CONCEPTOS DE LA SALA DE CONSULTA DEL CONSEJO DE ESTADO / HABEAS DATA / DERECHO AL HABEAS DATA / CONCEPTO DE HABEAS DATA / CONCEPTO DE DERECHO AL HABEAS DATA - Derecho autónomo que tiene como objeto la protección de los datos personales / ALCANCE DEL DERECHO AL HABEAS DATA / PROTECCIÓN DEL DERECHO AL HABEAS DATA / DATOS PERSONALES / PROTECCIÓN DE DATOS PERSONALES

La jurisprudencia, especialmente la constitucional, se ha pronunciado en múltiples oportunidades acerca del derecho al habeas data. En desarrollo de lo anterior, ha identificado las siguientes características: i) Es un derecho autónomo que tiene como objeto la protección de los datos personales. ii) Comprende las siguientes prerrogativas mínimas: "De conformidad con la jurisprudencia de esta Corporación, dentro de las prerrogativas –contenidos mínimos- que se desprenden de este derecho encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas está recogida en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de se (sic) provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien por que (sic) se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa." iii) El derecho al habeas data se encuentra íntimamente vinculado con los derechos a la intimidad, el buen nombre y el libre desarrollo de la personalidad. iv) Distintos instrumentos internacionales consagran la protección de los datos personales. Dentro de los más importantes, se encuentran la Carta de los Derechos Fundamentales de la Unión Europea de 1999 (que se cita aquí a título de importante referencia comparada), la Resolución 45/95 del 14 de diciembre de 1990 de Naciones Unidas y la Convención Americana de Derechos Humanos. v) En el ámbito interno, la protección a los datos personales se materializa, principalmente, a través de las Leyes Estatutarias 1266 de 2008 y 1581 de 2012. (…).

FUENTE FORMAL: CONSTITUCIÓN POLÍTICA - ARTÍCULO 15 / LEY 1266 DE 2008 / LEY 1581 DE 2012

NOTA DE RELATORÍA: Sobre las características del derecho al habeas data, ver: Corte Constitucional, sentencia C-748 de 2011

DATOS PERSONALES / PROTECCIÓN DE DATOS PERSONALES / MANEJO DE DATOS PERSONALES / DATOS PERSONALES EN MATERIA ECONÓMICA / ADMINISTRACIÓN DE LAS BASES DE DATOS PERSONALES / BASE DE DATOS PERSONALES / RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES / PRINCIPIOS DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES

Ante el ámbito restringido de la Ley 1266 de 2008; el interés de que el país fuera considerado en la comunidad internacional como un país seguro en la protección de datos, lo que le permitiría atraer inversión extranjera y generar empleos, y la necesidad de llenar el vacío jurídico existente en materia de protección de datos personales, fue promulgada la Ley Estatutaria 1581 de 2012. La Ley 1581 de 2012 tiene como finalidad asegurar la protección efectiva los datos personales, de tal manera que durante todo su tratamiento (recolección, almacenamiento, registro, uso o divulgación) se aseguren altos estándares de calidad en el manejo de la

información. Con este propósito, establece una serie de límites para el uso y administración de los datos personales; impone responsabilidades y deberes respecto al tratamiento de los datos, y brinda a sus titulares herramientas para exigir su protección frente a cualquier vulneración. De esta suerte, la Ley 1581 de 2012 constituye el marco legal general para el tratamiento de los datos personales en nuestro país. Una de las características más importantes de la Ley 1581 de 2012 es la incorporación de una serie de principios que contribuyen en la interpretación de sus disposiciones. Se trata de los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. El contenido de cada uno de estos principios fue establecido expresamente por el legislador a través del artículo 4º de la ley (…).

FUENTE FORMAL: LEY 1266 DE 2008 / LEY 1581 DE 2012 - ARTÍCULO 4

NOTA DE RELATORÍA: Sobre los estándares mínimos de protección de los datos personales, ver: Corte Constitucional, sentencias C-1011 de 2008 y C-748 de 2011.

DATOS PERSONALES / ADMINISTRACIÓN DE LAS BASES DE DATOS PERSONALES / BASE DE DATOS PERSONALES / MANEJO DE DATOS PERSONALES / PROTECCIÓN DE DATOS PERSONALES / RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES POR PARTE DE LAS ENTIDADES PÚBLICAS - Las entidades públicas pueden ser encargadas o responsables del tratamiento de datos personales / TRATAMIENTO DE DATOS PERSONALES / ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES / RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES / CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES – Excepción al tratamiento de datos personales

[E]s claro que las entidades públicas pueden ser encargadas o responsables del tratamiento de datos personales, con los deberes y obligaciones que la Ley 1581 y la jurisprudencia constitucional impone a cada uno de ellos. Como se recordará, el tratamiento solo puede ejercerse con el consentimiento, previo, expreso e informado del titular, es decir, los datos personales no podrán ser obtenidos o divulgados sin previa autorización del titular. No obstante, la misma ley establece excepciones. (…) De lo establecido por el artículo 10 de la Ley 1581 de 2012 y lo expuesto en la sentencia C-748 de 2011 de la Corte Constitucional, la Sala extrae los siguientes aspectos relevantes para resolver la consulta: i) El consentimiento del titular de la información es un presupuesto para la legitimidad de los procesos de administración de datos personales: ii) No existe una autorización tácita para la administración de dichos datos; iii) Sin embargo, el propio legislador consagró una serie de hipótesis en las cuales es posible acceder a información personal sin la autorización previa de su titular; iv) Dentro de las hipótesis señaladas por el legislador, se encuentra la información requerida por una autoridad pública o administrativa en el ejercicio de sus funciones legales, hipótesis que es concordante, además, con lo establecido en el artículo 13 de la Ley 1581 de 2012; v) El acceso a la información por parte de dichas autoridades está sujeto a la observancia de requisitos legales y, en ningún caso puede realizarse de manera abusiva. De esta manera, el dato personal puede ser requerido por la autoridad pública o administrativa bajo el condicionamiento de que la petición se sustente en la conexidad directa con alguna de sus funciones. vi) La conexidad que legitima la solicitud de información no corresponde a un asunto discrecional o de conveniencia, sino que debe fundamentarse en «una clara y específica competencia funcional de la entidad». vii) Asimismo, la autoridad administrativa

que acceda a la información debe cumplir con las obligaciones de protección y garantía al derecho fundamental de habeas data. viii) Con fundamento en el artículo 74 de la Constitución Política, el acceso a datos de naturaleza pública tampoco requiere de autorización previa. Es claro para la Sala que de conformidad con los antecedentes de la consulta, la Procuraduría General de la Nación, como responsable del tratamiento de datos, debe cumplir con las exigencias legales para el tratamiento de los datos personales a los que pretende acceder.

NOTA DE RELATORÍA: Sobre el concepto de tratamiento, la distinción entre encargado y responsable de datos personales y sobre la a excepción a la obligación de obtener el consentimiento del titular para el tratamiento de datos personales, ver: Corte Constitucional, sentencia C-748 de 2011.

FUENTE FORMAL: LEY 1581 DE 2012 - ARTÍCULO 10 / LEY 1581 DE 2012 - ARTÍCULO 3

DATOS PERSONALES / ADMINISTRACIÓN DE LAS BASES DE DATOS PERSONALES / BASE DE DATOS PERSONALES / MANEJO DE DATOS PERSONALES / PROTECCIÓN DE DATOS PERSONALES / RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES / ENTIDAD PÚBLICA / PROCURADURÍA GENERAL DE LA NACIÓN / FACULTADES DE LA PROCURADURÍA GENERAL DE LA NACIÓN / FUNCIONES DE LA PROCURADURÍA GENERAL DE LA NACIÓN / FUNCIÓN PREVENTIVA DE LA PROCURADURÍA GENERAL DE LA NACIÓN / REGISTRO ÚNICO NACIONAL DE TRÁNSITO - En ejercicio de la función preventiva la Procuraduría General de la Nación no puede acceder masivamente a datos personales

El Ministerio Público es un órgano de control (art. 117 CP), ejercido entre otros, por el procurador general de la Nación (funcionario que es su supremo director, art. 275 CP), por los procuradores delegados y los agentes del ministerio público, a quienes les corresponde la guarda y promoción de los derechos humanos, la protección del interés público y la vigilancia de la conducta oficial de quienes desempeñan funciones públicas (art. 118 CP). Si bien las funciones básicas del procurador general de la Nación, sus delegados y agentes se encuentran previstas en el artículo 277 CP, allí no se alude explícitamente a la «función preventiva», aunque sí se confiere la función de «exigir a los funcionarios públicos y a los particulares la información que considere necesaria» (núm. 9). (…) De esta manera, para dilucidar en qué consiste la «función preventiva» de ese órgano de control, resulta necesario acudir al Decreto Ley 262 de 2000 (…). [L]a PGN, dentro de su función preventiva, observa o cuida el ejercicio diligente de las funciones públicas, con el objeto de anticiparse, evitar, mitigar la ocurrencia de hechos que afecten los derechos de las personas o el patrimonio público. Y en desarrollo de tal labor preventiva puede exigir a los servidores públicos y a los particulares que cumplan funciones públicas «la información que se considere necesaria». Cabe destacar que en la «Guía Preventiva», la manera de solicitar dicha información se da a través de lo que denomina requerimientos. Nótese que la función preventiva que se comenta alude al «ejercicio de la función pública» correspondiente, y respecto de los servidores públicos y los particulares que cumplan la función, a quienes se les puede realizar el requerimiento de información. En consecuencia, la «clara y específica competencia funcional», exigida por la ley y la jurisprudencia, corresponde a que la PGN puede solicitar información a los servidores públicos y los particulares que cumplan la función pública respecto de la cual se está ejerciendo la función preventiva, con el objeto de anticiparse, evitar, mitigar la ocurrencia de hechos que afecten los derechos de las personas o el patrimonio público en desarrollo de dicha función pública. Claramente corresponde a una

información puntual o específica requerida para el ejercicio de la función preventiva, tendiente a evitar el riesgo identificado por la PGN, por lo que la solicitud de información no puede tener el carácter de «masiva». Además, la información que puede requerir la PGN es únicamente sobre las actividades que corresponden a la función pública, sin que tal facultad se extienda a que ese organismo de control solicite información relacionada con los datos personales consignados en el RUNT, sin la autorización del respectivo titular. Concluye entonces la Sala, que en ejercicio de la función preventiva la PGN no puede acceder masivamente a los datos personales (privados, semiprivados y sensibles) que reposan en una base de datos administrada por una entidad pública, o por particulares que cumplan funciones públicas, puesto que tal solicitud no corresponde a una «clara y específica competencia funcional» que le haya sido otorgada por la ley.

FUENTE FORMAL: CONSTITUCIÓN POLÍTICA - ARTÍCULO 117 / CONSTITUCIÓN POLÍTICA - ARTÍCULO 118 / CONSTITUCIÓN POLÍTICA - ARTÍCULO 275 / CONSTITUCIÓN POLÍTICA - ARTÍCULO 277 / DECRETO LEY 262 DE 2000 - ARTÍCULO 23 / DECRETO LEY 262 DE 2000 - ARTÍCULO 24 / DECRETO LEY 262 DE 2000 - ARTÍCULO 37 / DECRETO LEY 262 DE 2000 - ARTÍCULO 38 / DECRETO LEY 262 DE 2000 - ARTÍCULO 7

REGISTRO ÚNICO NACIONAL DE TRÁNSITO / AUTORIDAD DE TRÁNSITO / ORGANISMOS DE TRÁNSITO / INFORMACIÓN PÚBLICA / INFORMACIÓN PÚBLICA RESERVADA / INFORMACIÓN PÚBLICA CLASIFICADA / DATO PÚBLICO – La información contenida en el Registro Único Nacional de Tránsito es de naturaleza pública aunque puede contener información privada, semiprivada o sensible

El Registro Único Nacional de Tránsito se encuentra regulado en las Leyes 769 de 2002 (artículo 8 y ss.) y 1005 de 2006 (artículo 1º y ss.), es un sistema de información que: "[I]ncorpora lo relacionado con el registro de automotores, conductores, licencias de tránsito, empresas de transporte público, infractores, accidentes de tránsito, seguros, remolques y semirremolques, maquinaria agrícola y de construcción autopropulsada y de personas naturales o jurídicas que prestan servicio al sector transporte." En términos generales, el RUNT desarrolla tres procesos principales: i) valida información, ii) autoriza la realización de trámites por los organismos de tránsito y iii) registra actuaciones. (…) Es importante señalar que, de acuerdo con lo consagrado expresamente por el artículo 9º de la Ley 769 de 2002, la información contenida en el RUNT es de naturaleza pública. Con todo, la Superintendencia de Industria y Comercio ha señalado que, con base en el artículo 3º del Decreto Reglamentario 1377 de 2013, hoy compilado en el artículo 2.2.2.25.1.3. del Decreto 1074 de 2015, puede existir información que, a pesar de estar contenida en un documento público, no tenga dicha calidad, sino que corresponda a información privada, semiprivada o sensible.

