REPÚBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 43761 DE 2020

(31 de Julio)

Por la cual se resuelve un recurso de apelación

Radicación No. 19-89199

VERSIÓN ÚNICA

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCION DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por el artículo 21 de la Ley 1581 de 2012, el numeral 7 del artículo 16 del Decreto 4886 de 2011, y

CONSIDERANDO:

PRIMERO: Mediante escrito del 15 de abril de 2019, algunos funcionarios del **MUNICIPIO DE CAJIBÍO, CAUCA**, le remitieron a esta Superintendencia copia del oficio No. 01643 del 9 de abril de 2019, en el cual le ponen de manifiesto al señor alcalde de ese ente municipal su inconformidad frente al Decreto Municipal No. 00041 del 9 de abril de 2019, por el cual establece la implementación de un sensor de huella digital para el "*control de acceso y asistencia de los funcionarios de la Alcaldía Municipal de Cajibío (Cauca)*", sin tener en cuenta, según la carta, lo establecido en la normatividad en materia de protección de datos personales[1]. El decreto en discordia establece:

> *"(…)*
>
> ***ARTÍCULO CUARTO:** Control de Asistencia. Adóptese el sistema biométrico para el control de acceso y asistencia de los funcionarios de la Alcaldía Municipal de Cajibío (Cauca).*
>
> ***PARÁGRAFO PRIMERO.** Los funcionarios de la Alcaldía Municipal de Cajibío (Cauca), deberán estar previamente registrados en el sistema de control (biométrico) ubicado en el Despacho de la Secretaría de Gobierno, Tránsito y Transporte y Participación Comunitaria Municipal, a efectos de poder registrar su asistencia a laborar.*
>
> ***PARÁGRAFO SEGUNDO:** El sistema biométrico y los registros de asistencia que se produzcan mediante su uso, serán administrados y controlados por el Secretario de Gobierno, Tránsito y Transporte y Participación Comunitaria Municipal o quien haga sus veces en calidad de Jefe de Personal; y quien además definirá los lineamientos para su inmediata aplicación mediante las respectivas circulares.*
>
> ***ARTÍCULO QUINTO: Responsables del Control.** Los jefes inmediatos serán los responsables del control del horario del personal a cargo, para lo cual podrán asistirse de los registros de asistencia que genere el sistema biométrico implementado por la entidad.*
>
> *(…)".*[2]

SEGUNDO: Que mediante Resolución No. 69434 del 4 de diciembre de 2019, la Dirección de Investigación de Protección de Datos Personales encontró que el **MUNICIPIO DE**

[1] Folios 1 -5.
[2] Folios 6-10.

CAJIBÍO, CAUCA, carecía de políticas, procedimientos y procesos necesarios para cumplir con la Ley 1581 de 2012 y el Decreto 1074 de 2015. En mérito de lo anterior, la Dirección resolvió lo siguiente:

"***ARTÍCULO PRIMERO: ORDENAR*** *al* ***MUNICIPIO DE CAJIBÍO, CAUCA****, identificado con el Nit. 891.500.864-5, en su condición de Responsables del Tratamiento, que en los casos en que se haya recolectado datos personales sensibles sin haber mediado una autorización previa, expresa e informada del Titular (de conformidad con los requisitos establecidos en la Ley 1581 de 2012 y según lo señalado en la presente resolución), para la implementación del Sistema Biométrico del Municipio de Cajibío, proceda a suprimir de sus bases de datos y acredite técnicamente ante este despacho el cumplimiento de esta orden.*

ARTÍCULO SEGUNDO: ORDENAR *al* ***MUNICIPIO DE CAJIBÍO****, identificado con el Nit. 891.500.864-5, en su condición de Responsable del Tratamiento, que en adelante se abstenga de recolectar datos sensibles a través del sistema biométrico sin contar con la autorización de los Titulares, de la forma establecida en la Ley 1581 de 2012 y en este acto administrativo.*

Así mismo, en caso de que un Titular se rehúse a otorgar su autorización, el ***MUNICIPIO DE CAJIBÍO*** *deberá abstenerse de realizar el tratamiento de sus datos personales. Por lo que a efectos de llevar control de horario de trabajo de los funcionarios esa entidad, podrá implementar otro sistema.*

ARTÍCULO TERCERO: ORDENAR *al* ***MUNICIPIO DE CAJIBÍO, CAUCA****, identificado con el Nit. 891.500.864-5 que, en su condición de Responsable del Tratamiento, desarrolle e implemente una Política de Tratamiento de datos personales en la que:*

3.1 *Se mencione de manera específica y explícita el nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable del Tratamiento de los datos, conforme lo dispone el numeral 1 del artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015.*

3.2 *Se mencione de manera específica y explícita el procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización, conforme lo dispone el numeral 5 del artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015.*

3.3 *Se incorpore de manera específica y explícita el nombre o razón social, domicilio, dirección, correo electrónico y telefónico del Responsable de los datos, conforme lo dispone el numeral 1 del artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015.*

3.4 *Se mencione de manera específica y explícita cuál es la persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización, conforme lo dispone el numeral 4 del artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015.*

3.5 *Se incluye un acápite o el numeral en el que se mencione de manera expresa la entrada en vigencia de la misma y la vigencia de las bases de datos, la cual no puede ser ilimitada, así mismo se delimite la finalidad de los datos dentro del marco legal, conforme lo dispuesto el artículo 4 de la Ley 1581 de 2012, el numeral 6 del artículo 2.2.2.25.3.12 y el artículo 2.2.2.25.2.1 del Decreto Único Reglamentario 1074 de 2015.*

3.6 *Se indique al titular los derechos que le asisten de conformidad con el numeral 3 del artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015.*

Para efectos de cumplir con lo anterior, la entidad podrá valerse de las guías publicadas por esta Superintendencia en su portal web "http://www.sic.gov.co" a las cuales podrá acceder a

través del enlace "guías y cartillas" ubicado en el menú de "protección de datos personales" visible al ingresar al referido portal.

***ARTÍCULO CUARTO: ORDENAR** al **MUNICIPIO DE CAJIBÍO, CAUCA**, identificado con el Nit. 891.500.864-5, para que, en su condición de Responsable del Tratamiento, desarrolle e implemente un Manual de Seguridad para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, y el Manual de procedimientos para la recolección, uso, circulación y supresión de información almacenada en su base de datos, atendiendo a los presupuestos de la Ley 1581 de 2012, sus normas y decretos reglamentarios, así como lo expuesto en el presente acto administrativo.*

(…)."

TERCERO: Que en el término legal establecido para el efecto[3], mediante escrito radicado con el número 19-089199-17 del 27 de diciembre de 2019[4], el señor **LUIS HELMER VIVAS MANZANO**, en su calidad de alcalde y representante legal del **MUNICIPIO DE CAJIBÍO**, interpuso recurso de apelación contra la Resolución No. 69434 del 4 de diciembre de 2019, con base en los siguientes argumentos:

3.1. Señala que "*[t]al como se establece, con la certificación emitida por el Secretario de Gobierno y Tránsito y participación Comunitaria, el Municipio de Cajibío, no ha realizado recolección de dato alguno, de los funcionarios del Municipio de Cajibío*."

Agrega que "*a pesar de tener un acto administrativo, el cual goza de presunción de legalidad, no exigió su cumplimiento, pues el Municipio, estaba en la espera de la disposición final de la Superintendencia. Por lo tanto, al no haber recolección, no puede exigirse o sancionarse por la aparente falta de la protocolización de tratamiento de datos sensibles*."

Concluye, por tanto, que los hallazgos de la Superintendencia no se fundamentan en la realidad.

3.2. Recapitula la normatividad que obliga a los entes del orden territorial a establecer la jornada laboral de los trabajadores públicos a su cargo y la compensación para las personas que trabajan los días sábados. Entre ellas, cita el Decreto 1042 de 1978, el artículo 2° de la Ley 27 de 1992 y el artículo 87 de la Ley 443 de 1998.

En esa línea, considera que "*el cumplimiento del horario, por parte de los trabajadores públicos, hace parte fundamental, del servicio público que se presta, pues si no existen mecanismos que garanticen el cumplimiento del horario, no podría garantizar la prestación del servicio público que se prestan, en sus diferentes dimensiones, en cada una de las secretarías de Despacho*."

3.3. Frente a la falta de una política de protección de datos personales, pone de presente que ese municipio en Decreto No. 00082 de 26 de julio de 2019 adoptó la política de tratamiento de que trata el Decreto 1074 de 2015, razón por la cual, "*la afirmación que no se cuenta con MANUAL PARA EL MANEJO DE DATOS SENSIBLES, no es cierto, por lo tanto, solicitamos se analice el Decreto.*"

Agrega que ellos también cuentan con los siguientes textos: "*COMPROMISO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN, documentos que fueron*

[3] Conforme a constancia suscrita por la Coordinadora del Grupo de Notificaciones y Certificaciones de esta Superintendencia, visible a folios 78-83, la Resolución No. 69434 del 4 de diciembre de 2019 fue notificada por aviso al ente municipal el 13 de diciembre de 2019, por lo que el recurso fue presentado dentro del término legal.
[4] Folios 243 al 262

nombrados y relacionados en el oficio remitido a la Superintendencia, sin embargo, en esta oportunidad se anexa una copia."

3.4. Insiste en que "*el Municipio en este momento no ha realizado la recolección de datos biométricos (huella digital) de los funcionarios de planta del Municipio. Por ello, cualquier advertencia, esta de mas (sic), pues no existen datos que deban ser protegidos*."

