado Quinto Penal del Circuito de Medellín. Sentencia segunda instancia. (J. Gustavo Adolfo Restrepo Bolívar; 24 de junio de 2020).

Peña Valenzuela, D. (2015). Responsabilidad del Estado en la sociedad de la información. En J. C. Henao & A. F. Ospina Garzón (Eds.), *La responsabilidad extracontractual del Estado* (pp. 437-479). Bogotá: Universidad Externado de Colombia.

Reyes, Y. (2005). *Imputación objetiva*. Bogotá: Temis S. A.

Parlamento y Consejo Europeo. *Reglamento general de protección de datos*.

Romeo Casabona C. M. (2019). Revisión de las categorías jurídicas de la normativa europea ante la tecnología del *big data* aplicada a la salud. *Revista de Derecho y Genoma Humano: genética, biotecnología y medicina avanzada*, (Extra 1), 85-127.