FUENTE FORMAL: DECRETO 1074 DE 2015 - ARTÍCULO 2.2.2.25.1.3. / DECRETO REGLAMENTARIO 1377 DE 2013 - ARTÍCULO 3 / LEY 1005 DE 2006 - ARTÍCULO 1 / LEY 1712 DE 2014 - ARTÍCULO 6 / LEY 769 DE 2002 - ARTÍCULO 8 / LEY 769 DE 2002 - ARTÍCULO 9

DATOS SENSIBLES / INFORMACIÓN PÚBLICA / INFORMACIÓN PRIVADA / INFORMACIÓN SEMIPRIVADA / INFORMACIÓN / INFORMACIÓN PÚBLICA RESERVADA / REGISTRO ÚNICO NACIONAL DE TRÁNSITO - El acceso de las autoridades administrativas a información sensible para el cumplimiento de sus funciones no hace parte de las excepciones establecidas por el

legislador

[F]rente a la información que puede ser transferida a una autoridad pública, la Sala señala lo siguiente: i) Datos públicos: por su naturaleza pública y teniendo en cuenta lo dispuesto en el artículo 74 de la Constitución Política, a este tipo de datos puede acceder cualquier persona. En consecuencia, pueden ser entregados a una autoridad administrativa que los requiera para el cumplimiento de sus funciones. (…) ii) Datos semiprivados: la Corte Constitucional ha concluido que la información semiprivada, al ser información que está sometida a un grado mínimo de limitación, puede ser obtenida y ofrecida por una autoridad administrativa en cumplimiento de sus funciones (…). iii) Datos privados: a diferencia de la información pública y semiprivada, los datos privados no pueden ser ofrecidos ni obtenidos por una autoridad administrativa que los requiera para el cumplimiento de sus funciones. Lo anterior, por tratarse de información que se enmarca en el ámbito puramente privado (…). iv) Datos sensibles: estos datos no pueden ser entregados a otra autoridad administrativa en el cumplimiento de sus funciones. Lo anterior, teniendo en cuenta lo dispuesto por el artículo 6º de la Ley 1581 de 2012, disposición que establece, como regla general el no tratamiento de los mismos (…). Como puede observarse, el acceso de las autoridades administrativas a información sensible para el cumplimiento de sus funciones no hace parte de las excepciones establecidas por el legislador. Por lo tanto, no es posible el acceso de las referidas autoridades a esta información. (…) En suma, la información que puede entregarse a una autoridad administrativa sin la autorización del titular de los datos personales es aquella que corresponde a datos públicos y semiprivados. En este último caso, se requiere que la información sea necesaria para el cumplimiento de sus funciones. En lo que respecta a los datos privados y sensibles, a ellos no puede acceder la autoridad sin la autorización del titular.

FUENTE FORMAL: LEY 1266 DE 2008 - ARTÍCULO 3 / LEY 1581 DE 2012 - ARTÍCULO 10 / LEY 1581 DE 2012 - ARTÍCULO 5 / LEY 1581 DE 2012 - ARTÍCULO 6 / LEY 1712 DE 2014 - ARTÍCULO 6

NOTA DE RELATORÍA 1: Sobre los conceptos de información pública, pública clasificada y pública reservada, ver: Corte Constitucional, sentencia C-276 de 2019.

NOTA DE RELATORÍA 2: Sobre los conceptos de información pública, semiprivada y privada, ver: Corte Constitucional, sentencia T-058 de 2015

DERECHO AL HABEAS DATA / PROTECCIÓN DEL DERECHO AL HABEAS DATA / DIVULGACIÓN DE INFORMACIÓN / INFORMACIÓN PÚBLICA / INFORMACIÓN RESERVADA / PRINCIPIOS DE VERACIDAD E IMPARCIALIDAD EN LA INFORMACIÓN / SUMINISTRO DE INFORMACIÓN / REGISTRO ÚNICO NACIONAL DE TRÁNSITO / DERECHO A LA INFORMACIÓN / ENTREGA DE INFORMACIÓN DE MANERA ANÓNIMA / DIVULGACIÓN PARCIAL DE LA INFORMACIÓN PRINCIPIO DE MÁXIMA DIVULGACIÓN DE LA INFORMACIÓN / PRINCIPIO DE TRANSPARENCIA DE LA INFORMACIÓN / PRINCIPIO DE FACILITACIÓN DE LA INFORMACIÓN / PRINCIPIO DE LA CALIDAD DE LA INFORMACIÓN / PRINCIPIO DE FINALIDAD EN EL TRATAMIENTO DE LA INFORMACIÓN

[E]s posible concluir lo siguiente respecto a la manera como debe entregarse la información requerida por una autoridad administrativa en el cumplimiento de sus funciones: i) Por regla general, el acceso a la información que se encuentra en posesión, bajo control o custodia de una autoridad es pública. ii) En línea con lo

anterior, el acceso a dicha información solamente puede ser restringido de manera excepcional, esto es, cuando una disposición constitucional o legal así lo determine. iii) Por consiguiente, la información pública que no se encuentre cubierta por una excepción que restrinja su acceso, debe ser entregada a la parte solicitante. iv) Las autoridades deben responder de manera adecuada a las solicitudes de acceso a la información. En consecuencia, y dentro de los límites legales y constitucionales, deben facilitar el acceso a la información, de tal manera que no pueden establecer exigencias o requisitos que lo obstruyan o impidan. v) La entrega de la información debe realizarse de manera completa, exacta y comprensible. Asimismo, debe ser de fácil consulta, sin barreras técnicas y corresponder a la contenida en la base de datos. vi) Finalmente, por expreso mandato legal, es posible la divulgación parcial de información. A la luz de las conclusiones anteriores, resulta válido afirmar que no es posible la entrega de la información del RUNT de manera anónima, pues i) los nombres y apellidos de las personas son públicos, ii) la información debe entregarse de manera completa, exacta y comprensible, iii) ni la Constitución ni la ley autorizan la entrega anónima de información requerida por una autoridad administrativa en cumplimiento de sus funciones y iv) los responsables de la información no pueden imponer límites o exigencias que obstruyan o impidan el acceso a esta.

FUENTE FORMAL: LEY 1581 DE 2012 - ARTÍCULO 11 / LEY 1581 DE 2012 - ARTÍCULO 4 / LEY 1712 DE 2014 - ARTÍCULO 2 / LEY 1712 DE 2014 - ARTÍCULO 21 / LEY 1712 DE 2014 - ARTÍCULO 3 / LEY 1712 DE 2014 - ARTÍCULO 4

REGISTRO ÚNICO NACIONAL DE TRÁNSITO – Naturaleza de la información contenida en el RUNT / PROCURADURÍA GENERAL DE LA NACIÓN / FUNCIÓN PREVENTIVA DE LA PROCURADURÍA GENERAL DE LA NACIÓN / DATOS PERSONALES / ADMINISTRACIÓN DE LAS BASES DE DATOS PERSONALES / MANEJO DE DATOS PERSONALES / PROTECCIÓN DE DATOS PERSONALES – Protección del derecho al habeas data

Para la Sala, la adopción de un modelo analítico y el interés por identificar incrementos patrimoniales son instrumentos que, en sí mismos, no justifican el acceso a la información del RUNT por parte de la Procuraduría General de la Nación, puesto que teniendo en cuenta los parámetros establecidos por la ley y la jurisprudencia, no se cumpliría con el principio de finalidad. A lo anterior debe sumarse que, como se explicó anteriormente, la Procuraduría en ejercicio de su función preventiva, no está facultada para acceder a la información. (…) Como puede observarse, las motivaciones que justifican la recopilación y tratamiento de los datos que hacen parte del RUNT, no encuadran en el propósito alegado por la Procuraduría para acceder a los mismos, toda vez que el señalado registro no fue concebido como un instrumento para la lucha contra la corrupción, sino como un sistema de información para la adecuada administración de los datos relevantes en materia de transporte, los cuales están sujetos a la protección que la Constitución otorga a las personas -derecho al habeas data- en los términos expuestos en este concepto, en particular frente al principio de finalidad.

FUENTE FORMAL: LEY 1581 DE 2012 - ARTÍCULO 4

NOTA DE RELATORÍA: Sobre el principio de finalidad de la información, ver: Corte Constitucional, sentencias C-748 de 2011, SU-458 de 2012 y T-729 de 2002.

CONSEJO DE ESTADO

SALA DE CONSULTA Y SERVICIO CIVIL

Consejero ponente: ÁLVARO NAMÉN VARGAS

Bogotá D.C., seis (6) de mayo de dos mil veintiuno (2021)

Radicación número: 11001-03-06-000-2020-00234-00(2458)

Actor: MINISTERIO DE TRANSPORTE

Referencia: Habeas data. Acceso a la información pública. RUNT.

El Ministerio de Transporte consulta a la Sala sobre la posibilidad de que la Procuraduría General de la Nación en ejercicio de la función preventiva pueda acceder de manera masiva a las bases de datos administradas por entidades públicas del orden nacional, como los Ministerios, y por ende a datos personales de los usuarios de las mismas.

I. ANTECEDENTES

El Ministerio de Transporte expuso en el escrito de consulta las siguientes consideraciones:

1. Dando cumplimiento a lo establecido en el artículo 8 de la Ley 769 de 2002, el Ministerio de Transporte implementó el Registro Único Nacional de Tránsito (en adelante, RUNT).

2. Aunque la información contenida en el RUNT es de carácter público (artículo 9 de la Ley 769 de 2002), la información que reposa en los diferentes registros que lo integran contiene datos personales del titular de la información, es decir, información de carácter privado, semiprivado y sensible.

3. En virtud del artículo 13 de la Ley 1581 de 2012, las autoridades administrativas pueden realizar el tratamiento de los datos personales sin autorización del titular, siempre y cuando la solicitud de información esté basada en una clara y específica competencia funcional de la entidad y garanticen la protección de los derechos de habeas data del titular.

4. Teniendo en cuenta el principio de finalidad, establecido en el artículo 4º de la Ley 1581 de 2012, las entidades públicas deben utilizar los datos personales únicamente para los fines que justificaron la entrega de los mismos, esto es, aquellos relacionados con la competencia funcional específica que motivó la solicitud de suministro del dato personal. Asimismo, las autoridades deben informar al titular del uso de los datos e implementar las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos personales y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

5. La entidad pública solicitante adquiere la posición jurídica de usuario dentro del proceso de administración de datos personales, lo que le impone el deber de garantizar los derechos fundamentales del titular de la información, previstos en la

Constitución Política. En consecuencia, de acuerdo con la Sentencia C-748 de 2011 de la Corte Constitucional, deberá: (i) guardar reserva de la información que les sea suministrada por los operadores y utilizarla únicamente para los fines que justificaron la entrega, esto es, aquellos relacionados con la competencia funcional específica que motivó la solicitud de suministro del dato personal; (ii) informar a los titulares del dato el uso que le esté dando al mismo; (iii) conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento; y (iv) cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la legislación estatutaria.

6. El artículo 16 del Decreto Ley 2150 de 1995, modificado por el artículo 14 de la Ley 962 de 2005, consagra el deber de las entidades públicas de compartir información entre sí.

7. Sin embargo, teniendo en cuenta la jurisprudencia de la Corte Constitucional, el deber de las entidades públicas de compartir información no implica que se permita el acceso a las bases de datos de manera ilimitada, toda vez no puede vulnerarse el derecho fundamental de habeas data.

8. Mediante los oficios 430-20 del 19 de junio de 2020 y 434-20 del 24 de junio del mismo año, la Procuraduría General de la Nación, invocando el ejercicio de la función preventiva, solicitó al Ministerio del Transporte el acceso masivo a ciertos registros incorporados en el RUNT, los cuales contribuyen, según el referido ente de control, al análisis del patrimonio en cabeza de funcionarios públicos. Este acceso, «[p]ermitiría dar un paso al frente en la lucha contra la corrupción, nutriendo el sistema que ha de crearse de valiosos insumos que nos permitirían enfocar los esfuerzos disciplinarios para que, en el marco de ese proceso legalmente regulado, y con el uso de la información semiprivada a la que podremos acceder por virtud de las órdenes jurisdiccionales que se encuentren necesarias, podamos perseguir aquellos servidores públicos que incrementen de manera injustificada su patrimonio».

9. Posteriormente, a través del oficio 494-20 del 5 de agosto, la Procuraduría señaló el universo de ciudadanos de los cuales solicita hacer entrega de información: a) funcionarios públicos con mayor perfil de riesgos y sus familias, de acuerdo con lo reportado en SIGEP; b) solo los familiares mayores de edad, y c) la información correspondiente a los 3 últimos años.

10. La información que se encuentra en las bases de datos está catalogada como datos personales, privados, semiprivados, e incluso sensibles.

Teniendo en cuenta las consideraciones anteriores, el Ministerio de Transporte pregunta a la Sala:

> *1. ¿Tiene facultad la Procuraduría General de la Nación en ejercicio de la competencia a prevención para (sic) a acceder masivamente a las bases de datos en administración de una entidad pública?*
>
> *2. ¿La función preventiva de la Procuraduría se enmarca dentro del concepto de las (sic) excepción contenida en (sic) literales a) del artículo 10 de la Ley 1581 de 2012, que establece que no será necesaria la autorización del Titular cuando esta es "…requerida por una entidad pública o administrativa en ejercicio de sus funciones legales"?*
>
> *3. ¿Cuál sería la extensión de esa facultad de cara a las funciones preventivas de la Procuraduría, cuya competencia se desarrolla solamente*

con relación a los sujetos disciplinables, y en esa medida se debe determinar si en dicho ejercicio pueden tener acceso a los datos depositados de todos los ciudadanos sin discriminación a los sujetos disciplinables?