3.5. Resume sus argumentos, de la siguiente manera:

3.5.1. *"El Municipio de Cajibío no ha iniciado con la recolección de datos sensibles (…), por lo tanto, las políticas del tratamiento de los datos personales, no le son aplicables, si no existen datos objeto de protección."*

3.5.2. *"El establecer medidas para el cumplimento de horario de los funcionarios públicos, es parte integral de las funciones del Municipio de Cajibío, para el efectivo cumplimiento de los servicios que se prestan*."

3.5.3. "*A pesar que no existen datos recolectados, en este momento se cuenta con la política para el manejo de datos, así como el Compromiso de Confidencialidad y no divulgación, suscrito por el Alcaldía Municipal y el Secretario de Gobierno*."

CUARTO: Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho procede a resolver el recurso de apelación interpuesto por el **MUNICIPIO DE CAJIBÍO**, en adelante el municipio **RECURRENTE**, contra la Resolución No. 69434 del 4 de diciembre de 2019, de la siguiente manera:

CONSIDERACIONES DEL DESPACHO

4.1. COMPETENCIA DEL DESPACHO DEL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES.

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011[5] establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destacan las siguientes:

"(…)

7. Decidir los recursos de reposición y las solicitudes de revocatoria directa que se interpongan contra los actos que expida, así como los de apelación que se interpongan contra los actos expedidos por la Dirección a su cargo. (…)"

4.2. EL PRINCIPIO DE LIBERTAD EN EL TRATAMIENTO DE DATOS PERSONALES.

A continuación nos referiremos al principio de libertad como núcleo esencial del derecho al habeas data, el Tratamiento de datos personales en el contexto laboral, y el uso sistemas biométricos.

4.2.1. Del principio de libertad en el tratamiento de datos personales

[5] Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones.

El artículo 15 de la Carta Política de 1991 establece que en el Tratamiento de datos personales se respetará la libertad y demás garantías consagradas en la Constitución. Esto significa que tanto las entidades públicas como las organizaciones que procesen datos personales están sujetas a unos deberes específicos, ya sea aquellos establecidos en la Ley 1266 de 2008, Habeas Data Financiero, o en la Ley 1581 de 2012, Régimen General de Protección de Datos Personales, cuya inobservancia se traduce en una innegable violación de la Carta Política.

Sobre el principio de libertad, la jurisprudencia de la Corte Constitucional ha establecido que este es el "*pilar fundamental de la administración de datos*" que "*permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos*"[6]. Esta elección voluntaria del Titular es una manifestación de sus derechos de decidir sobre el manejo de su información personal. Por eso, la Corte ha establecido "*que con el principio de libertad previsto en el artículo 15 C.P., de acuerdo con el cual la legitimidad constitucional de los procesos de acopio, tratamiento y divulgación de datos personales se sustenta, entre otros aspectos, en que el sujeto concernido preste su autorización libre, previa y expresa*".[7]

Para el caso del Régimen General de Protección de Datos Personales, el literal c) del artículo 4 de la Ley 1581 de 2012 señala textualmente que "*el Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular*." El artículo 2.2.2.25.2.1 del Decreto 1074 de 2015 no sólo reitera la necesidad de la autorización para el Tratamiento de la información personal al disponer que "*salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin autorización del Titular*", sino que advierte en los siguientes términos que los medios para recolectar los datos deben ser lícitos y honestos: "*No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales*".

El artículo 9 de la Ley 1581 de 2012 recalca que la autorización es la regla general para legitimar la recolección, uso y divulgación de datos de carácter personal. Por eso, salvo que la ley diga lo contrario, *"en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior*". Nótese no sólo la importancia que da la ley en varios artículos al consentimiento del Titular, sino la necesidad de probar que se obtuvo la autorización, lo cual es consistente con el deber de responsabilidad demostrada.

Para la Corte Constitucional, "*los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Las únicas excepciones posibles serán las establecidas en el artículo 10 del proyecto de ley bajo examen*"[8]. Alternativamente, hay circunstancias específicas (o excepciones) en las que el procesamiento de los datos se considera legal, incluso en ausencia de consentimiento. A este respecto, el artículo 10 de la ley 1581 de 2012, por su parte, enuncia en los siguientes términos los casos en que no es necesaria la autorización del Titular para tratar su información personal:

> "***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;*

[6] Cfr. Corte Constitucional, sentencia C- 748 de 2011, numeral 2.6.5.2.3.
[7] Cfr. Corte Constitucional, sentencia C-1011 de 2008.
[8] Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.11.3.

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." (Énfasis añadido)

No debe perderse de vista que la recolección de datos sin autorización no significa que quede sin protección esa información y los ciudadanos titulares de los datos. En efecto, la parte final del artículo 10 de la Ley Estatutaria 1581 de 2012 señala que "*quien acceda a los datos personales sin que medie autorización previa* ***deberá en todo caso cumplir con las disposiciones contenidas en la presente ley***". (Destacamos)

La autorización es un mecanismo de legitimación para tratar datos personales, pero no, por si sola, una forma de protección de los derechos. La efectiva protección de los derechos dependerá de las medidas que implementen los Responsables del tratamiento para garantizar el uso debido de los datos, su seguridad, confidencialidad, etc

Desde luego, la exclusión del uso del consentimiento como base legal del Tratamiento de datos personales depende del análisis de varios factores, pero no limitado a:

(i) La existencia de una disposición legal u orden judicial a la cual el Responsable del Tratamiento está sujeto;
(ii) Un claro desequilibrio de poder en la relación entre el Responsable y el Titular de la Información;
(iii) La finalidad del procesamiento o categoría de información personal; esta circunstancia debe ser analizada caso por caso y no generalizada en abstracto.

No sobra poner de presente que señalar simplemente una disposición legal como la supuesta base legal para el tratamiento de datos personales no es suficiente en sí misma para satisfacer el principio de libertad. De ahí que el Responsable debe ser capaz de demostrar cómo el procesamiento de datos es necesario para el cumplimiento de la norma en cuestión.

Ahora bien, en caso en que el Tratamiento involucre datos de carácter sensible, el artículo 5 de la Ley 1581 de 2012[9] incluye una prohibición general, teniendo en cuenta los altos riesgos que puede generar su uso para los derechos y libertades de los Titulares, entre ellos, discriminación o revelación de su intimidad. Al respecto, precisó la Corte Constitucional:

"En relación con ***el primer contenido normativo****, la Sala estima que no solamente es compatible con la Carta, sino que es una exigencia del derecho a la intimidad y un desarrollo del principio del habeas data de acceso y circulación restringida.*

Ciertamente, como se explicó en la sentencia C-1011 de 2008, en tanto los datos sensibles pertenecen a la esfera de la intimidad de las personas, "(…) todo acto de divulgación mediante los procesos genéricos de administración de datos personales, distintos a las posibilidades de divulgación excepcional descritas en el fundamento jurídico 2.5 del presente análisis, se encuentra proscrita. Ello en la medida que permitir que información de esta naturaleza pueda

[9] Ley 1581 de 2012. "***ARTÍCULO 5o. 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."*

ser objeto de procesos ordinarios de acopio, recolección y circulación vulneraría el contenido esencial del derecho a la intimidad."

En todo caso, el artículo 6 contempla cinco excepciones a la prohibición general del Tratamiento de datos sensibles, a saber:

"***ARTÍCULO 6o. 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."

En términos prácticos, siempre que un Responsable requiera el uso de datos personales, entre ellos, los de carácter sensible, para los propósitos o finalidades por este perseguido, es importante que, antes que se inicie cualquier actividad que conlleve el procesamiento de datos personales, el Responsable determine cuál es la base jurídica que legitima dicho Tratamiento. Debe tenerse en cuenta, sin embargo, que debido a que las excepciones previstas en la norma involucran un derecho fundamental protegido por misma Constitución Política (Artículo 15), las mismas deben interpretarse de manera restringida.

No debe perderse de vista que la recolección, uso, circulación y tratamiento de datos sensibles debe estar rodeado de especial cuidado y diligencia en su recolección, uso, seguridad o cualquier otra actividad que se realice con los mismos. En efecto, la Corte Constitucional exige **responsabilidad reforzada** por parte de los Responsables y Encargados: "*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*"[10] de la Ley Estatutaria 1581 de 2012.

Adicionalmente, el párrafo final del artículo 6 del decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015) ordena que "*ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles*".

4.2.2. Sobre el procesamiento de datos personales en el contexto laboral

Aun cuando la autorización constituya la regla general para el Tratamiento de datos personales, para este Despacho es poco probable que en el contexto laboral los empleadores puedan basarse únicamente (o exclusivamente) en el consentimiento como

[10] Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.8.4

base legal para el uso de la información personal de sus empleados para ciertas finalidades o propósitos, en especial, para aquellas circunstancias en que los datos son recogidos, utilizados y divulgados para el cumplimiento de una obligación legal a la cual ellos están sujetos (por ejemplo: pago de la seguridad social, impuestos, etc.), pues en ese caso, la ley sería la base jurídica que legítima su Tratamiento.

En todo caso, con independencia que el Tratamiento esté soportado en el cumplimiento de una obligación legal a la que el Responsable en su calidad de empleador está sujeto, este Despacho aclara que esas circunstancias no anulan *per se* su deber de cumplir con los otros principios establecidos en el artículo 4º de la Ley 1581, entre ellos, los principios de finalidad y transparencia, que señalan:

> "***ARTÍCULO 4o. 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:*
>
> *(…)*
>
> ***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;*
> *(…)*
>
> ***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*."

