



CIRCULAR INTERNA 1100//

Bogotá D.C.,

PARA: Subdirectores, Directores, Direcciones Territoriales y Unidades Operativas.

DE: Jefe de Oficina Asesora Jurídica

ASUNTO: Tratamiento de datos personales y suministro de la información en cabeza del Instituto Geográfico Agustín Codazzi - IGAC.

El artículo 15 de la Constitución Política establece el derecho fundamental de las personas 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". Así mismo, determina que "en la recolección, tratamiento y circulación de datos, se respetarán la libertad y demás garantías consagradas en la Constitución".

El artículo 20 por su parte, regula el derecho a la información en condiciones de veracidad e imparcialidad y garantiza el derecho a la rectificación en condiciones de equidad.

En desarrollo de los artículos constitucionales señalados, se expidió la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 con el Régimen General de Protección de Datos Personales, así como la Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional".

Ahora bien, con el objeto de garantizar los derechos, libertades y garantías constitucionales relacionados con el tratamiento de los datos personales y el suministro de información pública, la Oficina Asesora Jurídica del Instituto Geográfico Agustín Codazzi - IGAC, en el marco de las funciones establecidas en los numerales 1, 3 y 9 del artículo 7° del Decreto Nacional 208 de 2004, fija los siguientes lineamientos:

1. Definición de dato personal

Se definen como dato personal "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables" (art. 3, Ley 1581 de 2012).

El dato personal cumple las siguientes características: "(i) está referido a aspectos exclusivos y propios de una persona natural, ii) permite identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el Titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación." (Superintendencia de Industria y Comercio, concepto 13-33980- -1-0).

2. Clasificación general de los datos personales

Dependiendo del mayor o menor grado de aceptabilidad de divulgación, los datos personales pueden ser:



Públicos: Se consideran datos públicos aquellos relativos al estado civil de las personas (número de identificación, apellidos, fecha y lugar de expedición del documento), 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 y los relativos al estado civil de las personas"* (Ley 1266 de 2008, art. 3, lit. f).

Semiprivados: Son aquellos datos que *"no tienen naturaleza 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"*. (Ley 1266 de 2008, art. 3, lit. g), la fecha y el lugar de nacimiento.

Privados: Son privados aquellos datos que *"por su naturaleza íntima o reservada sólo [son] relevante[s] para el Titular"* (Ley 1266 de 2008, art. 3, lit. h) como la historia clínica, la dirección de residencia y el teléfono.

Datos sensibles: Son sensibles aquellos datos 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."* (Decreto 1377, art. 3, num. 3). El artículo 6 *ibidem* prohíbe por regla general su tratamiento, salvo que, entre otros casos, el Titular haya dado su autorización.

Se recuerda que en virtud del artículo 7 de la Ley 1581 de 2012, **está prohibido el tratamiento de los datos personales de los niños, niñas y adolescentes, salvo que se trate de datos de naturaleza pública.** Para su tratamiento, los responsables verificarán el interés superior del menor, garantizarán sus derechos fundamentales y solicitarán la autorización de su representante legal o tutor, previo ejercicio del derecho del menor a ser escuchado. Esta opinión será valorada a partir de la madurez, autonomía y capacidad para entender el asunto.

3. Ámbito de aplicación de la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" y alcance del tratamiento.

Los principios y disposiciones de la norma son aplicables a los datos personales que se encuentren en bases de datos o archivos de entidades públicas o privadas, entendidos estos, como el conjunto o depósito organizado de datos personales que son objeto de tratamiento (art. 2, Ley 1581 de 2012).

El tratamiento por su parte, se refiere a la utilización, recolección, almacenamiento, circulación y supresión de los datos personales que se encuentren registrados en cualquier base de datos o archivos por parte de entidades públicas o privadas y en cuyo procesamiento se utilicen medios tecnológicos o manuales.

En ese sentido, el IGAC es responsable del tratamiento de los datos personales cuando decide sobre las bases de datos o su tratamiento, esto es, cuando realiza cualquier operación o conjunto de operaciones sobre datos personales como la recolección, almacenamiento, uso, suministro, circulación o supresión.