4. ¿En el evento de ser extensiva la excepción contenida en el literal a) del artículo 10 de la Ley 1581 de 2012, a los órganos de control en especial a la Procuraduría General de la Nación, en ejercicio de la "función preventiva", en virtud del principio de finalidad, previo a recibir la información requerida deben adoptar tratamiento de datos?

5. A la luz del literal a) del artículo 10 de la ley 1581 de 2012, ¿qué información es susceptible de ser entregada a una entidad pública sin autorización del titular de los datos personales, a la entidad solicitante? ¿Solo Datos públicos? ¿datos privados? ¿Datos semiprivados? ¿Incluso datos sensibles?

6. ¿La solicitud de transmisión de la información puede ser suscrita por cualquier funcionario de la Procuraduría General de la Nación o debe ser solicitada directamente por el Procurador General, como quiera que es la autoridad encargada de iniciar, adelantar y fallar las investigaciones que por faltas disciplinarias se adelanten en contra de servidores públicos?

7. En aras de proteger el derecho de habeas data en cabeza de sus titulares, a juicio de esta Sala, ¿es el modelo analítico y el interés de identificar incrementos patrimoniales injustificados, una finalidad legítima de acuerdo con la Constitución y la Ley para permitir el tratamiento y acceso a los datos personales que reposan en el RUNT?

8. Asimismo, en aras de proteger el derecho fundamental de habeas data de los titulares, el Ministerio de Transporte como responsable de dichos datos, podría entregar en un primer momento tal información de forma anonimizada, y una vez identificada alguna alerta de incremento patrimonial injustificado, proveer ya una información más específica?

9. De acuerdo con el principio de necesidad establecido en la sentencia C-748 de 2011, los datos personales registrados en el RUNT que son requeridos por la Procuraduría General de la Nación, en concepto de esta Sala, ¿son estrictamente necesarios para el cumplimiento de sus finalidades?

II. CONSIDERACIONES

De conformidad con los antecedentes y preguntas formuladas el problema jurídico central que debe resolver la Sala es el siguiente: *¿La Procuraduría General de la Nación, en ejercicio de la función preventiva, puede acceder masivamente a los datos personales que reposan en una base de datos administrada por una entidad pública?*

Con el fin de resolver el señalado problema jurídico, la Sala estima necesario abordar los siguientes temas: i) la protección de los datos personales; ii) el tratamiento de los datos personales por las entidades públicas; iii) las excepciones aplicables a las entidades públicas; iv) la función preventiva de la Procuraduría General de la Nación, y iii) la clasificación de la información que contiene el RUNT.

1. La protección de los datos personales

La Constitución Política establece el derecho al *habeas data* en el artículo 15, así:

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

La jurisprudencia, especialmente la constitucional, se ha pronunciado en múltiples oportunidades acerca del derecho al *habeas data*. En desarrollo de lo anterior, ha identificado las siguientes características:

i) Es un derecho autónomo[1] que tiene como objeto la protección de los datos personales[2].

ii) Comprende las siguientes prerrogativas mínimas:

> De conformidad con la jurisprudencia de esta Corporación, dentro de las prerrogativas –contenidos mínimos- que se desprenden de este derecho encontramos por lo menos las siguientes: **(i)** el derecho de las personas a **conocer** –acceso- la información que sobre ellas está recogida en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; **(ii)** el derecho a **incluir** nuevos datos con el fin de se (sic) provea una imagen completa del titular; **(iii)** el derecho a **actualizar** la información, es decir, a poner al día el contenido de dichas bases de datos; **(iv)** el derecho a que la información contenida en bases de datos sea **rectificada o corregida**, de tal manera que concuerde con la realidad; **(v)** el derecho a **excluir** información de una base de datos, bien por que (sic) se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa[3].

iii) El derecho al habeas data se encuentra íntimamente vinculado con los derechos a la intimidad[4], el buen nombre y el libre desarrollo de la personalidad[5].

---

[1] Estos preceptos leídos en conjunto con la primera parte del mismo artículo 15 –sobre el derecho a la intimidad, el artículo 16 –que reconoce el derecho al libre desarrollo de la personalidad- y el artículo 20 –sobre el derecho a la información activo y pasivo y el derecho a la rectificación- de la Carta, han dado lugar al reconocimiento de un derecho fundamental autónomo catalogado como derecho al habeas data, y en algunas oportunidades, como derecho a la autodeterminación informativa o informática. Corte Constitucional. Sentencia del 6 de octubre de 2011, C-748/11.

[2] En resumen, como lo muestra el anterior recuento, el reconocimiento del derecho al habeas data –identificado como un derecho fundamental autónomo tanto en el plano nacional como internacional- persigue la protección de los datos personales en un mundo globalizado en el que el poder informático es creciente. Ibidem.

[3] Ibidem.

[4] La protección de los datos personales surgió ligada al derecho a la intimidad, reconocido en varios instrumentos del derecho internacional de los derechos humanos. Ibidem.

iv) Distintos instrumentos internacionales consagran la protección de los datos personales. Dentro de los más importantes, se encuentran la Carta de los Derechos Fundamentales de la Unión Europea de 1999 (que se cita aquí a título de importante referencia comparada), la Resolución 45/95 del 14 de diciembre de 1990 de Naciones Unidas y la Convención Americana de Derechos Humanos.

v) En el ámbito interno, la protección a los datos personales se materializa, principalmente, a través de las Leyes Estatutarias 1266 de 2008[6] y 1581 de 2012[7].

Así, la Ley 1266 de 2008 tiene como propósito proteger los datos personales en materia financiera y crediticia. En este sentido, la Corte Constitucional señaló en la Sentencia C-1011 de 2008:

> Como se expondrá en detalle en el apartado 1.1. del análisis material de la iniciativa, el Proyecto de Ley, considerado a partir de criterios sistemáticos, históricos y teleológicos, tiene por objeto particular establecer un sistema de reglas para la administración de datos personales relacionados con el comportamiento crediticio, excluyéndose otras materias, como es el caso del derecho a la información, el derecho a la intimidad y la regulación de otros escenarios del ejercicio del derecho al hábeas data, distinto al expuesto.
>
> [...]
>
> En efecto, en el apartado 1.1. del análisis material del Proyecto de Ley se demostró, a partir de argumentos de naturaleza sistemática, teleológica e histórica, que la iniciativa es una regulación del derecho al hábeas data con un carácter sectorial, en la medida en que los mecanismos concretos para la protección del derecho contenidos en el Proyecto respondían exclusivamente a la recopilación de datos personales de contenido financiero, comercial y crediticio, destinados al cálculo de riesgo crediticio. Dentro de ese análisis se dieron algunos ejemplos de cómo conceder carácter genérico al Proyecto, esto es, extender sus reglas a todos los escenarios de administración de datos personales, llevaría a contrasentidos e, incluso, a vulneraciones de las normas constitucionales. Con base en lo anterior, se concluyó que el entendimiento acertado del Proyecto de Ley es el de un régimen particular y específico, dirigido a la fijación de reglas para la administración de datos personales financieros, comerciales y crediticios, con exclusión de otras modalidades de ejercicio del derecho al hábeas data. (Subrayas de la Sala).

Ante el ámbito restringido de la Ley 1266 de 2008; el interés de que el país fuera considerado en la comunidad internacional como un país seguro en la protección de datos, lo que le permitiría atraer inversión extranjera y generar empleos[8], y la

---

[5] Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre y el libre desarrollo de la personalidad. Ibidem.

[6] Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

[7] Por la cual se dictan disposiciones generales para la protección de datos personales.

[8] Este proyecto incorpora en su articulado las mejores prácticas internacionales en materia de protección de datos contempladas en Convenio 108 de 1981 del Consejo de Europa, la Directiva Europea 95/46 de 1995, la Resolución 45/95 de 1990 de la ONU y la Resolución de Madrid de 2009, con el objetivo de lograr con esta ley la acreditación de Colombia por parte de la Unión Europea como un país seguro en protección de datos y así poder acceder al mercado europeo sin restricciones atrayendo inversión extrajera y generando nuevos empleos. Gaceta del Congreso núm. 488 del 4 de agosto de 2010.

necesidad de llenar el vacío jurídico existente en materia de protección de datos personales[9], fue promulgada la Ley Estatutaria 1581 de 2012.

La Ley 1581 de 2012 tiene como finalidad asegurar la protección efectiva los datos personales, de tal manera que durante todo su tratamiento (recolección, almacenamiento, registro, uso o divulgación) se aseguren altos estándares de calidad en el manejo de la información. Con este propósito, establece una serie de límites para el uso y administración de los datos personales; impone responsabilidades y deberes respecto al tratamiento de los datos, y brinda a sus titulares herramientas para exigir su protección frente a cualquier vulneración[10]. De esta suerte, la Ley 1581 de 2012 constituye el marco legal general para el tratamiento de los datos personales en nuestro país[11].

Una de las características más importantes de la Ley 1581 de 2012 es la incorporación de una serie de principios que contribuyen en la interpretación de sus disposiciones[12]. Se trata de los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

El contenido de cada uno de estos principios fue establecido expresamente por el legislador a través del artículo 4º de la ley, disposición que señala:

> Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

---

[9] Este nuevo proyecto de ley busca llenar el vacío de estándares mínimos de protección de todos los datos personales –anunciado por la Corte Constitucional en la sentencia C-1011 de 2008, de ahí que su título sea precisamente "Por el cual se dictan disposiciones generales para la protección de datos personales". Esa intención también fue anunciada por el gobierno en la exposición de motivos, en la que afirmó: "(…) es necesario que el país cuente con una legislación integral y transversal que garantice la protección efectiva de los datos personales en todo el proceso de tratamiento". Corte Constitucional. Sentencia del 6 de octubre de 2011, C-748/11. Véase igualmente: Es importante señalar que este proyecto de ley complementa la Ley 1266 de 2008, que se refiere a un ámbito muy preciso de datos y responde a particulares necesidades de los usuarios del sector financiero que es necesario conservar. Este proyecto se encarga del universo de los demás datos personales que la Ley 1266 de 2008 no cobija. Gaceta del Congreso núm. 488 del 4 de agosto de 2010.

[10] Como quiera que en múltiples actividades cotidianas y en distintos ámbitos, los ciudadanos para acceder a bienes y servicios entregan una gama más o menos amplia de datos personales, y que en la circulación de los mismos no siempre se observa el debido cuidado frente al manejo de esa información, es necesario que el país cuente con una legislación integral y transversal que garantice la protección efectiva de los datos personales en todo el proceso de tratamiento. Esto significa que en su recolección, almacenamiento, registro, uso o divulgación se garantice que desde el otorgamiento del consentimiento por parte del Titular para que sean utilizados con los fines que se le indiquen, hasta el momento en que tal uso se efectúe legítimamente por parte de un tercero, se hayan utilizado altos estándares de calidad en el manejo de la información al tiempo que se le otorguen claras herramientas al Titular para exigir medidas concretas de protección frente a cualquier vulneración de que pudiera ser víctima. Ibidem.

[11] El proyecto de ley pretende crear un marco legal general para el tratamiento de cualquier clase de dato personal, propone una visión transversal de los límites en el uso y administración de datos personales creando responsabilidades para quienes los reciban y administren describiendo quienes son los responsables del dato cuando el titular lo entrega y este es objeto de tratamiento. Gaceta del Congreso núm. 1023 del 2 de diciembre de 2010.

[12] La introducción de principios resulta de fundamental importancia ya que los mismos irradian las disposiciones del proyecto de ley y se constituyen en la base para su construcción. Los principios que se recogen en el proyecto de ley no solo recogen los desarrollos jurisprudenciales que se han hecho en la protección del derecho de habeas data sino que se constituyen en la fuente básica de interpretación de todo su articulado. Gaceta del Congreso núm. 488 del 4 de agosto de 2010.

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

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

h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma. (Se Subraya).

Con base en los anteriores aspectos y principios generales se analizará a continuación lo relacionado con el tratamiento de datos personales por parte de entidades públicas.

2. Las entidades públicas frente al tratamiento de datos personales

La Ley 1581 de 2012, en su artículo 3, define el tratamiento de datos personales en los siguientes términos:

Artículo 3. Definiciones. Para los efectos de la presente ley, se entiende por:

[...]