No debe olvidarse tampoco que es un deber del Responsable del Tratamiento garantizar que el procesamiento de los datos de los trabajadores sea adecuado, relevante y limitado en relación con los fines perseguidos. Señala el artículo 2.2.2.25.2.1 del Decreto 1074 de 2015:

> "***Artículo 2.2.2.25.2.1. Recolección de los datos personales****.* ***En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente****. Salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin autorización del Titular.*
>
> *(…)*". (Negrillas fuera del texto original).

Fruto de lo que antecede, hay que tener en cuenta que, más allá de determinar la base legal del procesamiento de los datos en el contexto laboral, como se explicó en líneas anteriores, el Responsable del Tratamiento debe evaluar si la finalidad perseguida con el uso de la información se puede lograr por otros medios o mecanismos que resulten menos lesivos o intrusivos para los individuos concernidos. Este estudio es, por tanto, una medida preventiva que evita que una operación o conjunto de operaciones que involucren datos personales terminen afectando derechos o intereses jurídicos de alta envergadura para los Titulares.

Lo anterior, es una muestra elocuente con lo manifestado por la Corte al declarar la constitucionalidad de las excepciones previstas en el artículo 6º de la Ley 1581 de 2012, arriba citadas. En efecto, el Alto Tribunal concluyó lo siguiente:

> *"(…)*
>
> ***2.8.4.1. Constitucionalidad del literal a)***

> *La Sala considera que, de conformidad con el principio de libertad, es posible que las personas naturales den su consentimiento, por su puesto, expreso e informado, para que sus datos personales sean sometidos a tratamiento. En estos casos deberán cumplirse con todos los principios que rigen el tratamiento de datos personales, en especial cobrará importancia el principio de finalidad, según el cual el dato sensible solamente podrá ser tratado para las finalidades expresamente autorizadas por el titular y que en todo caso deben ser importantes desde el punto de vista constitucional. En este orden de ideas, la Sala encuentra que el primer contenido normativo del literal a) se ajusta a la Constitución.*
>
> *En relación con el segundo contenido normativo, este es, la posibilidad de tratar el dato sensible sin autorización explícita del titular cuando "(…) por ley no sea requerido el otorgamiento de dicha autorización", la Sala considera que es compatible con la Constitución, siempre y cuando se entienda, como se mencionará más adelante, que tal autorización,* ***además de estar contenida en una ley, sea conforme a las garantías que otorga el habeas data, por ejemplo en materia de finalidad, y cumpla las exigencias del principio de proporcionalidad****.*

El Responsable del Tratamiento está en la obligación de tener en cuenta que el párrafo final del artículo 2.2.2.25.2.3 del Decreto 1074 de 2015 establece que "***ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.****"* En otras palabras, si un Responsable condiciona una actividad (por ejemplo, la prestación de un servicio, el ofrecimiento de un producto, etc.), a que a que el Titular suministre sus datos de carácter sensible, esa recolección podría ser considerada ilegal, pues iría en contra del principio de legalidad establecido en el artículo 4 de la Ley 1581, el cual establece que "*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*"[11]. Lo anterior, a menos que, en un análisis caso por caso, la información sensible sea estrictamente necesaria para el desarrollo de la actividad por parte del Responsable o sea requerida por mandato legal.

Una aclaración que, por tanto, otorga sentido al caso objeto de estudio por parte de esta Delegatura, pues a pesar de que, el municipio **RECURRENTE** está sujeto, como se detallará más adelante, a un conjunto de disposiciones normativas para tratar los datos de sus funcionarios, el ente territorial omitió evaluar previamente si la implementación de un sensor de huella digital era el "adecuado, pertinente y no excesivo" en relación con la finalidad por ellos perseguida, en este caso: garantizar el control de acceso y asistencia[12] a las instalaciones del ente territorial.

4.2.2.1. De los sistemas biométricos y la aplicación de la Ley 1581 de 2012 a cualquier Tratamiento de Datos personales con independencia de las herramientas que se utilicen para dicho efecto

La Ley Estatutaria 1581 de 2012 es neutral tecnológica y temáticamente. Ello significa que aplica a cualquier Tratamiento con independencia de las técnicas, procesos o tecnologías –*actuales o futuras*- que se utilicen para dicho efecto. Por ende, debe observarse y aplicarse en la recolección, uso y Tratamiento de datos personales al margen de las "innovaciones tecnológicas" que usen para dicho efecto.

Desde antaño, los empleadores han utilizado diferentes mecanismos para el registro de horario y control de asistencia de sus trabajadores. Por ejemplo, han pasado de realizarlo de manera análoga a manera digital, para finalmente efectuarlo a través de sistemas de geolocalización, video vigilancia, lector de huella digital, reconocimiento del iris, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la voz, etc.

---

[11] Ley 1581 de 2012, artículo 4, literal a)
[12] Folio 9.

En el caso del reconocimiento dactilar, este sistema permite comparar la imagen de la huella de una persona, que es captada al momento en que el individuo coloca su dedo en una superficie de cristal o un prisma, con el conjunto de plantillas biométricas almacenadas previamente en el aplicativo biométrico. Esta técnica permite la identificación, verificación y autenticación de la persona en tiempo real.

Como es sabido, los datos biométricos, a su vez, son un ejemplo de dato sensible[13] tal y como se puede constatar en la definición legal del artículo 5 de la Ley Estatutaria 1581 de 2012. Los «datos biométricos»: incluyen información sobre las características físicas (rostro, huella dactilar, palma de la mano, retina, ADN) y "comportamentales" (forma de firmar, tono de voz) sobre las personas[14]. En la regulación europea son definidos como: "*datos personales obtenidos a partir de un tratamiento técnico específico, **relativos a las características físicas**, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*"[15] (Destacamos).

En este punto cabe mencionar que el Tratamiento de información de carácter sensible puede generar un alto riesgo para los Titulares para la protección de sus derechos fundamentales a la dignidad humana, datos personales, buen nombre e intimidad, razón por la cual, su procesamiento está fundamentalmente prohibido, de acuerdo con lo que establece textualmente el artículo 6 de la Ley 1581 de 2012, arriba citado, salvo que el Tratamiento esté amparado bajo alguna excepción que establece dicha norma, como se explicó en el punto 4.1.1.

Adicionalmente, es crucial tener presente lo que ordenan, entre otros, los artículos 4, 9, 12, 17 y 18 de la Ley Estatutaria 1581 de 2012 y el artículo 4 del Decreto 1377[16] de 2013 (Incorporado en el Decreto 1074 de 2015):

a) No se pueden utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales.
b) Se debe informar a la persona la finalidad específica de la recolección de sus datos.
c) No se puede recolectar cualquier dato sino solo aquel o aquellos que sean pertinentes y adecuados para la finalidad para la cual son requeridos. Los Responsables del Tratamiento deben estar en capacidad de justificar o explicar la necesidad de recolectar los datos que solicitan a las personas.
d) Salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin la autorización previa, expresa e informada del Titular. La autorización se puede obtener por cualquiera de los *mecanismos -escrito, verbal, electrónico o conductas inequívocas-* previstos en el artículo 7 del Decreto 1377 de 2013, pero el Responsable tiene el deber de conservar prueba de la misma.[17]

---

[13] Los datos sensibles fueron definidos en la ley 1581 de 2012 y en el decreto 1377 de 2013 como **"** *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*" (Artículo 5 de la ley 1581 de 2012, repetido en el numeral 3 del artículo 3 del decreto 1377 de 2013, incorporado en el Decreto 1074 de 2015) .

[14] Saini, Nirmala y Sinha, Aloka. *Soft biometrics in conjunction with optics based biohashing*. Optics Communications, Volume 284, Issue 3, pág. 756. February 2011.

[15] Cfr. Numeral 14 del artículo 4 del Reglamento europeo de protección de datos (2016) : PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA (2016) REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO (27 de abril de 2016) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[16] Por el cual se reglamenta parcialmente la Ley 1581 de 2012

[17] Cfr. Literal b) del artículo 17 de la Ley Estatutaria 1581 de 2012.

4.3. DEL CASO SOMETIDO A APELACIÓN.

Descendiendo al asunto sub judice, este Despacho procederá a analizar si el procesamiento de la huella dactilar de los funcionarios a través del sistema biométrico por parte del municipio **RECURRENTE**, en ese caso, era necesario para el cumplimiento de una obligación a cargo de ese ente territorial.