4. Principio de acceso y circulación restringida

El principio de acceso y circulación restringida indica que el tratamiento de los datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, las disposiciones de la ley y la Constitución y



los principios de su administración. En este sentido, la información personal solo podrá ser suministrada 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". (art. 13, Ley 1581 de 2012).

Sobre este aspecto, la Corte Constitucional ha determinado que el principio de acceso y circulación restringida "obliga a que la divulgación de datos personales se realice dentro de los límites específicos de la finalidad para el cual se hace el acopio de estos, de modo que está proscrita la circulación indiscriminada de los mismos" (Sentencia C-276 de 2019). Así mismo, ha reiterado que "(...) el manejo de información no pública debe hacerse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el Responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular". (Sentencia C-748 de 2011).

Por lo tanto, los datos personales que no sean de carácter público, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable y su conocimiento sea restringido a los Titulares o terceros autorizados por la ley.

5. Principio de finalidad

El principio de finalidad por su parte, determina que el tratamiento de los datos personales deberá obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. Para ello, el responsable del tratamiento informará al Titular de manera clara, suficiente y previa, la finalidad de la información recolectada.

A este respecto, la Superintendencia de Industria y Comercio ha precisado que "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 (...)" (Superintendencia de Industria y Comercio, concepto 13-33980- -1-0). Así, "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."

El principio de finalidad implica entonces, un *ámbito temporal*, es decir que el periodo de conservación de los datos personales no exceda el necesario para alcanzar la finalidad con que fueron solicitados y un *ámbito material*, el cual exige que los datos recaudados sean los estrictamente necesarios para el cumplimiento de las finalidades perseguidas, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objeto del archivo o la base de datos.

6. Principio de libertad

El principio de libertad determina que cualquier tratamiento requiere el consentimiento, previo, expreso e informado del Titular, de tal suerte que "los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento" (Artículo 4° literal c Ley 1581 de 2012).

Al respecto, la Corte Constitucional mediante Sentencia C-748 de 2011 señaló que este principio, como pilar fundamental de la administración de datos, "permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente".





Por lo anterior, el tratamiento de los datos personales solo puede realizarse cuando exista la autorización previa, expresa e informada del Titular o mandato legal o judicial, con el fin de garantizar que *"el Titular pueda conocer en dónde está su información personal, para qué propósitos ha sido recolectada y qué mecanismos tiene a su disposición para su actualización y rectificación"* (Sentencia C-748 de 2011).

7. Solicitud de autorización

Por regla general, el tratamiento de datos personales requiere el consentimiento previo, expreso e informado del Titular, salvo en los siguientes casos:

"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.*" (art. 10, Ley 1581 de 2012).

Para obtener la autorización, el Responsable informará al Titular: i) los datos personales que serán recolectados, ii) el Tratamiento al cual serán sometidos, iii) las finalidades del mismo, iv) los derechos que le asisten como Titular y v) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento (art. 12, Ley 1581 de 2012). Así mismo, indicará el carácter facultativo del Titular en materia de datos sensibles y/o de niñas, niños y adolescentes.

A su vez, deberá conservar copia de la autorización, velar por el uso de los datos de acuerdo con las finalidades para las cuales fue autorizada y conservar la información en condiciones de seguridad y confidencialidad suficientes que eviten su adulteración, acceso fraudulento o divulgación no autorizada.

En caso de que existan cambios sustanciales sobre la identificación del Responsable o la finalidad del tratamiento de los datos personales, comunicará estos cambios al Titular antes de o a más tardar al momento de implementarlos. Cuando el cambio verse sobre finalidad del tratamiento, deberá obtener una nueva autorización del Titular.

8. Suministro de datos personales

Teniendo en cuenta que el artículo 13 de la Ley 1581 de 2012 establece las personas y terceros a los cuales se puede suministrar la información personal, es importante señalar las condiciones bajo las cuales se entrega información a las entidades públicas o administrativas en ejercicio de sus funciones legales. En efecto, esta excepción a la autorización del Titular requiere hacer varias precisiones teniendo en cuenta que los datos personales de carácter privado o semiprivado en cabeza de las entidades públicas exigen un tratamiento y reserva especial, so pena de las sanciones de que trata el artículo 23 de la Ley 1581 de 2012.