> g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Igualmente, la misma disposición se refiere a los conceptos de «encargado» y «responsable» del tratamiento:

> d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;
>
> e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;

Frente al concepto de tratamiento y la distinción entre encargado y responsable, la Corte Constitucional concluyó lo siguiente:

> Sin embargo, se debe señalar desde ahora, al igual que se indicó en la sentencia C-1011 de 2008, que **todos los principios** de la administración de datos personales identificados en este proyecto -los cuales serán estudiados en otro acápite- son **oponibles a todos los sujetos** involucrados en el **tratamiento del dato**, entiéndase en la recolección, circulación, uso, almacenamiento, supresión, etc., sin importar la denominación que los sujetos adquieran, es decir, llámense fuente, responsable del tratamiento, operador, encargado del tratamiento o usuario, entre otros.
>
> [...]
>
> Ciertamente, el concepto «*decidir sobre el tratamiento*» empleado por el literal e) parece coincidir con la posibilidad de definir –jurídica y materialmente- los fines y medios del tratamiento. Usualmente, como reconocen varias legislaciones, el responsable es el propietario de la base de datos; sin embargo, con el fin de no limitar la exigibilidad de las obligaciones que se desprenden del habeas data, la Sala observa que la definición del proyecto de ley es amplia y no se restringe a dicha hipótesis. Así, **el concepto de responsable puede cobijar tanto a la fuente como al usuario**, en los casos en los que dichos agentes tengan la posibilidad de decidir sobre las finalidades del tratamiento y los medios empleados para el efecto, por ejemplo, para ponerlo en circulación o usarlo de alguna manera.
>
> De otro lado, el criterio de delegación coincide con el término «*por cuenta de*» utilizado por el literal e), lo que da a entender una relación de subordinación del encargado al responsable, sin que implique que se exima de su responsabilidad frente al titular del dato.
>
> Así, por ejemplo, será responsable del dato el hospital que crea la historia clínica de su paciente, la universidad o las instituciones educativas en relación con los datos de sus alumnos, pues estos determinan la finalidad (en razón de su objeto que, puede estar señalado en una ley o por el giro normal de la actividad que se desarrolla) para la recolección de los datos, así como la forma en que los datos serán procesados, almacenados, circulados, etc.
>
> Ahora bien, vale la pena advertir que el encargado del tratamiento no puede ser el mismo responsable, pues se requiere que existan dos personas identificables e independientes, natural y jurídicamente, entre las cuales una –el responsable- le señala a la otra –el encargado- como quiere el procesamiento de unos determinados datos. En este orden, el encargado recibe unas instrucciones sobre la forma como los datos serán administrados. Volvamos al ejemplo de la historia

> clínica, en el que la institución de salud contrata con una compañía el procesamiento de las historias para que con un programa especial que puede determinar el responsable o la empresa contratada, le organice la información contenida en ellas, siguiendo las indicaciones que establece el hospital. En este caso, el encargado del tratamiento de los datos es la persona jurídica que se contrata para el procesamiento de las hojas de vida.
>
> [...]
>
> En efecto, de acuerdo con las definiciones acogidas por el proyecto de ley, los responsables del tratamiento tienen mayores compromisos y deberes frente al titular del dato, pues son los llamados a garantizar en primer lugar el derecho fundamental al habeas data, así como las condiciones de seguridad para impedir cualquier tratamiento ilícito del dato. La calidad de responsable igualmente impone un haz de responsabilidades, específicamente en lo que se refiere a la seguridad y a la confidencialidad de los datos sujetos a tratamiento.

Conforme a lo expuesto, es claro que las entidades públicas pueden ser encargadas o responsables del tratamiento de datos personales, con los deberes y obligaciones que la Ley 1581 y la jurisprudencia constitucional impone a cada uno de ellos. Como se recordará, el tratamiento solo puede ejercerse con el consentimiento, previo, expreso e informado del titular, es decir, los datos personales no podrán ser obtenidos o divulgados sin previa autorización del titular. No obstante, la misma ley establece excepciones.

3. Excepciones aplicables a las entidades públicas

El artículo 10 de la Ley 1581 de 2012 establece los casos en los cuales no se requiere de la autorización del titular del dato para acceder a ellos, a saber:

> Artículo 10. Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:
>
> a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
>
> b) Datos de naturaleza pública;
>
> c) Casos de urgencia médica o sanitaria;
>
> d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
>
> e) Datos relacionados con el Registro Civil de las Personas.
>
> Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley. (Se subraya)

Al decidir sobre la constitucionalidad de la norma transcrita, la Corte Constitucional reconoció la procedencia de las excepciones allí consagradas, para lo cual tuvo en cuenta los intereses constitucionalmente legítimos que esta busca proteger. Asimismo, la Corte reiteró las obligaciones que surgen para las personas que acceden a la información con fundamento en dichas causales, las cuales están dirigidas a proteger los derechos fundamentales de los titulares de los datos:

> El artículo 10 desarrolla los casos en que no es necesaria su autorización, específicamente cuando: la información es requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, los datos de naturaleza pública, los casos de urgencia médica o sanitaria, tratamiento autorizado

por la Ley para fines históricos, estadísticos o científicos y datos relacionados con el registro civil de las personas.

El consentimiento de la titular de la información es un presupuesto para la legitimidad constitucional de los procesos de administración de datos personales. En concordancia con los expuesto frente al "principio de libertad", en el manejo de los datos no podrá existir una autorización tácita.

En relación con la posibilidad de excepcionar el consentimiento, en estos casos existen importantes intereses constitucionales que justifican tal limitación.

[...]

El artículo 10 del Proyecto de Ley bajo estudio señala las situaciones en las que no es necesaria la autorización, las cuales responden a la naturaleza misma del dato y al tipo de funciones que cumplen. Sin embargo, deben hacerse las siguientes precisiones:

En primer término, se señala que se prescindirá de la autorización cuando la información sea *"requerida por una autoridad pública o administrativa en ejercicio de sus funciones legales o por orden judicial".* Sin embargo, considera la Sala que deben hacerse las mismas observaciones que las contenidas en la Sentencia C-1011 de 2008, al hacer el estudio del Proyecto de Ley Estatutaria de los datos financieros.

En relación, con las autoridades públicas o administrativas, señaló la Corporación que tal facultad *"no puede convertirse en un escenario proclive al abuso del poder informático, esta vez en cabeza de los funcionarios del Estado. Así, el hecho que el legislador estatutario haya determinado que el dato personal puede ser requerido por toda entidad pública, bajo el condicionamiento que la petición se sustente en la conexidad directa con alguna de sus funciones, de acompasarse con la garantía irrestricta del derecho al hábeas data del titular de la información.* En efecto, amén de la infinidad de posibilidades en que bajo este expediente puede accederse al dato personal, la aplicación del precepto bajo análisis debe subordinarse a que la entidad administrativa receptora cumpla con las obligaciones de protección y garantía que se derivan del citado derecho fundamental, en especial la vigencia de los principios de finalidad, utilidad y circulación restringida.

Para la Corte, esto se logra a través de dos condiciones: (i) el carácter calificado del vínculo entre la divulgación del dato y el cumplimiento de las funciones de la entidad del poder Ejecutivo; y (ii) la adscripción a dichas entidades de los deberes y obligaciones que la normatividad estatutaria predica de los usuarios de la información, habida consideración que ese grupo de condiciones permite la protección adecuada del derecho.

En relación con el primero señaló la Corporación que *"la modalidad de divulgación del dato personal prevista en el precepto analizado devendrá legítima, cuando la motivación de la solicitud de información esté basada en una clara y específica competencia funcional de la entidad."* Respecto a la segunda condición, la Corte estimó que una vez la entidad administrativa accede al dato personal adopta la posición jurídica de usuario dentro del proceso de administración de datos personales, lo que de forma lógica le impone el deber de garantizar los derechos fundamentales del titular de la información, previstos en la Constitución Política y en consecuencia deberán: *(i) guardar reserva de la información que les sea suministrada por los operadores y utilizarla únicamente para los fines que justificaron la entrega, esto es, aquellos relacionados con la competencia funcional específica que motivó la solicitud de suministro del dato personal; (ii) informar a los titulares del dato el uso que le esté dando al mismo; (iii) conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento; y (iv) cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la legislación estatutaria."*

En relación con la orden judicial, dijo la Corporación que *si bien no existe una autorización expresa del titular que circunscriba la circulación del dato, la posibilidad*

de acceso resulta justificada en la legitimidad que tienen en el Estado Constitucional de Derecho las actuaciones judiciales, ámbitos de ejercicio de la función pública sometidos a reglas y controles, sustentados en la eficacia del derecho al debido proceso y rodeado de las garantías anejas a éste, en especial, los derechos de contradicción y defensa. Así, reconociéndose la importancia de esta actividad en el régimen democrático, entendida como pilar fundamental para la consecución de los fines estatales de asegurar la convivencia pacífica y la vigencia de un orden justo y advirtiéndose, del mismo modo, que el acto de divulgación en este caso responde a una finalidad constitucionalmente legítima, el precepto examinado es exequible."

En lo que se relaciona con los datos públicos y el registro civil de las personas, su naturaleza hace que no estén sujetos al principio de autorización. La información pública es aquella que puede ser obtenida sin reserva alguna, entre ella los documentos públicos, habida cuenta el mandato previsto en el artículo 74 de la Constitución Política. Esta información puede ser adquirida por cualquier persona, sin necesidad de autorización alguna[13].

De lo establecido por el artículo 10 de la Ley 1581 de 2012 y lo expuesto en la sentencia C-748 de 2011 de la Corte Constitucional, la Sala extrae los siguientes aspectos relevantes para resolver la consulta:

i) El consentimiento del titular de la información es un presupuesto para la legitimidad de los procesos de administración de datos personales:

ii) No existe una autorización tácita para la administración de dichos datos;

iii) Sin embargo, el propio legislador consagró una serie de hipótesis en las cuales es posible acceder a información personal sin la autorización previa de su titular;

iv) Dentro de las hipótesis señaladas por el legislador, se encuentra la información requerida por una autoridad pública o administrativa en el ejercicio de sus funciones legales, hipótesis que es concordante, además, con lo establecido en el artículo 13 de la Ley 1581 de 2012[14];

v) El acceso a la información por parte de dichas autoridades está sujeto a la observancia de requisitos legales y, en ningún caso puede realizarse de manera abusiva. De esta manera, el dato personal puede ser requerido por la autoridad pública o administrativa bajo el condicionamiento de que la petición se sustente en la conexidad directa con alguna de sus funciones.

vi) La conexidad que legitima la solicitud de información no corresponde a un asunto discrecional o de conveniencia, sino que debe fundamentarse en «una clara y específica competencia funcional de la entidad».

vii)Asimismo, la autoridad administrativa que acceda a la información debe cumplir con las obligaciones de protección y garantía al derecho fundamental de habeas data.

---

[13] Corte Constitucional. Sentencia del 6 de octubre de 2011, C-748/11.

[14] Artículo 13. Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:
a) A los Titulares, sus causahabientes o sus representantes legales;
b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
c) A los terceros autorizados por el Titular o por la ley.

viii) Con fundamento en el artículo 74 de la Constitución Política, el acceso a datos de naturaleza pública tampoco requiere de autorización previa.

Es claro para la Sala que de conformidad con los antecedentes de la consulta, la Procuraduría General de la Nación, como responsable del tratamiento de datos, debe cumplir con las exigencias legales para el tratamiento de los datos personales a los que pretende acceder.

De esta manera, la Procuraduría General de la Nación planea usar los datos del RUNT para el ejercicio de su función preventiva. Así, en el oficio 430-20 del 19 de junio de 2020, la Procuraduría manifestó al Ministerio de Transporte su interés en acceder a dichos datos como parte de un modelo analítico que pretende desarrollar para identificar incrementos patrimoniales injustificados:

> La Procuraduría General de la Nación tiene interés en acceder a la información contenida en el RUNT para perseguir, desde su función disciplinaria, el incremento patrimonial injustificado y hacer así frente, de una manera más efectiva al fenómeno de corrupción que tanto daño hace a nuestro país.
>
> [...]
>
> Esos trabajos de consultoría nos han llevado a tomar la decisión de crear un modelo analítico que, desde la función preventiva encomendada por la Constitución Política a la Procuraduría, nos permitan generar alertas que sirvan para direccionar los esfuerzos disciplinarios posteriores.
>
> Respetuosos de los derechos fundamentales de todos los colombianos, que esta Entidad debe proteger, entendemos las limitaciones legales del uso de datos personales que nos impone el ordenamiento. Sin embargo, una interpretación integral del marco legal nos ha llevado a la certeza de que tanto el modelo analítico como los convenios de transferencia de información que este necesita para su funcionamiento, se ajustan al ordenamiento jurídico vigente.
>
> [...]
>
> El acceso a las bases de datos en poder del RUNT, permitiría a la Procuraduría dar un paso al frente en la lucha contra la corrupción, nutriendo el sistema que ha de crearse de valiosos insumos que nos permitirían enfocar los esfuerzos disciplinarios para que, en el marco de ese proceso legalmente regulado, y con el uso de la información semiprivada a la que podremos acceder por virtud de las órdenes jurisdiccionales que se encuentren necesarias, podamos perseguir aquellos servidores públicos que incrementen de manera injustificada su patrimonio".

Igualmente, en el oficio 434-20 del 24 de junio de 2020, la Procuraduría señaló frente al uso de los datos del RUNT:

> Esta *(sic)* datos, permiten complementar la información registrada por el funcionario público en el SIGEP, de tal manera que, en el análisis de la Procuraduría se detecten diferencias significativas que permitan determinar un incremento patrimonial injustificado.
>
> Es de resaltar que el acceso se realizará únicamente para realizar consultas vía remota desde las estaciones indicadas exclusivamente por la Procuraduría, y solo se podrá por número de cédula o NIT de los presuntos sujetos disciplinables.
>
> No obstante, para el sistema de monitoreo es necesario que la información se pueda acceder de manera masiva y que esta sea de calidad, de tal forma que

> alimente la fase pre-investigativa, permitiendo la revisión constante de los datos en el sistema y que el mismo permita determinar los posibles casos de incremento patrimonial injustificado para ser evaluados por la persona experta.