(i) En el presente asunto, los denunciantes presentaron su inconformidad con la decisión adoptada por el municipio **RECURRENTE** de implementar un sistema de lectura de huella biométrica para fines de "*control de acceso y asistencia*". En efecto, con memorial radicado bajo el número 19-089199 del 15 de abril de 2019, se aportó copia del oficio S.D.G. 500 - 01643 de fecha 2 de abril de 2019, con asunto: "*Observaciones al decreto N°. 00041 del 09 de abril de 2019*", en el cual se precisaron los siguientes aspectos:

> *"Se da a conocer a los distintos despachos adscritos a la administración municipal a través del correo institucional el día de hoy 09/04/20189 el decreto N°. 00041 emanado de la fecha precipitada por medio del cual se establece el horario laboral de los funcionarios públicos de la alcaldía municipal de Cajibío y se adopta el sistema biométrico para el control de asistencia, contemplado dentro de su articulado que la implementación de dicho cometido datara según el parágrafo 2 del artículo 4º mediante 'circulares' mismas sobre las cuales NO se tiene conocimiento en ninguna de las dependencias impidiendo a su paso dar cumplimiento al parágrafo primero del mismo artículo en referencia pues para dicho registro se debe agotar primero la puesta en conocimiento del protocolo de seguridad y confiabilidad con el que contara (sic) tal sistema electrónico."*
>
> *(…)*
>
> *El artículo 6 del decreto en mención señala que se deben cumplir una serie de obligaciones por parte de obligaciones por parte de quien pretenda recolectar o tratar los datos personales entre ellas: "informar al titular al titular que por tratarse de un dato sensible NO SE ESTÁ OBLIGADO A AUTORIZAR EL TRATAMIENTO." Adicional a ello es obligación "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.*
>
> *Obligaciones que no se tuvieron en cuenta al momento de la expedición del decreto municipal en comento y al recolectar la huella de algunos compañeros de trabajo el día sábado 06 de abril de 2019 por parte del señor secretario de gobierno quien verbalmente y sin mayores explicación solicitaba a los funcionarios asentar la huella en el sistema biométrico adquirido para tales efectos.*
>
> *(…)*
>
> *Es así que por considerarse un decreto municipal contrario a la ley y sobre todo violatorio de derechos fundamentales tales como la intimidad, la libertad, el libre desarrollo de la personalidad, el debido proceso y ante todo el habeas data.*"[18]

(ii) Durante el trámite administrativo, las partes aportaron copias de los siguientes decretos emanados del municipio **RECURRENTE**:

a. **Copia del DECRETO NO. 0041 DEL 9 DE ABRIL DE 2019**[19], "*POR MEDIO DEL CUAL SE ESTABLECE EL HORARIO LABORAL DE LOS FUNCIONARIOS PÚBLICOS DE LA*

[18] Folios 6 al 10.
[19] Folios 44 al 46.

ALCALDÍA MUNICIPAL DE CAJIBÍO (CAUCA), Y SE ADOPTA EL SISTEMA BIOMÉTRICO PARA EL CONTROL DE ASISTENCIA."

b. **Copia del DECRETO NO. 0044 DEL 10 DE ABRIL DE 2019**[20], "*POR MEDIO DEL CUAL SE ADICIONA EL DECRETO N° 0041 DEL 09 DE ABRIL DE 2019*", en el cual concretamente, señala:

"(…)

Que se hace necesario para la alcaldía municipal de Cajibío (Cauca) adecuar la jornada laboral de acuerdo con las necesidades de la institución y ejercer control de asistencia de los funcionarios mediante el sistema biométrico implementado, para lo cual se establecen los horarios dentro de los que se prestaran los servicios, respetando la jornada máxima establecida por la ley.

Que con la expedición del Decreto Municipal No. 0041 del 09 de abril de 2019, no se estipulo el tiempo para realizar la socialización, capacitación, pedagogía e instrucción a los funcionarios públicos de la administración municipal, frente al funcionamiento del sistema biométrico que se implementará para realizar el registro y control de la asistencia de los mismos a la entidad, motivo por el cual se efectuara (sic) la pedagogía necesaria para que entre en funcionamiento el nuevo sistema de control y registro biométrico en la entidad hasta el miércoles 15 de mayo de 2019.

En mérito de lo expuesto.

DECRETA:

***ARTÍCULO PRIMERO:** Adicionar el artículo Noveno del Decreto 0041 de 09 de abril de 2019, el cual quedará así:*

***ARTÍCULO NOVENO: VIGENCIA:** El presente decreto, iniciará a regir a partir de su publicación, sin embargo para su implementación se tendrá en cuenta las siguientes Etapas: **ETAPA DE SOCIALIZACIÓN Y PEDAGOGÍA**. Establecer como periodo de instrucción del sistema biométrico, adoptado a través del Decreto Municipal 0041 del 09 de abril de 2019 desde la publicación del acto administrativo y hasta el martes catorce (14) de mayo de 2019. **ETAPA DE IMPLEMENTACIÓN**: El sistema biométrico adoptado por la administración municipal de Cajibío (cauca), entrará en vigencia a partir del miércoles quince (15) de mayo de 2019."*

c. **Copia del DECRETO NO. 00082 DEL 26 DE JULIO DE 2019**[21], que derogó el Decreto No. 00041 del 9 de abril de 2019, para incorporar lo siguiente:

"*La Ley 1581 de 2012, tiene por objeto "… desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma…"*

1. El artículo 3 de la Ley 1581 de 2012, no establece restricción o requisito que exija autorización alguna, sino establece o clarifica las definiciones.
*2. Mas (sic) adelante, el artículo ibídem, establece, cuando **no se requiere** autorización para el manejo de datos, a saber:*

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

[20] Folios 47 al 48.
[21] Folios 49 al 52.

(…)

El Municipio de Cajibío, como entidad pública y empleador, en el marco de la Ley y los Decretos Reglamentarios, requiere implementar medidas, con el fin de garantizar por parte de los funcionarios públicos, el cumplimiento del horario establecido, en el manual de funciones del Municipio, el cual es ampliamente conocido por los empleados públicos, razón por la cual nos encontramos en la excepción establecida en el literal "a" del artículo 10 ibídem.

Es de aclarar que la huella, necesaria para el funcionamiento del sensor biométrico, y esta información, no será divulgada o entregada a terceros, además los datos no se encuentran en las hojas de vida de los funcionarios públicos, adscritos a la planta de personal, además estos datos, que deben ingresarse en el sensor de huella, no son para difundirlos, ni colocarlos en conocimiento de terceros.

En mérito de lo expuesto,

DECRETA

(…)

***ARTÍCULO CUARTO:** control de asistencia: Adóptese el Sistema Biométrico para el Control de acceso y asistencia de los funcionarios de la Alcaldía Municipal de Cajibío (Cauca).*

***PARÁGRAFO PRIMERO:** Los Funcionarios de la Alcaldía Municipal de Cajibío, deberán realizar el registro ante el Sistema de Control Biométrico, ubicado en el Despacho de la Secretaría de Gobierno, Tránsito y Transporte y Participación Comunitaria. Labor que debe realizar todos los funcionarios entre el 30 de julio al 06 de agosto de 2019.*

***PARÁGRAFO SEGUNDO: ETAPA DE SOCIALIZACIÓN.** Establecer como periodo de socialización del presente decreto del 30 de julio al 06 de agosto de 2019.*

***PARÁGRAFO TERCERO: ETAPA DE IMPLEMENTACIÓN:** El sistema biométrico, entrará en vigencia a partir del siete (07) de agosto de 2019.*

***PARÁGRAFO CUARTO:** El sistema biométrico y los registros de asistencia que se produzca mediante su uso sera (sic) administrados y Controlados por el Secretario de Gobierno, Tránsito y Transporte y Participación Comunitaria del Municipio.*

***ARTÍCULO QUINTO:** A partir del siete (07) de agosto de 2019, el alcalde Municipal, descontará del sueldo, los retardos injustificados de acuerdo con la información que arroje el Sistema Biométrico, lo anterior de acuerdo a lo señalado por la Honorable Corte Constitucional al establecer que resulta improcedente reconocer y pagar salarios por servicios no prestados efectivamente a la entidad sin justificar legal, cada vez que ello implicaría permitir un enriquecimiento sin causa a favor del servidor en detrimento de la administración pública (Sentencia T-927 del 10 de octubre de 2003 y T-331 A del 2 de mayo de 2006) y el artículo 2.2.5.4.17 del Decreto Ley 648 de 2017."*

(…)".

(iii) Por su parte, mediante escrito del 27 de agosto de 2019, con radicado 19-89199-7[22], el municipio **RECURRENTE** le precisó a la Dirección lo siguiente:

"*La relación entre la administración pública y los funcionarios es **legal y reglamentaria,** la cual está regulada por la Ley, Decretos reglamentarios y el Manual de Funciones y el marco de estas disposiciones tenemos:*

[22] Folios 26 al 38.

Por medio de Decreto – Ley 1074 de 1978 se estableció las horas que componen como límite máximo la jornada laboral de los empleados públicos, en los siguientes términos:

Artículo 33º- De la Jornada de trabajo. La asignación mensual fijada en las escalas de remuneración a que se refiere el presente Decreto, corresponde a jornadas de cuarenta y ocho horas semanales. A los empleos cuyas funciones implican el desarrollo de actividades discontinuas, intermitentes o de simple vigilancia podrá señalarse una jornada de trabajo de doce horas, sin que en la semana exceda un límite de 66 horas.

El numeral 11 del artículo 34, de la Ley 734 de 2002, (Artículo derogado a partir del 1 de julio de 2021, por el artículo 265 de la Ley 1952 de 2019) establece como deber de los servidores públicos "Dedicar la totalidad del tiempo reglamentario de trabajo al desempeño de las unciones (sic) encomendadas, salvo las excepciones legales".

En el numeral 2 del artículo 22 de la Ley 909 de 2004, se establece la ordenación de la jornada laboral "en las plantas de personal de los diferentes organismos y entidades a las que se aplica la presente ley se determinará qué empleos corresponden a tiempo completo, a tiempo parcial y cuáles a medio tiempo, de acuerdo con la jornada laboral establecida en el Decreto-ley 1042 de 1978

(…)

En el Decreto Municipal 0095 de 2017 (…) se establece como función propia del Alcalde Municipal: "Dirigir la acción administrativa del municipio; asegurar el cumplimiento de las funciones y la prestación de los servicios a su cargo; representarlo judicial y extrajudicialmente: y nombrar y remover a los funcionarios bajo su dependencia y a los gerentes o directores de los establecimientos públicos y las empresas industriales o comerciales de carácter local, de acuerdo con las disposiciones pertinentes.

