

MEMORANDO

11.2.2
Bogotá,

PARA: JORGE HERNAN PALACINO CORDOBA
Dirección Técnica de Sanidad Vegetal

DE: OFICINA ASESORA JURÍDICA

ASUNTO: Concepto Jurídico No. 007-2020. Entrega de Bases de Datos a otras entidades dentro del proceso de "Inscripción de intención de siembra anual de arroz". Su memorando No.20193113655

Apreciado doctor Palacino:

Para dar respuesta a la solicitud del asunto, recibida para trámite mediante memorando No. 20193113655; se emite el siguiente Concepto Jurídico.

I. TESIS CONCLUSIVA.

Sí es necesario suscribir un acuerdo de confidencialidad entre el Instituto Colombiano Agropecuario- ICA y las entidades adscritas al proceso de inscripción de intención de siembra anual de arroz para garantizar el derecho fundamental al hábeas data.

II. PROBLEMA JURÍDICO.

¿Se debe implementar un acuerdo de confidencialidad entre el Instituto Colombiano Agropecuario ICA, con las entidades que conforman las mesas de trabajo dentro del proceso de "Inscripción de intención de siembra anual de arroz" para garantizar la protección de bases de datos?

III. NORMA(S) CONTROLANTE(S).

- Constitución Política de Colombia.
- Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales- Ley de hábeas data.
- 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 y se dictan otras disposiciones.
- Ley 1755 de 2015, Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

IV. APLICACIÓN AL CASO CONCRETO.

El derecho fundamental al hábeas data se encuentra consagrado en el artículo 15 superior que dispone que todas las personas tienen derecho a la intimidad personal, al buen nombre, a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los diferentes bancos de datos y en los archivos de entidades públicas y privadas. Adicionalmente, establece la obligación que tiene el Estado de hacer respetar tales derechos. Asimismo, de conformidad con el artículo 152 de la Constitución Política, corresponde al Congreso de la República regular los derechos fundamentales de las personas, los procedimientos y recursos para su protección a través de la expedición de leyes estatutarias. No obstante, ante el vacío generado por la falta de regulación inicial para el ejercicio del derecho fundamental al hábeas data, la Corte Constitucional se ocupó de caracterizarlo y determinar su alcance mediante sentencias de revisión de tutela.¹

Por otro lado, la Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales- Ley de hábeas data establece en su artículo 5: 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.

Así mismo, prohíbe el tratamiento de datos sensibles con excepción de los siguientes casos: (I) cuando el titular otorga su consentimiento, (II) el Tratamiento es necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado, (III) el tratamiento es 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, (IV) el Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y (V) el Tratamiento tenga una finalidad histórica, estadística o científica, en este último caso deben adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

Por otro lado, la Corte Constitucional define la información privada como:

(...) Aquella que se encuentra en el ámbito propio del sujeto a quien le incumbe y, por ende, sólo puede accederse a sta por orden de autoridad judicial en el ejercicio de sus funciones. La información personal comprende la relacionada con los libros de los comerciantes, los documentos privados, las historias clínicas, la información extraída a partir de la inspección del domicilio o luego de la práctica de pruebas en procesos penales sujetas a reserva . De igual forma, tiene naturaleza de información privada la información genética que reposa en bancos de sangre,

esperma, laboratorios, consultorios médicos u odontológico o similares. La Corte ha advertido que en los eventos aludidos, esta información revela facetas importantes de la vida personal, social y económica del individuo y que, debido a expresa disposición constitucional o por su propia naturaleza, solo puede ser divulgada por autorización de la persona a la que se refiere, o por la existencia de una decisión judicial (...)2.

Así mismo esta misma corporación en Sentencia C-748 de 2011, señaló lo siguiente:

(...) Principio de seguridad: Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, 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. De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto diluvio de datos, a través del cual día a día la masa de datos personales existente, objeto de tratamiento y de ulterior transferencias, no cesa de aumentar. Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riesgos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación(...)3.

A su turno y con el fin de materializar el principio en mención, el artículo 17 de la Ley 1581 de 2012 ha establecido, entre otros, los siguientes deberes a cargo de los responsables del tratamiento de datos personales:

(...) Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: "(...) d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento (...) i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular (...) n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares (...)".

De acuerdo con lo anterior, es un deber tanto de los Responsables como Encargados del Tratamiento de los datos personales el establecer medidas con el fin de garantizar la seguridad de las bases de datos, y en especial que: (I) no sea adulterada la información contenida en las bases de datos, (II) no se pierda la información de las bases de datos, (III) no se pueda hacer uso, consultar o acceder sin autorización o de manera fraudulenta a las bases de datos.4

Existe entonces un deber tanto del ICA como de las entidades adscritas al proceso de inscripción de intención de siembra anual de arroz de garantizar el derecho fundamental al hábeas data, pues si bien al momento de la inscripción el titular de la información, autorizó su uso, el mismo debe ceñirse a los postulados constitucionales y legales sobre la materia, conforme lo señalado en las líneas que anteceden.

V. CONCLUSIÓN FINAL.

Del análisis de la normatividad reseñada, se puede llegar a la conclusión de que los datos sensibles de las personas son objeto de una especial protección, en virtud de su derecho fundamental a la intimidad y del derecho al hábeas data, es decir, los que se refieren en el artículo 5 de la Ley 1581 de 2012; para el caso concreto, datos relativos a la base de datos generada al momento de hacer la inscripción de intención de siembra anual de arroz.

En los anteriores términos, procedo a dar una respuesta de fondo a su solicitud, indicando que la misma se surte bajo los parámetros del artículo 28 de la Ley 1755 de 2015.

Cordialmente,

JUAN FERNANDO ROA ORTIZ
Jefe Oficina Asesora Jurídica (E)

Respuesta a: Radicación No. 20193113655 del: 12/06/2019
Elaboró: Alvaro Andres De La Hoz Gutierrez

1. Corte Constitucional de Colombia. Sentencia T-238/18 [MP. JOSÉ FERNANDO REYES CUARTAS].

2. Corte Constitucional de Colombia. Sentencia T-114/18 [MP. DIANA FAJARDO RIVERA].

3. Corte Constitucional de Colombia. Sentencia T-748/11 [MP. MARÍA VICTORIA CORREA].

4. Universidad Externado de Colombia. (2017). Recuperado de: <https://dernegocios.uexternado.edu.co/comercio-electronico/superintendencia-de-industria-y-comercio-concepto-16-075042-00003-0000/>