A pesar de que en las comunicaciones citadas se menciona la potestad disciplinaria de que es titular la Procuraduría General de la Nación, la cual como se afirma se encuentra reglada por procedimientos específicos, lo que realmente se pretende es que en ejercicio de la «función preventiva», se pueda acceder a datos personales consignados en el RUNT, con el fin de «crear un modelo analítico» que permita «generar alertas que sirvan para direccionar los esfuerzos disciplinarios posteriores».

En pocas palabras, se trata de un «sistema de monitoreo» para el cual se requiere acceder de manera «masiva» a los datos personales que contiene el RUNT.

Así las cosas, corresponde analizar si respecto de las funciones preventivas asignadas a la Procuraduría General de la Nación, existe «una clara y específica competencia funcional» para que ese organismo de control pueda requerir la información sobre datos personales consignados en el RUNT, sin la autorización del respectivo titular.

4. La función preventiva de la Procuraduría General de la Nación

El Ministerio Público es un órgano de control (art. 117 CP), ejercido entre otros, por el procurador general de la Nación (funcionario que es su supremo director, art. 275 CP), por los procuradores delegados y los agentes del ministerio público, a quienes les corresponde la guarda y promoción de los derechos humanos, la protección del interés público y la vigilancia de la conducta oficial de quienes desempeñan funciones públicas (art. 118 CP).

Si bien las funciones básicas del procurador general de la Nación, sus delegados y agentes se encuentran previstas en el artículo 277 CP, allí no se alude explícitamente a la «función preventiva», aunque sí se confiere la función de «exigir a los funcionarios públicos y a los particulares la información que considere necesaria» (núm. 9).

Es preciso indicar que la consulta elevada no está referida al ejercicio de la potestad disciplinaria de la Procuraduría General de la Nación, ni a los procedimientos bajo los cuales esta se ejerce, sujetos a reglas propias, incluida por supuesto la competencia para decretar y practicar pruebas en el curso de una actuación disciplinaria, por lo que ninguno de esos aspectos será objeto de análisis por la Sala.

De esta manera, para dilucidar en qué consiste la «función preventiva» de ese órgano de control, resulta necesario acudir al Decreto Ley 262 de 2000, «*por el cual se modifican la estructura y la organización de la Procuraduría General de la Nación y del Instituto de Estudios del Ministerio Público; el régimen de competencias interno de la Procuraduría General; se dictan normas para su funcionamiento; se modifica el régimen de carrera de la Procuraduría General de la Nación, el de inhabilidades e incompatibilidades de sus servidores y se regulan las diversas situaciones administrativas a las que se encuentren sujetos».*

Respecto de las funciones del procurador general de la Nación, se alude a las preventivas en el artículo 7, *ibidem*:

> **ARTÍCULO 7. Funciones.** El Procurador General de la Nación cumple las siguientes funciones:
> (…)
> 2. Formular las políticas generales y criterios de intervención del Ministerio Público en materia de control disciplinario, vigilancia superior con fines preventivos, actuación ante las autoridades administrativas y judiciales y centros de conciliación, y promoción, protección y defensa de los derechos humanos.
>
> 36. Expedir, como supremo director del Ministerio Público, las directivas y circulares que resulten conducentes para el ejercicio de las funciones públicas y para prevenir la comisión de faltas disciplinarias de los servidores públicos. (Se subraya).

Por su parte, los procuradores delegados ejercen varias funciones, entre ellas, las preventivas:

> **ARTÍCULO 23. Funciones.** Las procuradurías delegadas ejercerán funciones preventivas y de control de gestión, disciplinarias, de protección y defensa de los derechos humanos y de intervención ante las autoridades administrativas y judiciales, de conformidad con la Constitución Política, las leyes y lo dispuesto en este título, cuando lo determine el Procurador General en virtud de las facultades contenidas en el artículo 7 de este decreto (…).

El artículo 24 del Decreto 262 establece las diferentes funciones preventivas que cumplen los procuradores delegados, las cuales serán analizadas más adelante.

A su vez, los procuradores judiciales también tienen asignadas funciones preventivas, así:

> **ARTÍCULO 37. Funciones.** Los procuradores judiciales ejercerán funciones preventivas y de control de gestión, disciplinarias, de protección y defensa de los derechos humanos y de intervención ante las autoridades administrativas y judiciales, de conformidad con lo dispuesto en la Constitución Política, las leyes y en este capítulo cuando lo determine el Procurador General en virtud de las facultades contenidas en el artículo 7 de este decreto.

Y en cuanto a las funciones preventivas estas se desarrollan de la siguiente manera:

> **ARTÍCULO 38. Funciones preventivas y de control de gestión.** Los procuradores judiciales tienen las siguientes funciones preventivas y de control de gestión:
>
> 1. Interponer las acciones populares, de tutela, de cumplimiento, de nulidad de actos administrativos y nulidad absoluta de los contratos estatales, y las demás que resulten conducentes para asegurar la defensa del orden jurídico, en especial las garantías y los derechos fundamentales, sociales, económicos, culturales, colectivos o del ambiente o el patrimonio público.
>
> 2. Intervenir en el trámite especial de tutela que adelanten las autoridades judiciales ante quienes actúan, cuando sea necesario en defensa del orden jurídico, del patrimonio público o de los derechos y garantías fundamentales, sociales, económicos, culturales, colectivos o del ambiente, de conformidad con lo previsto en el numeral 7 del artículo 277 de la Constitución Política.
>
> 3. Las demás que les asigne o delegue el Procurador General.

De esta forma, tanto el procurador general de la Nación, como los procuradores delegados y los judiciales, tienen asignadas funciones preventivas. Las de estos

últimos corresponden, esencialmente, a interponer acciones constitucionales o intervenir en acciones de tutela.

Queda por analizar las funciones preventivas de los procuradores delegados, las cuales se establecen en el artículo 24 del Decreto 262 de 2000, en los siguientes términos:

> **ARTÍCULO 24. Funciones preventivas y de control de gestión.** Sin perjuicio de lo dispuesto en la ley, las procuradurías delegadas tienen las siguientes funciones de vigilancia superior, con fines preventivos y de control de gestión:
>
> 1. Velar por el cumplimiento de las disposiciones constitucionales y legales, así como de las decisiones judiciales y administrativas.
> 2. Velar por el ejercicio diligente y eficiente de las funciones públicas y ejercer control de gestión sobre ellas, para lo cual podrán exigir a los servidores públicos y a los particulares que cumplan funciones públicas la información que se considere necesaria.
> 3. Ejercer, de manera selectiva, control preventivo de la gestión administrativa y de la contratación estatal que adelantan los organismos y entidades públicas.
> 4. Vigilar la gestión de las procuradurías distritales.
> 5. Intervenir ante las autoridades públicas, cuando sea necesario para defender el orden jurídico, el patrimonio público, las garantías y los derechos fundamentales, sociales, económicos, culturales, colectivos o del ambiente, así como los derechos de las minorías étnicas.
> 6. Realizar visitas a las entidades estatales o particulares que cumplen función pública, a solicitud de cualquier persona u oficiosamente, cuando sea necesario para proteger los recursos públicos y garantizar el cumplimiento de los principios que rigen la función pública.
> 7. Ejercer, de oficio o a petición de parte, de manera temporal o permanente, vigilancia superior de las actuaciones judiciales.
> 8. Ejercer vigilancia sobre los bienes y recursos de la Nación, especialmente sobre las islas, islotes, cayos y morros, el subsuelo, el mar territorial, la zona contigua, la plataforma continental, la zona económica exclusiva y el patrimonio arqueológico, histórico y cultural, y procurar la adopción inmediata de las medidas que resulten necesarias para su protección por parte de los funcionarios encargados de su custodia y administración.
> 9. Vigilar el cumplimiento de las políticas relacionadas con la descentralización administrativa y ordenamiento territorial, el ejercicio de la autonomía y de los derechos de las entidades territoriales y promover las acciones pertinentes cuando se desborden los límites de la autonomía o se desconozcan los derechos de las entidades territoriales.
> 10. Velar porque se haga efectiva la responsabilidad patrimonial de los servidores o ex servidores públicos y los particulares por cuya conducta pueda ser o haya sido declarada responsable una entidad estatal, mediante sentencia proferida por el Consejo de Estado, conforme a la Constitución y la ley.
> 11. Velar porque se haga efectiva la responsabilidad patrimonial de los servidores o ex servidores públicos y los particulares, cuando se hubieren conciliado ante el Consejo de Estado pretensiones de la misma naturaleza y de ello se deriven obligaciones patrimoniales a cargo de las entidades estatales.
> 12. Velar por la eficiente prestación de los servicios públicos.
> 13. Velar por la defensa de los derechos del consumidor y usuarios de los servicios públicos domiciliarios.
> 14. Vigilar el cumplimiento y la cancelación oportuna de las órdenes de captura.
> 15. Llevar un registro actualizado de las sentencias proferidas contra las entidades públicas del orden nacional, mediante las cuales se les condene al pago o la devolución de una cantidad líquida de dinero, así como de los acuerdos conciliatorios celebrados por éstas, y exigir a los servidores públicos la inclusión de las partidas correspondientes, de conformidad con lo dispuesto en el Código Contencioso Administrativo y en la Ley Anual del Presupuesto General de la Nación.

16. Las demás que les asigne o delegue el Procurador General.

Adicionado numerales 17 y 18 por el Artículo 1 del Decreto 2246 de 2011:

17. Apoyar a las víctimas, con el fin de que puedan tener acceso a la verdad, la justicia y reparación, por daños que hayan sufrido con ocasión del conflicto armado interno; así mismo brindar atención, orientación, seguimiento y apoyo en la gestión que adelanten y requieran en su gestión ante las entidades competentes encargadas de adelantar los respectivos trámites.
18. Adoptar o sugerir las medidas pertinentes ante las autoridades competentes, tendientes a evitar la suplantación o reclamación ilegal por parte de quienes no ostentando la condición de víctimas se presentan ante las autoridades como víctimas.

Como puede apreciarse, son múltiples las actividades que pueden adelantar los procuradores delegados para el ejercicio de la función preventiva y de control de gestión que les ha sido asignada. No obstante, su descripción es genérica y sin especificar una noción legal de lo que se entendería por «función preventiva», lo que lleva a una necesaria labor de interpretación.

El adjetivo preventivo/va, en su sentido natural y obvio, corresponde a «que previene»; prevenir, por su parte, tiene siete acepciones, destacándose: «prever, conocer con anticipación un daño o perjuicio», «precaver o impedir algo», o «advertir, informar o avisar a alguien de algo»[15].

Por su parte, revisada la «Guía preventiva» de la Procuraduría General de la Nación[16] (en adelante, PGN), se aprecia un glosario que en relación con lo que puede entenderse por «función preventiva», acoge varias de las acepciones naturales de la palabra, a saber:

> Función preventiva. Es la función misional de la Procuraduría General de la Nación a través de la cual la entidad busca anticiparse y evitar la ocurrencia de hechos que afecten los derechos, mediante la detección y advertencia temprana de riesgos en la gestión pública. De igual manera promueve el respeto de las garantías de los derechos constitucionales.
>
> La función preventiva comprende las actuaciones que se realizan con fines preventivos y de control de gestión [Se resalta].

En el mismo documento refiere las actividades preventivas en los siguientes términos:

> Actividades preventivas. Son el conjunto de acciones que realizan los operadores en el ejercicio de la función preventiva con el fin de evitar o mitigar hechos que vulneren los derechos de las personas en el marco de los diferentes escenarios y tipos de actuación.

---

[15] https://dle.rae.es/prevenir. **1.**tr. Preparar, aparejar y disponer con anticipación lo necesario para un fin.
2.tr. Prever, ver, conocer de antemano o con anticipación un daño o perjuicio.
3.tr. Precaver, evitar, estorbar o impedir algo.
4.tr. Advertir, informar o avisar a alguien de algo.
5.tr. Imbuir, impresionar, preocupar a alguien, induciéndolo a prejuzgar personas o cosas.
6. tr. Anticiparse a un inconveniente, dificultad u objeción.
7. prnl. Disponer con anticipación, prepararse de antemano para algo. Consultado el 27 de abril de 2021.
[16] https://apps.procuraduria.gov.co/gp/index.html

Por su parte la función de «control de gestión», tampoco es definida en el Decreto Ley 262 de 2000. En la citada «Guía preventiva» de la PGN, se encuentra lo siguiente:

> Control. Actividad de verificación que efectúa la PGN sobre la gestión pública, que implica la interacción directa con el sujeto vigilado, con el fin de requerir el cumplimiento de la normatividad vigente, el respeto de los principios que orientan la función administrativa, de los derechos humanos o recursos públicos involucrados

Ahora bien, en el Decreto 262 la única mención expresa a solicitudes de información aparece en el numeral 2 de la siguiente manera:

> 2. Velar por el ejercicio diligente y eficiente de las funciones públicas y ejercer control de gestión sobre ellas, para lo cual podrán exigir a los servidores públicos y a los particulares que cumplan funciones públicas la información que se considere necesaria.