Mediante Decreto Municipal 0014 del 22 de enero de 2014 se estableció el horario de trabajo para la Alcaldía Municipal de Cajibió (Cauca).

Es así Como la administración municipal de Cajibió, por medio del proceso contractual N° SMC-CC-F39-010-2019, adquirió el servicio de suministro con el objeto de contractual "EL SISTEMA BIOMÉTRICO DE CONTROL DE ASISTENCIA DE PERSONAL DE LA ALCALDÍA MUNICIPAL DE CAJIBIO CAUCA A TRAVÉS DE LA HUELLA DIGITAL" para el control de acceso y asistencia de los funcionarios de la alcaldía municipal de Cajibío (Cauca), a efectos de poder tener un registro de los horarios de entrada y salida de los empleados a las instalaciones de la alcaldía municipal."

De acuerdo con los antecedentes expuestos, este Despacho encuentra, como lo describe el ente **RECURRENTE**, que existe un régimen especial que reglamenta las relaciones laborales de las entidades del orden nacional con los empleados públicos, en este caso, el Decreto 1042 de 1978; ámbito de aplicación que fue extendido para las entidades del orden departamental y municipal mediante la Ley 27 de 1992. Al respecto, en Sentencia del 9 de diciembre de 2019, la Sala de Consulta y Servicio Civil del Consejo de Estado conceptuó lo siguiente:

"*Es reiterada la jurisprudencia de la Sección Segunda del Consejo de Estado en el sentido de que las normas que rigen la «administración de personal» de los empleados públicos del orden territorial es el contenido en el Decreto Ley 1042 de 19783, según se aprecia a continuación»:*

«Si bien el Decreto 1042 de 1978 en principio rigió para los empleados de la rama ejecutiva del orden nacional, el artículo 3 (sic) 4 de la Ley 27 de 1992 hizo extensiva a las entidades territoriales las disposiciones que regulan el régimen de administración de personal contenidos no solamente en la norma citada, sino en los decretos leyes 2400 y 3074 de 1968, Ley 13 de 1984 y 61 de 1987, sus decretos reglamentarios y las normas que las modifiquen o

adicionen. La extensión de dicha normatividad fue reiterada por el artículo 87, inciso segundo, de la Ley 443 de 1998.

El Decreto 1042 de 1978 aplica para los empleados de la rama ejecutiva en el orden territorial, en materia de jornada de trabajo y trabajo en días de descanso obligatorio, pues la remisión inicial que hizo la Ley 27 de 1992 no solamente mencionó el régimen de carrera administrativa, sino también el régimen de administración de personal, el cual, dentro de una interpretación amplia, comprende así mismo el concepto de jornada de trabajo.

La Sala prohíja una vez más, en esta oportunidad, la tesis ya definida por la jurisprudencia sobre la normatividad aplicable a los empleados territoriales en materia de jornada laboral y el trabajo en días de descanso obligatorio, pues además de lo expuesto, debe considerarse adicionalmente que partiendo de que el régimen de administración de personal civil contenido en el Decreto 2400 de 1968 se refiere a la clasificación de empleos, condiciones para el ejercicio del empleo (ingreso, deberes, derechos, prohibiciones, régimen disciplinario, calificación de servicios, situaciones administrativas, retiro del servicio), capacitación, carrera administrativa, organismos para la administración de personal, resulta válido afirmar que la jornada de trabajo es un concepto que hace parte de la noción genérica de administración de personal"

De esta manera, las normas que rigen la «administración de personal» de los empleados públicos del orden territorial son las contenidas en el Decreto Ley 1042 de 1978."[23]

Ahora bien, conforme al artículo 33 del decreto arriba mencionado, la jornada laboral corresponde a 44 horas semanales, la cual deberá ser cumplida de lunes a sábado; sin embargo, el jefe de la entidad podrá distribuir dicha jornada compensando el sábado con tiempo diario adicional en los restantes. Precisa la Sala de Consulta y Servicio Civil del Consejo de Estado:

"Como se observa, la disposición transcrita no solo refiere a la noción de jornada laboral, sino también a la de horario de trabajo.

La jornada laboral en el sector público es aquel tiempo máximo establecido por la ley, durante el cual los empleados deben cumplir o desarrollar las funciones previamente asignadas por la Constitución, la Ley o el reglamento.

El artículo 33 del Decreto Ley 1042 de 1978 señala que la regla general aplicable a los empleos públicos del nivel nacional o territorial corresponderá a una jornada laboral de cuarenta y cuatro (44) horas semanales, la cual se encuentra vigente pues no existe reglamentación posterior a ella, como lo reconoce la remisión hecha por el artículo 22 de la Ley 909 de 2004, citado.

De otra parte, el horario de trabajo, esto es la distribución de la jornada laboral según las necesidades de cada entidad, dependerá de las funciones impuestas y las condiciones en que deban ejecutarse. De conformidad con lo dispuesto como regla general en el artículo 33 del Decreto Ley 1042 de 1978, es una competencia administrativa del jefe de la entidad establecer el horario de trabajo que deben cumplir los servidores públicos, dentro del límite de la jornada laboral de 44 horas semanales."[24].

Así mismo, los numerales 7 y 10 del artículo 91 de la Ley 136 de 1994, modificado por el artículo 29 de la Ley 1551 de 2012, consagran las siguientes funciones en cabeza del Alcalde Municipal en relación con la Administración Municipal:

"(…)

---

[23] Cfr. Consejo de Estado, Sala de Consulta y Servicio Civil. Consejero Ponente: Álvaro Namén Vargas En: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=105933#2422

[24] Ibídem.

> ***7.*** *Velar por el cumplimiento de las funciones de los empleados oficiales municipales y dictar los actos necesarios para su administración.*
>
> *(…)*
>
> ***10.*** *Ejercer el poder disciplinario respecto de los empleados oficiales bajo su dependencia.*
>
> *(…).”*

Es importante agregar en esta línea de análisis que el cumplimiento de la jornada laboral es una obligación del servidor público, pues así lo establece el literal 11 del artículo 34 del Ley 734 de 2002 (derogado por el numeral 12 del artículo 38 de la Ley 1952 de 2019).

Por todo lo anterior, es claro que el municipio **RECURRENTE** cuenta con la facultad legal para (i) fijar la jornada laboral de sus trabajadores; (ii) controlar el acceso a las instalaciones; (iii) verificar el cumplimiento del horario y sus funciones; (iv) iniciar las actuaciones disciplinarias en caso de un posible incumplimiento.

Bajo ese entendido, el Tratamiento de los datos de los empleados por parte de la entidad públicas para fines de “*garantizar el cumplimiento del horario”*[25], está plenamente soportado en una obligación legal aplicable al ente territorial, razón por la cual, en este caso, no se requiere el consentimiento de los Titulares para dicho propósito específico.

No obstante lo anterior, aunque el municipio **RECURRENTE** no requiere contar con el consentimiento de los funcionarios para tratar la información personal para el “*control de acceso y asistencia”*, advierte el Despacho que el ente territorial no acreditó, al menos sumariamente, que:

1. Incorporó salvaguardas significativas, incluida una referencia a la naturaleza voluntaria del suministro de la huella para ser procesada a través de un sistema de lectura biométrica.

2. Si contaba con otros mecanismos para lograr el fin propuesto por ellos, en caso en que un empleado se negaré a suministrar su huella para ser procesada a través de un sistema biométrico, de conformidad con el párrafo final del artículo 2.2.2.25.2.3, arriba citado.

3. Si el sistema biométrico de lectura de huella dactilar era el único mecanismo efectivo para garantizar el cumplimiento del horario por parte de los empleados.

4. Si la finalidad perseguida por ellos podría alcanzarse con otros mecanismos menos intrusivos o lesivos para los derechos y libertades de los Titulares concernidos. Son métodos menos intrusivos el uso de etiquetas RFID o tarjetas de banda magnética, que no requieren el Tratamiento de datos biométricos.

5. Si se hubiera presentado un abuso de los sistemas ya implementados, entre ellos, situaciones de fraude; circunstancia que hubiera podido justificar la necesidad de la implementación del lector de huella biométrica.

Con ocasión a todas las anteriores consideraciones, en el entendido que no se ha implementado todavía el sistema de huella biométrico (Folio 85, reverso), este Despacho procederá a modificar los artículos primero y segundo de la Resolución No. 69434 del 4 de

[25] Folio 27, reverso.

diciembre de 2019, respectivamente, en el sentido de ordenarle al **MUNICIPIO DE CAJIBÍO, CAUCA**:

Primero: Antes de poner en marcha el sistema biométrico, evaluar si el mismo es el adecuado, pertinente y no excesivo en relación con la finalidad perseguida por el ente municipal. O, por el contrario, si existen otros mecanismos menos lesivos o invasivos para los Titulares, es decir, que no requieran el Tratamiento de datos de carácter sensible, pero que al mismo tiempo, le permitan cumplir con las obligaciones legales a las que está sujeto. En el evento que el sistema biométrico no sea estrictamente necesario para el fin perseguido, el **MUNICIPIO DE CAJIBÍO, CAUCA** deberá implementar un sistema menos lesivo para los derechos y libertades de las personas

Segundo: Contar con una alternativa que no requiera el Tratamiento de datos sensibles, en el caso en que un empleado se rehúse a suministrar su huella digital.