En efecto, la Corte Constitucional ha señalado 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, [en todo caso debe garantizar] el derecho al hábeas data del Titular de la información"*. (Sentencia C-748 de 2011).

Por lo tanto, ha indicado que este suministro debe cumplir dos condiciones:



a) El carácter calificado del vínculo entre la divulgación del dato y el cumplimiento de una clara y específica competencia funcional de la entidad.

b) Una vez la entidad administrativa accede al dato personal adopta la posición jurídica de garante¹ dentro del proceso de administración de datos personales, lo que de forma lógica le impone el deber de proteger los derechos fundamentales del Titular de la información, previstos en la Constitución Política.

Por tanto, la entidad pública o administrativa en ejercicio de sus funciones legales 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.*" (Sentencia C-748 de 2011).

Sobre este aspecto, la Corte Constitucional también ha señalado que el suministro de datos de la entidad administradora al peticionario se debe realizar bajo dos principios. Por un lado, el principio de responsabilidad compartida, según el cual, *"tanto quien solicita la información como quien la suministra, deben desarrollar su conducta teniendo en cuenta la existencia de un interés protegido en cabeza del titular del dato"*. Por otro, el principio de cargas mutuas de acuerdo con el cual *"a mayor información solicitada por un tercero, mayor detalle sobre su identidad y sobre la finalidad de la información"* (Sentencia C-729 de 2002).

9. Obligaciones del responsable del tratamiento de datos personales

Como responsable del tratamiento de datos personales, el IGAC asumirá como mínimo, los siguientes deberes:

1. Garantizar al Titular, en todo tiempo, el ejercicio pleno y efectivo del derecho de hábeas data, esto es, conocer, actualizar, rectificar o suprimir la información que se haya recogido en bancos de datos y archivos de las entidades públicas.
2. Informar debidamente al Titular sobre la finalidad de la recolección de los datos y los derechos que le asisten. Esta información deberá estar consignada en la respectiva Política de Tratamiento de Datos Personales.
3. Transferir y transmitir únicamente datos cuyo tratamiento esté previamente autorizado por el Titular o la ley.
4. Conservar la información bajo condiciones de seguridad necesarias que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. En caso de que se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares, deberán informar oportunamente a la autoridad de protección de datos.
5. Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

¹ La posición de garante tiene origen en el nivel de riesgo que aparece la actividad de las administradoras de datos personales, lo que se traduce en términos de la Corte, en un "deber de especial diligencia" asociado al deber de garantizar el respeto a la dignidad humana y los derechos fundamentales a la libertad, buen nombre y honra de los titulares de los datos. (Sentencias T-414 de 1992 y T-1085 de 2001).





6. Dar trámite a las consultas y reclamos formulados en los términos señalados por la ley.

7. Cumplir las instrucciones y atender los requerimientos que imparta la Superintendencia de Industria y Comercio en materia de protección de datos personales.

II. ACCESO Y SUMINISTRO DE LA INFORMACIÓN

1. Definición y clasificación de la información

Teniendo en cuenta que eventualmente el derecho a la información y al *habeas data* pueden entrar en colisión, la Corte Constitucional establece una clasificación de la información con el fin de determinar su publicidad y la posibilidad legal de obtener acceso a la misma. En este sentido, se reconocen cuatro tipos de información:

La información pública: Se define como aquella *"información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal"*. Vale señalar que la información producida o administrada por las autoridades públicas se presume pública y debe ser interpretada a la luz del principio de máxima divulgación. Cuando la información no esté publicada, podrá ser solicitada por cualquier ciudadano sin el deber de satisfacer requisito alguno.

La información semi-privada: Es aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo 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 al comportamiento financiero de las personas (Sentencia T-828 de 2014).

La información privada: Es aquella que por versar sobre información personal o impersonal, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, los documentos privados, las historias clínicas o la información extraída a partir de la inspección del domicilio (Sentencia T-828 de 2014).