La palabra velar, tiene diez acepciones en el diccionario, pero las más aproximadas al caso que ocupa la atención de la Sala corresponden a «4. [o]bservar atentamente algo», o «7. [c]uidar solícitamente de algo».

De esta forma la PGN, dentro de su función preventiva, observa o cuida el ejercicio diligente de **las funciones públicas**, con el objeto de anticiparse, evitar, mitigar la ocurrencia de hechos que afecten los derechos de las personas o el patrimonio público. Y en desarrollo de tal labor preventiva puede exigir a los servidores públicos y a los particulares que cumplan funciones públicas «la información que se considere necesaria». Cabe destacar que en la «Guía Preventiva», la manera de solicitar dicha información se da a través de lo que denomina requerimientos[17].

Nótese que la función preventiva que se comenta alude al «ejercicio de la función pública» correspondiente, y respecto de los servidores públicos y los particulares que cumplan la función, a quienes se les puede realizar el requerimiento de información.

En consecuencia, la «clara y específica competencia funcional», exigida por la ley y la jurisprudencia, corresponde a que la PGN puede solicitar información a los servidores públicos y los particulares que cumplan la función pública respecto de la cual se está ejerciendo la función preventiva, con el objeto de anticiparse, evitar, mitigar la ocurrencia de hechos que afecten los derechos de las personas o el patrimonio público en desarrollo de dicha función pública. Claramente corresponde a una información puntual o específica requerida para el ejercicio de la función preventiva, tendiente a evitar el riesgo identificado por la PGN, por lo que la solicitud de información no puede tener el carácter de «masiva».

Además, la información que puede requerir la PGN es únicamente sobre las actividades que corresponden a la función pública, sin que tal facultad se extienda a que ese organismo de control solicite información relacionada con los datos personales consignados en el RUNT, sin la autorización del respectivo titular.

---

[17] «• Requerimientos: se refiere a solicitudes de actuación o de información dirigidos a las distintas entidades públicas y/o privadas, en desarrollo de la función preventiva. Estos requerimientos pueden realizarse de manera formal o a través de diferentes medios (comunicación escrita, telefónica, correo electrónico, etc)».

Concluye entonces la Sala, que en ejercicio de la función preventiva la PGN no puede acceder masivamente a los datos personales (privados, semiprivados y sensibles) que reposan en una base de datos administrada por una entidad pública, o por particulares que cumplan funciones públicas, puesto que tal solicitud no corresponde a una «clara y específica competencia funcional» que le haya sido otorgada por la ley.

5. El RUNT y los datos que incorpora

El Registro Único Nacional de Tránsito se encuentra regulado en las Leyes 769 de 2002 (artículo 8 y ss.) y 1005 de 2006 (artículo 1º y ss.), es un sistema de información que:

> [I]ncorpora lo relacionado con el registro de automotores, conductores, licencias de tránsito, empresas de transporte público, infractores, accidentes de tránsito, seguros, remolques y semirremolques, maquinaria agrícola y de construcción autopropulsada y de personas naturales o jurídicas que prestan servicio al sector transporte[18].

En términos generales, el RUNT desarrolla tres procesos principales: i) valida información, ii) autoriza la realización de trámites por los organismos de tránsito y iii) registra actuaciones.

El RUNT está conformado por los siguientes registros:

- Registro Nacional de Automotores (RNA).
- Registro Nacional de Conductores (RNC).
- Registro Nacional de Empresas de Transporte público y privado (RNET).
- Registro Nacional de Licencias de Tránsito (RNLT).
- Registro Nacional de Infracciones de Tránsito y Transporte (RNITT).
- Registro Nacional de Centros de Enseñanza Automovilística (RNCEA).
- Registro Nacional de Seguros (RNS).
- Registro Nacional de Personas Naturales y/o Jurídicas que prestan servicios al sector del tránsito (RNPNJ).
- Registro Nacional de Remolques y Semirremolques (RNRYS).
- Registro Nacional de Accidentes de Tránsito (RNAT).
- Registro Nacional de Maquinaria Agrícola y de Construcción Autopropulsada (RNMA).

Es importante señalar que, de acuerdo con lo consagrado expresamente por el artículo 9º de la Ley 769 de 2002, la información contenida en el RUNT es de naturaleza pública[19].

---

[18] Consejo de Estado. Sala de Consulta y Servicio Civil. Bogotá, D. C. Decisión del 24 de octubre de 2018. Radicación número: 11001-03-06-000-2018-00151-00(C). Véase igualmente: Ministerio de Transporte. Oficio 20151340043451 del 20 de febrero de 2015.

[19] «Toda la información contenida en el RUNT será de carácter público». Asimismo, la Sala de Consulta y Servicio Civil ha señalado: El RUNT es de carácter público y busca mantener actualizada, centralizada y validada la información sobre el sector de tránsito y transporte. Este sistema de información electrónico se alimenta de la información reportada por los organismos de tránsito y por la Federación Colombiana de Municipios, a través del SIMIT. Consejo de Estado. Sala de Consulta y Servicio Civil. Bogotá, D. C. Decisión del 24 de octubre de 2018. Radicación número: 11001-03-06-000-2018-00151-00(C).

Con todo, la Superintendencia de Industria y Comercio ha señalado que, con base en el artículo 3º del Decreto Reglamentario 1377 de 2013[20], hoy compilado en el artículo 2.2.2.25.1.3. del Decreto 1074 de 2015, puede existir información que, a pesar de estar contenida en un documento público, no tenga dicha calidad, sino que corresponda a información privada, semiprivada o sensible. Así, en la Resolución 41510 de 2014, por medio de la cual impuso una sanción por violaciones a la Ley 1581 de 2012, la Superintendencia indicó:

> Tal y como lo menciona la citada definición [artículo 3 del Decreto 1377, dato público], el dato público tiene un carácter residual, pues para que la información tenga dicha categorización el dato no puede tener características que lo hagan privado, sensible, ni semiprivado. Adicionalmente y sobre el particular, vale la pena hacer referencia a la definición del dato semiprivado contenida en el literal g) del artículo 3 de la Ley 1266 de 2008, el cual establece que son aquellos que "(… no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino cierto sector o grupo de personas (…)".
>
> Visto lo anterior, el Despacho encuentra que si bien es cierto la información contenida en la tarjeta de propiedad de un vehículo en su mayoría es de carácter público por tratarse de un documento de dicha naturaleza, no sucede así con la totalidad de los datos incorporados a ésta, pues se observa que en la misma se incluye información referente a la limitación de la propiedad del bien mueble, datos que indican la entidad financiera a la cual le fue otorgada la prenda del vehículo, información que de acuerdo a las definiciones antes referenciadas, corresponde a un dato semiprivado, toda vez que es información que interesa no solo a su titular sino a un grupo de personas o a la sociedad en general, en tal virtud no se puede acceder a ella son contar con la autorización previa y expresa de su titular.
>
> De otro lado, al consultar la página web del Registro Único Nacional de Tránsito (RUNT), se determinó que, tal y como lo indica la investigada, efectivamente se puede tener acceso a los datos generales y técnicos de un vehículo, e incluso a los datos referentes a la licencia de tránsito de un titular, sin embargo, la limitación a la propiedad del bien no es puesta al conocimiento público de cualquier ciudadano[21].

Lo anterior, es concordante con lo establecido en el artículo 6º de la Ley 1712 de 2014, disposición que incluye dentro del concepto de información pública clasificada los datos privados y semiprivados:

> c) Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias

---

[20] «por el cual se reglamenta parcialmente la Ley 1581 de 2012»

[21] Asimismo, la Corte Constitucional ha señalado: La clasificación de la información en pública, pública clasificada y pública reservada, recoge una categorización tradicionalmente empleada para delimitar el derecho a la información pública.
Dado el margen de configuración con que cuenta el legislador en esta materia, es compatible con la Carta la opción tomada por el legislador. Si bien pudo haber escogido otra categorización con el fin de determinar frente a qué tipo de información o documentos pueden establecerse restricciones al derecho de acceso de información pública, la terminología elegida no se opone a nuestro ordenamiento, y de hecho es compatible con el lenguaje empleado en otras leyes estatutarias sobre el derecho al habeas data.
Así por ejemplo, cuando reguló el derecho al hábeas data y la protección de los datos personales, el legislador estatutario optó por una terminología distinta, pero armónica con la contenida en el proyecto de ley, mediante la cual se restringe la posibilidad de acceso a la información. En efecto, en el literal (c) dentro de la categoría de información pública clasificada quedarían todos los datos privados, semiprivados o sensibles a los que hacen referencia las leyes estatutarias 1266 de 2008 y 1581 de 2012, cuya difusión afecta gravemente del derecho a la intimidad de las personas. Corte Constitucional. Sentencia del 9 de mayo de 2013, C-274/13.

> legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;
>
> d) Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Hecha la anterior precisión, pasará la Sala a analizar la información que puede entregarse a una entidad pública.

6. La información susceptible de ser entregada a la entidad pública

El ministerio consultante pregunta también a la Sala sobre la naturaleza de la información susceptible de ser entregada a la entidad pública, a la luz de lo dispuesto en el literal a) del artículo 10 de la Ley 1581 de 2012.

Establecido que en virtud de la norma citada es posible, sin la autorización previa del titular, la entrega de información a una autoridad pública cuando así lo requiera esta para el cumplimiento de sus funciones, con las salvedades señaladas en este concepto, resulta necesario determinar, tal como lo pregunta el ministerio consultante, el tipo de información que puede ser transmitida o entregada.

Para resolver este interrogante, es necesario referirse a los conceptos de datos sensibles, públicos, privados y semiprivados.

Los datos sensibles fueron definidos expresamente por el artículo 5º de la Ley 1581 de 2012 en los siguientes términos:

> Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos[22].

Debido a que la Ley 1581 de 2012 no se refirió a los conceptos de datos públicos, privados y semiprivados, resulta necesario acudir a las definiciones que sobre estos términos estableció la Ley 1266 de 2008[23]. Así, el artículo 3º dispone:

---

[22] El artículo 2.2.2.25.1.3. del Decreto 1074 de 2015 define el dato sensible así: 3. Datos sensibles. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

[23] Ahora bien, es cierto que el propio legislador estatutario adoptó algunas de estas clasificaciones, como la de datos sensibles, cuyo tratamiento se prohíbe con algunas excepciones en el artículo 6 del proyecto. Para poder dar sentido a este precepto, a juicio de la Sala, basta con acudir a las definiciones elaboradas por la jurisprudencia constitucional o a las definiciones de otros preceptos legales, como la Ley 1266, cuyo artículo 3 dispone: […] En este orden de ideas, dado que la clasificación de los datos personales no es un elemento indispensable de la regulación y, dicho vacío en todo caso puede ser remediado acudiendo a la jurisprudencia constitucional y a otras definiciones legales, especialmente al artículo 3 de la Ley 1266, en virtud del principio de conservación del derecho, el literal c) será declarado exequible en este respecto. Corte Constitucional. Sentencia del 6 de octubre de 2011, C-748/11.

> f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas[24].
>
> g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.
>
> h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Ahora bien, en el caso específico del RUNT, teniendo en cuenta que este contiene información pública, es necesario referirse a los conceptos de: a) información, b) información pública, c) información pública clasificada, y d) información pública reservada, los cuales fueron definidos de manera expresa por el artículo 6º de la Ley 1712 de 2014:

> a) Información. Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen;
>
> b) Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal;
>
> c) Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;
>
> d) Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

La jurisprudencia se ha referido a la relación que existe entre los conceptos de información pública, pública clasificada y pública reservada con los datos públicos, privados, semiprivados y sensibles. Así, la Corte Constitucional señaló en la sentencia C-276 de 2019:

> En ese sentido, la posibilidad de prever la reserva de la información personal responde necesariamente a una gradación, que está definida en virtud de la intensidad de la afectación del derecho a la intimidad. Así, los datos sensibles o reservados, entre los que se destacan la orientación e identidad sexual, la historia clínica, la identificación política o religiosa y los hábitos de la persona, en aquellos casos que dicha información conste en registros administrados por las autoridades

[24] El artículo 2.2.2.25.1.3. del Decreto 1074 de 2015 define el dato público así: 2. Dato público. Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

> del Estado, tienen la condición de información pública clasificada y, por lo mismo, objeto de reserva según el régimen jurídico antes explicado. En los demás casos, esto es, respecto de aquella información personal que no tenga carácter público, los datos pertenecerán a la categoría de semiprivados, por lo que su divulgación resultará constitucionalmente admisible cuando se cumplan determinadas condiciones, como la verificación sobre el interés público que justifica la circulación del dato, la autorización del titular de éste en su divulgación o la concurrencia de orden judicial[25].

Ahora bien, frente a la información que puede ser transferida a una autoridad pública, la Sala señala lo siguiente:

i) Datos públicos: por su naturaleza pública y teniendo en cuenta lo dispuesto en el artículo 74 de la Constitución Política, a este tipo de datos puede acceder cualquier persona. En consecuencia, pueden ser entregados a una autoridad administrativa que los requiera para el cumplimiento de sus funciones.