4.4. DEL DEBER DE ADOPTAR UN MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS PARA GARANTIZAR EL ADECUADO CUMPLIMIENTO DE LA LEY 1581 DE 2012.

El municipio **RECURRENTE** manifiesta que en Decreto No. 00082 de 26 de julio de 2019, ese ente adoptó la Política de Tratamiento de Información Personal de que trata el Decreto 1074 de 2015, razón por la cual, "*la afirmación que no se cuenta con MANUAL PARA EL MANEJO DE DATOS SENSIBLES, no es cierto, por lo tanto, solicitamos se analice el Decreto*."

Agrega que el ente *"suscribió el documento COMPROMISO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN, documentos que fueron nombrados y relacionados en el oficio remitido a la Superintendencia, sin embargo, en esta oportunidad se anexa una copia*."

Antes de entrar a decidir sobre el fondo del asunto, así como las peticiones planteadas por el municipio **RECURRENTE**, este Despacho pone de presente, en primer lugar, que las medidas adoptadas posteriormente a la entrada en vigencia de la Ley 1581 de 2012 como de sus normas reglamentarias, entre ellos, contar con una Política de Tratamiento de Información Personal, no subsana el hecho que ese ente territorial se haya abstenido u omitido cumplir con esa regulación por más de 6 años. La norma estatutaria entró en vigencia el 18 de octubre de 2012.

En segundo lugar, este Despacho aclara que la Política de Tratamiento de Información Personal de que trata el artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015 es un documento diferente al Manual Interno de que trata el literal k) del artículo 17 de la Ley 1581 de 2012, pues, como se explicará a continuación, son documentos que obedecen a fines diferentes bajo la normatividad en protección de datos personales:

a) Política de Tratamiento de Información Personal:

La Política de Tratamiento de Información personal es una herramienta que permite a los Titulares: (i) pedir, en cualquier tiempo, cuentas a los Responsables del Tratamiento; (ii) controlar el uso que se le están dando a sus datos personales; y, (ii) conocer donde puede ejercer sus derechos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización.

La política debe ser transparente y de fácil acceso para los Titulares, ya sea por medio escrito[26], formato electrónico[27] o cualquier otra tecnología disponible, siempre y cuando cumpla con el deber de informar sobre el uso que se le está dando o dará a los datos personales recolectados. Dicho documento debe además estar redactado en un lenguaje sencillo y claro.

El requisito de que el lenguaje sea claro y sencillo significa que la política sea comprensible para el tipo de audiencia; esto reviste una especial importancia cuando se trata de niños, niñas o adolescentes, personas con alguna discapacidad, tercera edad, o aquellos que no hablen el idioma castellano, etc., razón por la cual, en una política de tratamiento se debe evitar, pero no limitado a: (i) contener un lenguaje o terminología de naturaleza excesivamente legal, técnica o especializada; (ii) incluir ambigüedades, oraciones y estructuras lingüísticas complejas.

Así mismo, los Responsables del Tratamiento deberán poner en conocimiento al Titular de la Información, **a más tardar al momento de la recolección de los datos personales**, la Política de Tratamiento y el Aviso de Privacidad, en los casos en los que no sea posible poner a disposición de ellos la política.

b) Manual Interno de Políticas y Procedimientos para garantizar el adecuado cumplimiento de la Ley 1581 de 2012:

El Manual Interno es un documento escrito donde se detalla de una manera precisa las políticas, procesos y procedimientos implementados por un Responsable del Tratamiento al interior de la organización para cumplir con lo que ordena la Ley 1581 de 2012 y sus normas reglamentarios, teniendo en cuenta su estructura organizativa y tamaño, la naturaleza, el alcance, el contexto y los fines del tratamiento de datos, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de los Titulares de los Datos.

Este documento incluye, pero no limitado a: (1) descripción de roles y responsabilidades, (2) sistemas de gestión de incidentes de seguridad en datos personales, (3) desarrollo de evaluaciones de impacto en protección de datos y sistemas de auditorías, (4) sistemas para promover la conciencia y la capacitación de los empleados y/o contratistas sobre las políticas y prácticas de protección de datos del Responsable del Tratamiento, (5) política de transferencia y transmisión de datos personales, ya sea nacional o internacional, (6) políticas de seguridad y confidencialidad de información personal, (7) procedimiento para la recolección, almacenamiento, uso, circulación y supresión de datos personales, (8) persona o área encargada de gestionar el programa de protección de datos personales. Debido a la naturaleza e impacto del Tratamiento sobre los Titulares, datos de carácter sensible o de niños, niñas y adolescentes, Tratamiento a gran escala, etc., es trascendental que el manual incorpore políticas, procesos y procedimientos más robustos.

De igual manera, el Manual Interno le permite al Responsable del Tratamiento establecer internamente cómo se gestionará los requerimientos presentados por los Titulares, así como los lineamientos que deben seguir los empleados para asegurar que en ese trámite el Responsable del Tratamiento cumpla con lo que establece la Ley 1581 de 2012 y sus decretos reglamentarios.

---

[26] Por ejemplo: medios impresos, anuncios impresos, formularios, etc.
[27] Electrónicamente - en mensajes de texto; en los sitios web; en correos electrónicos; en aplicaciones móviles.

Hechas las anteriores precisiones, entra esta Delegatura a determinar si en efecto el municipio **RECURRENTE** cumplió con sus obligaciones legales de contar con una Política de Tratamiento de Información Personal y Manual Interno:

1. El "*MANUAL DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES": Código: F-ICI-01. Versión: 01. Fecha: 02-04-2019*"[28] fue aprobado en el año 2019. Se concluye, por tanto, que dicho instrumento fue documentado, como se señaló en líneas anteriores, con mucha posterioridad a la entrada en vigencia el Régimen General de Protección de Datos Personales.

2. Ahora, más allá del debate sobre la fecha en que fue aprobado el "*MANUAL DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES*" por parte del ente municipal, este Despacho encuentra que ese documento no cumple con la Ley 1581 de 2012 ni con el Decreto 1074 de 2015, por las siguientes razones:

- El texto, según su contenido, sólo está dirigido al procesamiento de los datos biométricos de los empleados. El municipio **RECURRENTE** omite, en este punto, que ellos recolectan información de otra clase de Titulares, por ejemplo, contratistas, ciudadanos, proveedores, etc., e incluso trata otras categorías de datos relacionados con los mismos empleados.

- El documento para ser una "Política de Tratamiento" carece de la siguiente información:

¿Qué información requiere proporcionar el Responsable del Tratamiento?	**Cumple**	**Observación**
Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.	**SI**	
Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.	**NO**	Solo incluye el Tratamiento de empleados, así como la de contratistas y proveedores. Tampoco incluye aquellas finalidades que escapan del ámbito laboral y/o contractual, si aplica.
Derechos que le asisten como Titular.	**NO**	**No se incluye.**
Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.	**NO**	**No es claro.**
Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.	**NO**	**No se incluye.**
Fecha de entrada en vigencia de la política de tratamiento de la	**SI**	**04 de abril de 2019.**

[28] Folios 90 al 94.

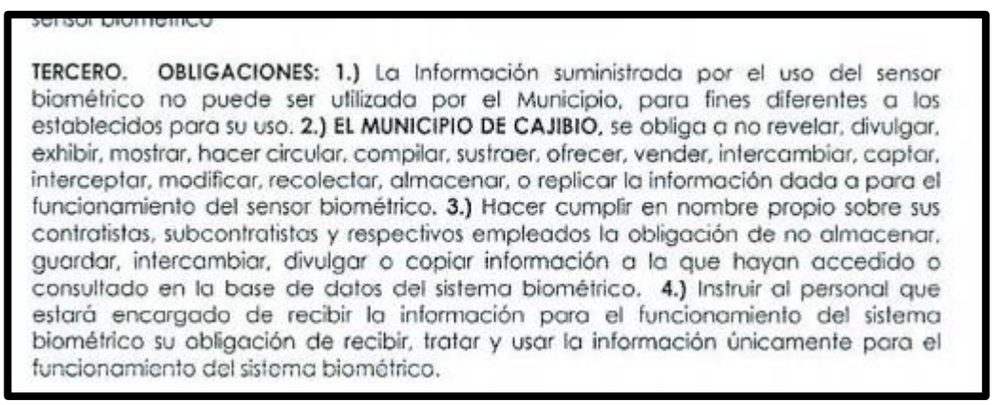
información y período de vigencia de la base de datos.		

- El documento tampoco se puede considerar como el Manual Interno de Políticas y Procedimientos de que trata el literal k) del artículo 17 de la Ley 1581 de 2012, pues, como se señaló en párrafos anteriores, este documento no sólo debe estar limitado a reproducir textualmente lo que señala la ley, sino que, por el contrario, este debe incluir un conjunto de políticas, procesos y procedimientos para que el Responsable del Tratamiento garantice efectivamente el cumplimiento de la regulación en materia de protección de datos personales.

- En el texto se le está asignando "*el manejo, recolección, y uso del sistema biométrico*" al Secretario de Gobierno y Tránsito y Transporte y Participación Comunitaria. No obstante, este Despacho encuentra que el ente territorial no ha efectuado un análisis detallado para determinar si en efecto el secretario actúa como Encargado del Tratamiento de que trata el literal d) del artículo 3º de la Ley 1581 de 2012[29].