Información reservada: Por versar sobre información personal y tener una estrecha relación con los derechos fundamentales del titular como la dignidad, la intimidad y la libertad, se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. En esta categoría se encuentran los datos sensibles.

2. Ley de Transparencia y del Derecho de Acceso a la Información Pública: ámbito de aplicación

De acuerdo con el artículo 2 de la Ley 1712 de 2014, *"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"*. Vale aclarar que son sujetos obligados, entre otros, *"a) [las] entidad[es] pública[s], incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital, c) Las personas naturales y jurídicas, públicas o privadas, que presten función pública, que presten servicios públicos respecto de la información directamente relacionada con la prestación del servicio público; d) Cualquier persona natural, jurídica o dependencia de persona jurídica que desempeñe función pública o de autoridad pública, respecto de la información directamente relacionada con el desempeño de su función."* (art. 5).



En ese sentido, la información pública en cabeza del IGAC, como sujeto obligado, deberá estar a disposición del público a través de medios físicos, remotos o locales de comunicación electrónica, así como en la web, a fin de que la ciudadanía puedan obtener la información, de manera directa o mediante impresiones (art. 7).

3. La información pública y el suministro de información personal

Ahora bien, la información producida o administrada por las autoridades públicas se presume pública y debe ser interpretada a la luz del principio de máxima divulgación, de tal suerte que la reserva de información pública sólo podrá ser excepcional en los casos previstos en la Constitución y la ley. Entre dichas excepciones, se prevé:

1. Información pública reservada definida como "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". Por lo tanto, su acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a alguno de los siguientes derechos:

- a) La defensa y seguridad nacional;
- b) La seguridad pública;
- c) Las relaciones internacionales;
- d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
- e) El debido proceso y la igualdad de las partes en los procesos judiciales;
- f) La administración efectiva de la justicia;
- g) Los derechos de la infancia y la adolescencia;
- h) La estabilidad macroeconómica y financiera del país;
- i) La salud pública."

2. Información pública clasificada definida como "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". En consecuencia, su acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a alguno de los siguientes derechos:

a) El derecho a la intimidad, bajo las limitaciones propias que impone la condición de servidor público.
[...]


b) El derecho de toda persona a la vida, la salud o la seguridad.

c) Los secretos comerciales, industriales y profesionales."

Sobre el particular, la Corte Constitucional ha señalado que tratándose de información pública personal, la posibilidad de divulgación y suministro se debe analizar a partir de la relación del dato con el derecho a la intimidad, la vida, la salud, la seguridad o la dignidad del titular. En términos de la Corte, "Las mencionadas condiciones de excepcionalidad y precisión pueden ser diluidas a partir de la tipología de datos personales que ofrece la jurisprudencia constitucional. En particular, en el caso de los datos públicos, su distribución es libre y se inserta en el ámbito propio del principio de máxima divulgación. En contraste, los datos sensibles son por su misma naturaleza reservados, caso en el cual se predica la reserva prima facie de los mismos. La información semiprivada, en cambio, exige un estándar de argumentación más exigente para que opere su reserva, puesto que deberá demostrarse que la limitación en el acceso es una medida necesaria para la protección de los derechos fundamentales mencionados anteriormente (Sentencia C-276-19).

De acuerdo con lo anterior y en aplicación del principio de eficacia, celeridad y transparencia que rige el derecho de acceso a la información pública, toda información en poder del IGAC se presume pública y deberá estar dispuesta a través de los medios más amplios posibles, salvo las excepciones constitucionales y legales antes señaladas.

Así las cosas, se solicita a las Subdirecciones y Oficinas, Direcciones Territoriales y Unidades Operativas del Instituto tener en cuenta el régimen legal señalado a fin de garantizar el derecho al hábeas data de los titulares de los datos personales, así como el derecho a la información de los ciudadanos.


OLGA LUCÍA LÓPEZ MORALES
Directora General

Revisó y aprobó: Patricia del Rosario Triviño - Jefe Oficina Asesora Jurídica
Proyectó: Laura Villarraga Albino - Contratista Oficina Asesora Jurídica