En este sentido, la Corte Constitucional ha señalado:

> 3.4.1.1. En primer lugar, la información pública, calificada como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si se trata de información general o personal. En este grupo, pueden incluirse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; así como los datos sobre el estado civil de las personas o sobre la conformación de la familia[26].

ii) Datos semiprivados: la Corte Constitucional ha concluido que la información semiprivada, al ser información que está sometida a un grado mínimo de limitación, puede ser obtenida y ofrecida por una autoridad administrativa en cumplimiento de sus funciones:

> 3.4.1.2. La información semi-privada, hace referencia a aquella de carácter personal o impersonal que no está contemplada en la categoría anterior [información pública] y que para su acceso o conocimiento se requiere un grado mínimo de limitación. En ese sentido, la misma solo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas[27].

En el mismo sentido, en otra oportunidad indicó:

> La **información semiprivada** es aquella información personal o impersonal cuyo acceso presenta un grado mínimo de limitación, de modo que puede ser obtenida en virtud de orden de autoridad administrativa en ejercicio de sus funciones o en el marco de un proceso de administración de datos personales, precedido de la autorización del titular. Ejemplos de esta información son los datos relativos a la seguridad social o aquella de contenido financiero, comercial y crediticio[28].

---

[25] Corte Constitucional. Sentencia del 19 de junio de 2019, C-276 de 2019.
[26] Corte Constitucional. Sentencia del 12 de febrero de 2015, T-058/15.
[27] Ibidem.
[28] Corte Constitucional. Sentencia del 19 de junio de 2019, C-276/19. Para la Superintendencia de Industria y Comercio, los corres electrónicos personales corresponden a un dato semiprivado: Con lo cual se concluye que los correos electrónicos que han sido “recopilados” no son en su totalidad correos institucionales o relacionados con la profesión u oficio de las personas, sino que corresponden a datos semiprivados al tratarse de cuentas de uso personal.

iii) Datos privados: a diferencia de la información pública y semiprivada, los datos privados no pueden ser ofrecidos ni obtenidos por una autoridad administrativa que los requiera para el cumplimiento de sus funciones. Lo anterior, por tratarse de información que se enmarca en el ámbito puramente privado:

> 3.4.1.3. Por otra parte, la información privada puede tener contenidos personales o no y por encontrarse en un ámbito puramente privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Como ejemplos, se exponen los libros de los comerciantes, los documentos privados, las historias clínicas, los datos obtenidos en razón de la inspección a un domicilio o aquellos que se obtienen con posterioridad a la práctica de pruebas en procesos penales sujetos a reserva[29].

iv) Datos sensibles: estos datos no pueden ser entregados a otra autoridad administrativa en el cumplimiento de sus funciones. Lo anterior, teniendo en cuenta lo dispuesto por el artículo 6º de la Ley 1581 de 2012, disposición que establece, como regla general el no tratamiento de los mismos:

> **Artículo 6°**. Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:
>
> a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
>
> b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
>
> c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
>
> d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
>
> e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares[30].

Lo expuesto se afirma dado que el correo electrónico de uso personal, no es un dato público ya que no hay ley que así lo determine, pues son datos que pueden interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, por ejemplo, para efectos del envío de facturas electrónicas para el pago de servicios, el envío de constancias para el pago de las EPS, la participación en foros de internet o como dato de contacto en un aviso clasificado. Por lo anterior, tales datos personales tienen el carácter de datos semiprivados. Superintendencia de Industria y Comercio. Resolución número 15339 del 31 de marzo de 2016, por el cual se impone una sanción y se dispone la suspensión de las actividades relacionadas con el tratamiento de información personal.

[29] Corte Constitucional. Sentencia del 12 de febrero de 2015, T-058/15.

[30] Adicionalmente, el artículo 2.2.2.25.2.3 del Decreto 1074 de 2015 dispone: *De la autorización para el Tratamiento de datos personales sensibles.* El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley.
En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6° de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:

Como puede observarse, el acceso de las autoridades administrativas a información sensible para el cumplimiento de sus funciones no hace parte de las excepciones establecidas por el legislador[31]. Por lo tanto, no es posible el acceso de las referidas autoridades a esta información.

En esta dirección, la Corte Constitucional ha indicado:

> Por último, la **información reservada** corresponde a los datos sensibles, la cual no está sujeta a divulgación al estar vinculada al núcleo esencial de los derechos a la libertad, la dignidad y la intimidad del sujeto concernido[32].

En suma, la información que puede entregarse a una autoridad administrativa sin la autorización del titular de los datos personales es aquella que corresponde a datos públicos y semiprivados. En este último caso, se requiere que la información sea necesaria para el cumplimiento de sus funciones.

En lo que respecta a los datos privados y sensibles, a ellos no puede acceder la autoridad sin la autorización del titular.

7. Entrega de la información de manera anónima

El Ministerio de Transporte pregunta a la Sala si, con el propósito de proteger el derecho fundamental de habeas data de los titulares, es posible, inicialmente, entregar la información de forma de manera anónima, y, una vez se identifique una alerta de incremento patrimonial injustificado, proveer una información más específica.

Para responder a este interrogante, resulta pertinente tomar en consideración lo dispuesto en el artículo 21 de la Ley 1712 de 2014[33], norma relativa a la divulgación parcial de la información:

---

1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.
Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.

[31] Frente a esta norma, la Corte Constitucional señaló: El segundo contenido normativo del artículo 6, de otro lado, establece excepciones a la proscripción de tratamiento de datos sensibles. Antes de examinar la constitucionalidad de cada hipótesis, la Sala estima necesario hacer las siguientes precisiones:
Como se indicó en apartes previos, la prohibición de tratamiento de datos sensibles es una garantía del habeas data y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana. Sin embargo, en ciertas ocasiones el tratamiento de tales datos es indispensable para la adecuada prestación de servicios -como la atención médica y la educación- o para la realización de derechos ligados precisamente a la esfera íntima de las personas -como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión. Las excepciones del artículo 6 responden precisamente a la necesidad del tratamiento de datos sensible en dichos escenarios.
Ahora bien, como se trata de casos exceptuados y que, por tanto, pueden generar altos riesgos en términos de vulneración del habeas data, la intimidad e incluso la dignidad de los titulares de los datos, los agentes que realizan en estos casos el tratamiento tienen una responsabilidad reforzada que se traduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y los deberes del título VI. Esa mayor carga de diligencia se deberá también traducir en materia sancionatoria administrativa y penal.
Finalmente, las excepciones, en tanto limitaciones de alcance general al derecho al habeas data, al igual que en el caso de las excepciones del artículo 2, deben ser desarrolladas por el legislador estatutario. Corte Constitucional. Sentencia del 6 de octubre de 2011, C-748/11.

[32] Corte Constitucional. Sentencia del 19 de junio de 2019, C-276/19.

> **Artículo 21**. Divulgación parcial y otras reglas. En aquellas circunstancias en que la totalidad de la información contenida en un documento no esté protegida por una excepción contenida en la presente ley, debe hacerse una versión pública que mantenga la reserva únicamente de la parte indispensable. La información pública que no cae en ningún supuesto de excepción deberá ser entregada a la parte solicitante, así como ser de conocimiento público. La reserva de acceso a la información opera respecto del contenido de un documento público pero no de su existencia.
>
> Ninguna autoridad pública puede negarse a indicar si un documento obra o no en su poder o negar la divulgación de un documento, salvo que el daño causado al interés protegido sea mayor al interés público de obtener acceso a la información.
>
> Las excepciones de acceso a la información contenidas en la presente ley no aplican en casos de violación de derechos humanos o delitos de lesa humanidad, y en todo caso deberán protegerse los derechos de las víctimas de dichas violaciones.

Esta norma tiene como propósito permitir el acceso a documentos que contienen tanto información pública, como información clasificada o reservada. De esta suerte, hace posible el acceso a aquella información que no está sujeta a una excepción o reserva constitucional o legal. Asimismo, la divulgación parcial armoniza el principio de máxima divulgación con otros derechos constitucionales como el de habeas data e intimidad, entre otros. En esta dirección, la Corte Constitucional ha señalado:

> El artículo 21 recoge la posibilidad de permitir el acceso a documentos que contengan simultáneamente información pública e información clasificada o reservada. Esta disposición ordena la creación de versiones públicas de documentos en la que sea posible conocer aquellos apartes no protegidos por excepciones o reservas constitucionales o legales, con lo cual se garantiza el principio de máxima divulgación, de manera armónica con los parámetros constitucionales que protegen el derecho a acceder a la información pública. En estas versiones públicas se debe mantener la reserva solo de la parte indispensable, y hacer entrega de tales versiones a quienes lo soliciten. Igualmente, obliga a la entrega de la información pública no amparada por ninguna regla excepcional.

De otra parte, el artículo 4 de la Ley 1581 de 2012 establece el principio de veracidad o calidad, en virtud del cual la información sujeta a tratamiento debe ser, entre otras características, completa, exacta y comprensible:

> d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

Adicionalmente, el artículo 11 de la misma ley, relativo al suministro de la información solicitada, consagra que la información que se entregue debe ser de fácil lectura, sin barreras técnicas que impidan su acceso, y corresponder a aquella que repose en la base de datos:

> **Artículo 11.** Suministro de la información. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan

---

[33] Es preciso señalar que el artículo 21 fue corregido por el artículo 3 del Decreto 1494 de 2015 en obedecimiento de la Sentencia C-274 de 2013, que realizó la revisión previa de constitucionalidad realizada de la Ley Estatutaria 1712 de 2014.

su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

Además de las normas de la Ley 1581 de 2012, debe tomarse en consideración lo dispuesto en la Ley 1712 de 2014. Lo anterior, habida cuenta de que el RUNT incorpora información pública, información pública clasificada e información pública reservada, modalidades de información que contienen, a su vez, datos privados, semiprivados o sensibles.

En esta dirección, son varias las disposiciones de la Ley 1712 de 2014 que permiten determinar la manera como debe realizarse la entrega de la información:

Así, el artículo 2º consagra el principio de máxima divulgación, en virtud del cual toda información que se encuentre en posesión o bajo el control, o custodia de un sujeto obligado es pública. Por lo tanto, su acceso puede ser reservado o limitado, siempre y cuando exista disposición constitucional o legal que así lo prevea:

> **ARTÍCULO 2o. PRINCIPIO DE MÁXIMA PUBLICIDAD PARA TITULAR UNIVERSAL.** Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley.

Por su parte, el artículo 3º establece, entre otros, los principios de transparencia, facilitación y calidad de la información. En virtud del principio de transparencia, los sujetos obligados tienen el deber de proporcionar y facilitar, en los términos más amplios posibles, el acceso a la información que tienen en su poder:

> **Principio de transparencia**. Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.

En lo que atañe al principio de facilitación, este impone a los sujetos obligados el deber de facilitar el ejercicio del derecho a la información pública, de tal suerte que deben excluir exigencias o requisitos que puedan obstruirlo o impedirlo:

> **Principio de facilitación**. En virtud de este principio los sujetos obligados deberán facilitar el ejercicio del derecho de acceso a la información pública, excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo.

En relación con el principio de calidad, toda información de interés público debe ser, entre otras características, completa, procesable y estar disponible en formatos accesibles:

> **Principio de la calidad de la información**. Toda la información de interés público que sea producida, gestionada y difundida por el sujeto obligado, deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad.

Por su parte, el artículo 4º de la Ley 1712 de 2014, relativo al concepto del derecho al acceso a la información pública, consagra que este solamente puede ser restringido de manera excepcional. Asimismo, dispone que los sujetos

obligados tienen el deber de responder de manera adecuada a las solicitudes de acceso:

> *Concepto del derecho*. En ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente. Las excepciones serán limitadas y proporcionales, deberán estar contempladas en la ley o en la Constitución y ser acordes con los principios de una sociedad democrática.
>
> El derecho de acceso a la información genera la obligación correlativa de divulgar proactivamente la información pública y responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes de acceso, lo que a su vez conlleva la obligación de producir o capturar la información pública. Para cumplir lo anterior los sujetos obligados deberán implementar procedimientos archivísticos que garanticen la disponibilidad en el tiempo de documentos electrónicos auténticos.
>
> **Parágrafo.** Cuando el usuario considere que la solicitud de la información pone en riesgo su integridad o la de su familia, podrá solicitar ante el Ministerio Público el procedimiento especial de solicitud con identificación reservada.

De las citadas disposiciones, es posible concluir lo siguiente respecto a la manera como debe entregarse la información requerida por una autoridad administrativa en el cumplimiento de sus funciones:

i) Por regla general, el acceso a la información que se encuentra en posesión, bajo control o custodia de una autoridad es pública.

ii) En línea con lo anterior, el acceso a dicha información solamente puede ser restringido de manera excepcional, esto es, cuando una disposición constitucional o legal así lo determine.

iii) Por consiguiente, la información pública que no se encuentre cubierta por una excepción que restrinja su acceso, debe ser entregada a la parte solicitante.

iv) Las autoridades deben responder de manera adecuada a las solicitudes de acceso a la información. En consecuencia, y dentro de los límites legales y constitucionales, deben facilitar el acceso a la información, de tal manera que no pueden establecer exigencias o requisitos que lo obstruyan o impidan.

v) La entrega de la información debe realizarse de manera completa, exacta y comprensible. Asimismo, debe ser de fácil consulta, sin barreras técnicas y corresponder a la contenida en la base de datos.

vi) Finalmente, por expreso mandato legal, es posible la divulgación parcial de información.