  En este punto, es necesario destacar que, tratándose de operaciones de transmisión de datos personales entre un Responsable a un Encargado, es necesario que las partes suscriban un contrato o cualquier acto jurídicamente vinculante que regule ese flujo de información personal, de conformidad con lo previsto en la Ley 1581 de 2012 y sus decretos reglamentarios; documento que no se vislumbra por ninguna parte de los documentos aportados por el municipio **RECURRENTE**.

- Sin que sea la intención de la Delegatura profundizar si todas las personas que intervienen en el conjunto de operaciones de tratamiento de datos personales en custodia o posesión del ente municipal cuentan (o no) con un acuerdo de confidencialidad, el texto "*DOCUMENTO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN"*[30] evidencia que el municipio **RECURRENTE** sólo ha implementado un acuerdo de confidencialidad para una persona y un tipo de tratamiento en específico, prescindiendo, por ejemplo, tal como lo señala el mismo artículo 3º del documento en mención, que otras personas pueden tener acceso a la información.



sensor biométrico

TERCERO. OBLIGACIONES: 1.) La Información suministrada por el uso del sensor biométrico no puede ser utilizada por el Municipio, para fines diferentes a los establecidos para su uso. **2.) EL MUNICIPIO DE CAJIBIO,** se obliga a no revelar, divulgar, exhibir, mostrar, hacer circular, compilar, sustraer, ofrecer, vender, intercambiar, captar, interceptar, modificar, recolectar, almacenar, o replicar la información dada a para el funcionamiento del sensor biométrico. **3.)** Hacer cumplir en nombre propio sobre sus contratistas, subcontratistas y respectivos empleados la obligación de no almacenar, guardar, intercambiar, divulgar o copiar información a la que hayan accedido o consultado en la base de datos del sistema biométrico. **4.)** Instruir al personal que estará encargado de recibir la información para el funcionamiento del sistema biométrico su obligación de recibir, tratar y usar la información únicamente para el funcionamiento del sistema biométrico.

Todo lo anterior implica que el ente territorial está desconociendo el principio de confidencialidad incorporado en el literal f), del artículo 4 de la Ley 1581 de 2012, que dice:

---

[29] "***ARTÍCULO 3o. DEFINICIONES.*** *Para los efectos de la presente ley, se entiende por: (…) 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; (…)".*

[30] Folios 93 reverso al 94.

"***ARTÍCULO 4o. 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:*

(…)

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."*[31]*.*

- Pese a que el municipio **RECURRENTE** insiste en que "*no ha iniciado con la recolección de datos sensibles, que sean objeto de protección, por lo tanto, las políticas del tratamiento de los datos personales, no le son aplicables*," no escapa a este Despacho el hecho de que, tanto la Política de Tratamiento de Información Personal como el Manual Interno de Políticas y Procedimientos, se deben aplicar al Tratamiento de todos los datos personales bajo custodia o posesión del ente territorial, no sólo a un tipo de procesamiento en concreto.

Bajo todas las circunstancias anteriormente descritas, encuentra este Despacho que los argumentos expuestos por el municipio **RECURRENTE** no están llamados a prosperar, razón por la cual, se confirmará las órdenes emitidas por la Dirección de Investigación de Protección de Datos Personales.

QUINTO: Aunque las razones anteriores son suficientes para confirmar la Resolución No. No. 69434 del 4 de diciembre de 2019, esta Delegatura considera pertinente destacar lo siguiente:

5.1. RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY) EN EL TRATAMIENTO DE DATOS PERSONALES EN EL SECTOR PÚBLICO.

El cumplimiento de la Ley 1581 de 2012 es un elemento indispensable para generar confianza en la población respecto del Tratamiento de sus datos personales, tanto por las organizaciones privadas como por las entidades públicas.

"*La confianza se entiende como la expectativa de que "se puede contar con la palabra del otro" y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera recíproca. Cuando existe confianza, la persona cree que la empresa es fiable, cumple su palabra, es sincera, íntegra y lleva a cabo las acciones prometidas*"[32].

La confianza requiere que los Responsables del Tratamiento demuestren un alto nivel de lealtad, transparencia y responsabilidad en la recolección, uso y divulgación de los datos personales.

Tratándose de entidades públicas, ese nivel de diligencia es mayor, ya sea por la cantidad de información personal bajo su custodia, el conjunto de datos de poblaciones o subconjuntos de poblaciones, la sensibilidad de la información o relacionada con niños, niñas

---

[31] Ley 1581 de 2012, artículo 4, literal f).

[32] Superintendencia de Industria y Comercio (SIC), GUÍA SOBRE EL TRATAMIENTO DE DATOS PERSONALES PARA FINES DE COMERCIO ELECTRÓNICO, en: https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf

y adolescentes o personas vulnerables, la duración de los programas o actividades gubernamentales, o el uso de la información personal como parte de un proceso de toma de decisiones que pueden afectar directamente a los ciudadanos.

Conforme al principio de legalidad, el Tratamiento de los datos personales es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen (Literal a), artículo 4º de la Ley 1581).

Por su parte, el principio de transparencia obliga a los Responsables a informar a los ciudadanos, en cualquier momento y sin restricciones, información acerca de la existencia de los datos que le conciernan (Literal e), artículo 4º de la Ley 1581).

Como se señaló en la Guía sobre el Tratamiento de Datos Personales para fines de comercio electrónico, "*una organización transparente puede generar mayor confianza en sus clientes y en los Titulares de los datos*."[33]. Son medidas para garantizar el principio de transparencia: mantener canales abiertos de comunicación y divulgación del uso de los datos personales o cumpliendo en la práctica lo que se dice o promete en las Políticas de Tratamiento de Información.

Unido a ellos, el principio de responsabilidad demostrada le impone a los Responsables del Tratamiento el deber de garantizar la eficacia de los derechos del Titular, la cual no puede ser simbólica ni formal, sino ser una realidad. Téngase presente que según nuestra jurisprudencia "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante"*[34]*.*

El artículo 2.2.2.25.6.1[35] del Decreto 1074 de 2015 requiere que los Responsables del Tratamiento demuestren que han implementado medidas apropiadas y efectivas para garantizar el correcto cumplimiento de los deberes que imponen la Ley 1581 y sus normas reglamentarias. Acorde al artículo 2.2.2.25.6.2 del mismo decreto, dichas políticas deberán garantizar lo siguiente:

> *"1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este capítulo.*
> *2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.*
> *3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento."*

---

[33] Ibídem.
[34] Cfr. Corte Constitucional, sentencia T-227 de 2003.
[35] El texto completo del artículo 2.2.2.25.6.1 del Decreto 1074 de 2015 ordena lo siguiente: Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:
1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.
En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas".

Las anteriores medidas deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

Ahora, con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la "*Guía para implementación del principio de responsabilidad demostrada (accountability)*"[36]. La guía trate las siguientes recomendaciones:

1. Diseñar y activar un programa integral de gestión de datos. Esto exige compromisos y acciones concretas de los directivos de la organización. Igualmente requiere la implementación de controles de diversa naturaleza.
2. Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP, y
3. Demostrar el debido cumplimiento de la regulación sobre Tratamiento de datos personales.

Un programa integral de gestión de datos, con prácticas transparentes y efectivas, puede ayudar a generar confianza tanto en las organizaciones como en las entidades públicas, al demostrar debida diligencia por parte de ellas en el cumplimiento de los requisitos legales, así como con los principios rectores establecidos en la ley 1581 de 2012.

Ahora bien, el reto de las entidades públicas frente al principio de responsabilidad demostrada va mucho más allá de la mera expedición de documentos o redacción de manuales, requiere que ellas incorporen la protección de datos personales como una política pública.

Una política pública en materia de protección de datos personales busca que la Ley 1581 de 2012 sea parte integral de cualquier iniciativa normativa, programa político, actividad o proyecto que involucren datos personales. En efecto, tener en cuenta el Régimen General de Protección de Datos supone adoptar un conjunto de medidas adecuadas y necesarias, que logren transformar la estructura de la entidad pública, de forma tal, que se asegure que todo proyecto o iniciativa, desde el diseño y por defecto, sea respetuosa de los derechos y libertades de los Titulares de la Información, en particular los derechos a la protección de datos y privacidad.

Este Despacho debe señalar, por ejemplo, que de acuerdo con las "*Directrices para evaluar la proporcionalidad de las medidas que limitan los derechos fundamentales a la privacidad y a la protección de datos personales*"[37] del Supervisor Europeo de Protección de Datos (en adelante "SEPD"), una medida de política pública es que los derechos a la protección de los datos y la privacidad sean tenidos en cuenta cuando las entidades públicas diseñan sus programas institucionales, adoptan una medida regulatoria o una decisión administrativa general, o proyectan decretos y resoluciones - en el caso concreto, el Decreto Municipal No. 0041 del 9 de abril de 2019, que adoptó el sistema biométrico para el control de asistencia de los funcionarios públicos de la alcaldía municipal de Cajibío (Cauca)-, o implementan nuevas tecnologías.

Agrega el SEPD que para "*garantizar que la protección de datos se convierta en una parte integral de la formulación de políticas de la UE requiere no sólo una comprensión de los principios expresados en el marco legal y en la jurisprudencia pertinente, pero también un*

---

[36] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

[37] Supervisor Europeo de Protección de Datos (EDPS), "EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data.", en https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

enfoque práctico y creativo en soluciones a complejo problemas, con prioridades políticas a menudo en competencia." Para facilitar el cumplimiento de ese objetivo, el SEPD establece la realización de un test de necesidad y uno de proporcionalidad.