A la luz de las conclusiones anteriores, resulta válido afirmar que no es posible la entrega de la información del RUNT de manera anónima, pues i) los nombres y apellidos de las personas son públicos[34], ii) la información debe entregarse de

---

[34] Establecido lo anterior, es importante aclarar que un dato personal no tiene la naturaleza de dato público por el simple hecho de que se encuentre en una fuente de acceso público, como por ejemplo, avisos clasificados que se publican en medios de comunicación, redes sociales o foros en internet. De conformidad con lo establecido en la ley, como se precisó líneas atrás, el dato púbico es aquél que: (i) es calificado como tal según los mandatos de la ley o de la Constitución, como ocurre con el nombre, los apellidos y el número de cédula, y (ii) no es semiprivado, privado o sensible (carácter residual). Superintendencia de Industria y Comercio. Resolución número 15339

manera completa, exacta y comprensible, iii) ni la Constitución ni la ley autorizan la entrega anónima de información requerida por una autoridad administrativa en cumplimiento de sus funciones y iv) los responsables de la información no pueden imponer límites o exigencias que obstruyan o impidan el acceso a esta.

8. El modelo analítico y la identificación de incrementos patrimoniales como finalidades legítimas

El ministerio consultante pregunta a la Sala si el modelo analítico y el interés de identificar incrementos patrimoniales injustificados constituyen una finalidad legítima de acuerdo con la Constitución y la Ley para permitir el tratamiento y acceso a los datos personales que reposan en el RUNT

El artículo 4º de la Ley 1581 de 2012, al definir el principio de finalidad establece:

> Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

Respecto a esta definición, la Corte Constitucional señaló:

> 2.6.5.2.2. Principio de finalidad: En virtud de tal principio, el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.
>
> La definición establecida por el legislador estatutario responde a uno de los criterios establecidos por la Corporación para el manejo de las bases de datos. Sin embargo, debe hacerse algunas precisiones.
>
> Por una parte, los datos personales deben ser procesados con un propósito específico y explícito. En ese sentido, la finalidad no sólo debe ser legítima sino que la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. Cualquier utilización diversa, deberá ser autorizada en forma expresa por el Titular.
>
> [...]
>
> Así mismo, los datos personales deben ser procesados sólo en la forma que la persona afectada puede razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento previo del titular.
>
> Por otro lado, de acuerdo la jurisprudencia constitucional y los estándares internacionales relacionados previamente, se observa que el principio de finalidad implica también: (i) un ámbito temporal, es decir que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y (ii) un ámbito material, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.
>
> En razón de lo anterior, el literal b) debe ser entendido en dos aspectos.
>
> Primero, bajo el principio de necesidad se entiende que los datos deberán ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos. Es

---

del 31 de marzo de 2016, por el cual se impone una sanción y se dispone la suspensión de las actividades relacionadas con el tratamiento de información personal.

> decir, el periodo de conservación de los datos personales no debe exceder del necesario para alcanzar la necesidad con que se han registrado.
>
> [...]
>
> Segundo, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: (i) adecuados, (ii) pertinentes y (iii) acordes con las finalidades para las cuales fueron previstos[35].

Igualmente, en otra oportunidad la Corte indicó:

> Según el principio de finalidad tales actividades "*deben obedecer a un fin constitucionalmente legítimo (…) definido de forma clara, suficiente y previa.* [Por lo cual, está prohibida, por un lado] *la recopilación de información personal sin que se establezca el objetivo de su incorporación a la base de datos (…) y* [por el otro] *la recolección, procesamiento y divulgación de información personal para un propósito diferente al inicialmente previsto...*"[36].

Adicionalmente, señaló:

> Según *el principio de finalidad*, los datos, además de procurar un objetivo constitucionalmente protegido, deben conservar el propósito por el cual fueron suministrados u obtenidos, el cual está determinado generalmente por los ámbitos específicos en los que dicha operación se realiza y que en este caso es el propio de las relaciones privadas entre el titular de los datos y las entidades de la seguridad social[37].

No escapa a la Sala que la lucha contra la corrupción es un propósito que tiene fundamento en el ordenamiento jurídico colombiano[38] y constituye un imperativo de ética pública.

Ahora bien, de acuerdo con lo que obra en el expediente, la Procuraduría desea acceder a la información del RUNT como parte de una estrategia de lucha contra la corrupción, tal como lo manifestó en el oficio 430-20 del 19 de junio de 2020, transcrito en una acápite anterior de este concepto.

Para la Sala, la adopción de un modelo analítico y el interés por identificar incrementos patrimoniales son instrumentos que, en sí mismos, no justifican el acceso a la información del RUNT por parte de la Procuraduría General de la Nación, puesto que teniendo en cuenta los parámetros establecidos por la ley y la

---

[35] Corte Constitucional. Sentencia del 6 de octubre de 2011, C-748/11.
[36] Corte Constitucional. Sentencia del 21 de junio de 2012, SU458/12.
[37] Corte Constitucional. Sentencia del 5 de septiembre de 2002, T-729/02.
[38] En lo que respecta a la lucha contra la corrupción, Colombia ha suscrito varios tratados internacionales en la materia. Entre los más importantes se destacan: i) la Convención Interamericana de Lucha contra la Corrupción (Ley 412 de 1997), ii) la Convención de las Naciones Unidas de Lucha contra la Corrupción (Ley 970 de 2005), y iii) la Convención para Combatir el Cohecho de Servidores Públicos Extranjeros en Transacciones Comerciales Internacionales (Ley 1537 de 2012).
Asimismo, se promulgaron las Leyes 1474 de 2011 (Estatuto Anticorrupción), 1757 de 2015 (Promoción y Protección de la Participación Democrática), y 1778 de 2016 (Soborno Transnacional). Adicionalmente, cuenta con la Política Pública Integral Anticorrupción (PPIA), la cual fue incorporada en el Documento CONPES 167 de 2013.

jurisprudencia, no se cumpliría con el principio de finalidad. A lo anterior debe sumarse que, como se explicó anteriormente, la Procuraduría en ejercicio de su función preventiva, no está facultada para acceder a la información.

En efecto, frente a los objetivos perseguidos por el RUNT, se ha señalado:

> *¿Cuáles son los objetivos del RUNT?*
>
> • Lograr un flujo seguro de la información, desde su origen en el momento de realización de los trámites, su registro en el RUNT y su posterior consulta.
> • Hacer que el sistema de registro de Tránsito y Transporte sea uno de los modelos con los mejores niveles de servicio del país.
> • Habilitar al Estado para que, en conjunto, asegure la alta confiabilidad de la información para garantizar, entre otras, la idoneidad de los conductores y la propiedad de los vehículos.
> • Incrementar la calidad y pertinencia de la información del Ministerio de Transporte, para la definición de políticas de Planeación, Control y Regulación del Tránsito y Transporte.
> • Validar, registrar y autorizar las transacciones relacionadas con los siguientes once (11) registros:
> ○ Registro Nacional de Automotores (RNA)
> ○ Registro Nacional de Conductores (RNC)
> ○ Registro Nacional de Empresas de Transporte público y privado (RNET)
> ○ Registro Nacional de Licencias de Tránsito (RNLT)
> ○ Registro Nacional de Infracciones de Tránsito y Transporte (RNITT)
> ○ Registro Nacional de Centros de Enseñanza Automovilística (RNCEA)
> ○ Registro Nacional de Seguros (RNS).
> ○ Registro Nacional de Personas Naturales y/o Jurídicas que prestan servicios al sector del tránsito (RNPNJ)
> ○ Registro Nacional de Remolques y Semirremolques (RNRYS)
> ○ Registro Nacional de Accidentes de Tránsito (RNAT)
> ○ Registro Nacional de Maquinaria Agrícola y de Construcción Autopropulsada (RNMA) [39].

Como puede observarse, las motivaciones que justifican la recopilación y tratamiento de los datos que hacen parte del RUNT, no encuadran en el propósito alegado por la Procuraduría para acceder a los mismos, toda vez que el señalado registro no fue concebido como un instrumento para la lucha contra la corrupción, sino como un sistema de información para la adecuada administración de los datos relevantes en materia de transporte, los cuales están sujetos a la protección que la Constitución otorga a las personas -derecho al habeas data- en los términos expuestos en este concepto, en particular frente al principio de finalidad.

En mérito de lo anterior,

La Sala RESPONDE:

1. ¿Tiene facultad la Procuraduría General de la Nación en ejercicio de la competencia a prevención para a acceder masivamente a las bases de datos en administración de una entidad pública?

2. ¿La función preventiva de la Procuraduría se enmarca dentro del concepto de las (sic) excepción contenida en literales a) del artículo 10 de la Ley 1581 de 2012, que establece que no será necesaria la autorización del Titular cuando esta es "…requerida por una entidad pública o administrativa en ejercicio de sus funciones legales"?

---

[39] https://www.runt.com.co/sobre-runt/que-es-runt (visitado el 28 de abril de 2021).

3. ¿Cuál sería la extensión de esa facultad de cara a las funciones preventivas de la Procuraduría, cuya competencia se desarrolla solamente con relación a los sujetos disciplinables, y en esa medida se debe determinar si en dicho ejercicio pueden tener acceso a los datos depositados de todos los ciudadanos sin discriminación a los sujetos disciplinables?

4. ¿En el evento de ser extensiva la excepción contenida en el literal a) del artículo 10 de la Ley 1581 de 2012, a los órganos de control en especial a la Procuraduría General de la Nación, en ejercicio de la "función preventiva", en virtud del principio de finalidad, previo a recibir la información requerida deben adoptar tratamiento de datos?

6. ¿La solicitud de transmisión de la información puede ser suscrita por cualquier funcionario de la Procuraduría General de la Nación o debe ser solicitada directamente por el Procurador General, como quiera que es la autoridad encargada de iniciar, adelantar y fallar las investigaciones que por faltas disciplinarias se adelanten en contra de servidores públicos?

En ejercicio de la función preventiva, la Procuraduría General de la Nación no puede acceder masivamente a los datos personales (privados, semiprivados y sensibles) que reposan en una base de datos administrada por una entidad pública o por particulares que cumplan funciones públicas, puesto que tal solicitud no corresponde a una «clara y específica competencia funcional», que le haya sido otorgada por la ley.

Es preciso indicar que la anterior respuesta en nada refiere al ejercicio de la potestad disciplinaria de la Procuraduría General de la Nación, ni a los procedimientos bajo los cuales esta se ejerce, los cuales están sujetos a reglas especiales, que incluyen la competencia para decretar y practicar pruebas en el curso de una actuación disciplinaria, toda vez que ninguno de esos aspectos correspondía al objeto de la consulta.

5. A la luz del literal a) del artículo 10 de la ley 1581 de 2012, ¿qué información es susceptible de ser entregada a una entidad pública sin autorización del titular de los datos personales, a la entidad solicitante? ¿Solo Datos públicos? ¿datos privados? ¿Datos semiprivados? ¿Incluso datos sensibles?

La información que puede entregarse a una autoridad administrativa sin la autorización del titular de los datos personales es aquella que corresponde a datos públicos y semiprivados. En este último caso, se requiere que la información sea estrictamente necesaria para el cumplimiento de sus funciones, aspecto que, como quedó señalado, no se da en el marco de la función preventiva de la Procuraduría General de la Nación.

7. En aras de proteger el derecho de habeas data en cabeza de sus titulares, a juicio de esta Sala, ¿es el modelo analítico y el interés de identificar incrementos patrimoniales injustificados, una finalidad legítima de acuerdo con la Constitución y la Ley para permitir el tratamiento y acceso a los datos personales que reposan en el RUNT?

La adopción de un modelo analítico y el interés por identificar incrementos patrimoniales son instrumentos que, en sí mismos, no justifican el acceso a la información del RUNT por parte de la Procuraduría General de la Nación, puesto

que bajo los parámetros establecidos por la ley y la jurisprudencia constitucional, no se cumpliría con el principio de finalidad. A lo anterior debe sumarse que, como se respondió anteriormente, la Procuraduría en ejercicio de su función preventiva, no está facultada para acceder a dicha información.

8. Asimismo, en aras de proteger el derecho fundamental de habeas data de los titulares, [¿] el Ministerio de Transporte como responsable de dichos datos, podría entregar en un primer momento tal información de forma anonimizada, y una vez identificada alguna alerta de incremento patrimonial injustificado, proveer ya una información más específica?

No es posible la entrega de la información del RUNT de manera anónima, pues i) los nombres y apellidos de las personas son públicos, ii) la información debe entregarse de manera completa, exacta y comprensible, iii) ni la Constitución ni la ley autorizan la entrega anónima de información requerida por una autoridad administrativa en cumplimiento de sus funciones, y iv) los responsables de la información no pueden imponer límites o exigencias que obstruyan o impidan el acceso a esta.

Remítase al Ministerio de Transporte, y envíese copia a la Secretaría Jurídica de la Presidencia de la República

ÁLVARO NAMÉN VARGAS
Presidente de la Sala

ÓSCAR DARÍO AMAYA NAVAS
Consejero de Estado

ÉDGAR GONZÁLEZ LÓPEZ
Consejero de Estado

GERMÁN ALBERTO BULA ESCOBAR
Consejero de Estado

REINA CAROLINA SOLÓRZANO HERNÁNDEZ
Secretaria de la Sala