El concepto de necesidad implica una evaluación combinada, basada en hechos, tanto de la efectividad de la medida pensada para el objetivo administrativo perseguido como si la misma es menos intrusiva en comparación con otras opciones para lograr el mismo fin. Mientras que el concepto de proporcionalidad prevé una evaluación respecto a cuáles "salvaguardas" deben acompañar la medida (por ejemplo, en la adopción de un sistema biométrico) para reducir los posibles riesgos que se generan para los derechos y libertades de los Titulares, a un nivel "aceptable". Si el proyecto de medida no pasa la prueba de necesidad, no hay necesidad de examinar su proporcionalidad.[38]

Por lo tanto, implementar los tests de proporcionalidad y necesidad ayudará a las entidades públicas a establecer de manera preliminar el impacto que tendrá una iniciativa normativa, que involucre datos personales en los derechos y libertades de los Titulares de la Información, en particular cuando se trate de propuestas de monitoreo sistemático a gran escala, proceso de toma de decisiones automatizadas, uso de una tecnología innovadora, etc. En esa misma línea, les evitará la pérdida de confianza de la población en el Tratamiento de los datos personales por parte de las entidades, e incurrir en costos innecesarios o soluciones inadecuadas.

Es importante aclarar que los tests de necesidad y proporcionalidad no tienen la intención de identificar, evaluar y tratar en detalle los riesgos asociados a un tipo específico Tratamiento de datos personales, pues esa es la tarea de la "Evaluación de Impacto en Protección de Datos (o Evaluación de Impacto en Privacidad)". Por el contrario, estos conceptos tienen como objetivo determinar de una manera abstracta si la iniciativa normativa debe ser replanteada.

Sobre este último punto, subraya el SEPD: "*la proporcionalidad podrían ser considerada como un "Evaluación de Impacto sobre la ley" (para realizarse en el contexto de la función de asesoramiento sobre medidas legislativas impacto en el derecho a la privacidad y a la protección de datos personales). No obstante, puede ser útil observar que muchos de los factores que son relevantes para realizar la [EIPD] son también relevantes para la evaluación de los costos de privacidad de una medida legislativa.*[39]

En virtud de todo lo anterior se exhortará al Representante Legal del **MUNICIPIO DE CAJIBIÓ**, para que adopte medidas pertinentes, útiles, efectivas y verificables con miras, pero no limitado, a:

1. Respetar los derechos de los Titulares al acceso, actualización, rectificación o supresión de los datos personales en custodia del ente territorial, así como la revocatoria de la autorización, si aplica.

2. Hacer efectivo el pleno respeto de los principios rectores en materia de protección de datos personales.

3. Garantizar que la protección de datos personales se convierta en una parte integral de la formulación de políticas públicas del municipio.

[38] Ibídem. Traducción no oficial.
[39] Ibídem.

4. Asegurar que en cualquier proyecto, propuesta, iniciativa o actividad, que involucre datos personales, se realicen los tests de necesidad y proporcionalidad, a fin de que se logre el objetivo administrativo perseguido, pero al mismo tiempo proteja los derechos a la protección de datos personales y privacidad de los Titulares de la Información.

5. Realizar evaluaciones de impacto para identificar, evaluar y gestionar los riesgos asociados al Tratamiento de los datos personales bajo custodia o posesión del ente municipal. Dicha evaluación debe estar documentada y ser permanente, a fin de determinar su nivel de eficacia en cuanto al cumplimiento de la normatividad y evitar que se vulneren los derechos de los Titulares.

6. Determinar si el sistema biométrico adquirido por el ente municipal cumple con requisitos de calidad[40]exactitud, seguridad y confidencialidad para proteger los datos personales procesados por esta herramienta. Adicionalmente, implementar mecanismos de auditoría para garantizar el cumplimiento de los mismos.

7. Establecer cuál es el rol que está desempeñando la Secretaría de Gobierno y Tránsito y participación Comunitaria en el Tratamiento de los datos personales bajo custodia y posesión de la alcaldía municipal, de conformidad con los conceptos de Responsables y Encargados del Tratamiento que trae el artículo 3º de la Ley 1581 de 2012.

8. Cumplir las órdenes emitidas por la Dirección de Investigación de Protección de Datos Personales, confirmadas mediante la presente resolución.

Por lo anterior, este Despacho invita al municipio **RECURRENTE** para que tenga en cuenta las orientaciones de la Superintendencia de Industria y Comercio incorporadas en la "*Guía para implementación del principio de responsabilidad demostrada (accountability)*"[41].

SEXTO: Sin perjuicio de lo previamente establecido, este Despacho no accede a las peticiones del municipio **RECURRENTE** por las siguientes razones:

a) La Ley Estatutaria 1581 de 2012 es neutral tecnológica y temáticamente. Ello significa que aplica a cualquier Tratamiento con independencia de las técnicas, procesos o tecnologías *–actuales o futuras-* que se utilicen para dicho efecto. Por ende, debe observarse y aplicarse en la recolección, uso y Tratamiento de datos personales al margen de las "innovaciones tecnológicas" que usen para dicho efecto.

b) La recolección, uso, circulación y tratamiento de datos sensibles debe estar rodeado de especial cuidado y diligencia en su recolección, uso, seguridad o cualquier otra actividad que se realice con los mismos. La Corte Constitucional exige **responsabilidad reforzada** por parte de los Responsables y Encargados: "*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*"[42] de la Ley Estatutaria 1581 de 2012.

c) La recolección de datos sin autorización no significa que quede sin protección esa información y los ciudadanos titulares de los datos. En efecto, la parte final del artículo 10

---

[40] La no calidad de un sistema biométrico puede dar lugar a falsos rechazos o a falsas correspondencias o a casos de suplantación.

[41] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

[42] Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.8.4

de la Ley Estatutaria 1581 de 2012 señala que "*quien acceda a los datos personales sin que medie autorización previa* ***deberá en todo caso cumplir con las disposiciones contenidas en la presente ley***". (Destacamos)

d) En caso que una obligación legal constituya la base jurídica para el Tratamiento de información personal, todos los demás principios rectores en materia de protección de datos seguirán siendo aplicables.

Los principios de necesidad y proporcionalidad son conceptos centrales en la protección de los datos, pues en ausencia del consentimiento, cualquier tratamiento basado en una excepción debe ser siempre necesario para el objetivo perseguido.

Así pues, a pesar de que la finalidad perseguida por el municipio **RECURRENTE** está plenamente soportada legalmente, pues la misma está basada en el cumplimiento de un decreto nacional, el ente territorial desconoció los principios rectores establecidos en la normatividad.

El cumplimiento del artículo 2.2.2.25.2.1 del Decreto 1074 de 2015 implica una evaluación estricta caso por caso de la necesidad y la proporcionalidad de la finalidad del Tratamiento y, en particular, si la misma podría alcanzarse con otros mecanismos menos lesivos para los derechos y libertades de los Titulares.

En el caso objeto de estudio, el Municipio **RECURRENTE** se abstuvo de evaluar de manera previa si existían otros medios menos lesivos e intrusivos para los empleados en relación con el suministró de un dato biométrico; pero al mismo tiempo, le permiten cumplir con el mandato legal a su cargo.

e) El municipio **RECURRENTE** omitió contar una Política de Tratamiento de Información personal, como lo establece la sección 3, del Capítulo 25, del Decreto 1074 de 2015.

Lo anterior, generó, desde el punto de vista de esta Delegatura, que se pusiera en riesgo los principios en materia de protección de datos, entre ellos, el de finalidad y el transparencia, que se refieren a que las personas conozcan antes de la recolección, y durante todo el ciclo de vida del dato, el uso que se le dará y se le está dando a sus información de carácter personal.

f) El municipio **RECURRENTE** incumplió su deber de contar con un Manual interno que incluyera las políticas, procesos y procedimientos necesarios para cumplir con las obligaciones establecidas en la Ley 1581 de 2012, de conformidad con el literal k) del artículo 17 de la misma norma, en concordancia con los artículos 2.2.2.25.2.1 y 2.2.2.25.6.1 del Decreto 1074 de 2015.

Esto, a su vez, se tradujo en que el sistema biométrico por ellos implementado carecía de las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

g) El Municipio **RECURRENTE** desconoce que la Política de Tratamiento de Información Personal y el Manual Interno de Políticas y Procedimientos son documentos establecidos en la normatividad que deben aplicar al Tratamiento de todos los datos personales en custodia o posesión del ente territorial.

Al respecto, es un hecho claro que el municipio **RECURRENTE** procesa datos de sus habitantes, proveedores, usuarios, etc., para diferentes tipos de finalidades o propósitos. De hecho, según el reporte del censo elaborado por el Departamento Administrativo Nacional de Estadística (DANE), el municipio de **CAJIBÍO** reporta un total de población de 32.237[43], tal y como lo muestra la siguiente imagen:

f) Las órdenes no son sanciones de carácter administrativo, por el contrario, son herramientas que buscan prevenir que se ponga en riesgo los derechos de los Titulares de la Información.

SÉPTIMO: Que analizada la cuestión planteada, se encuentra que no fueron desvirtuados los argumentos que fundamentaron la resolución impugnada y teniendo en cuenta lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirmará la Resolución No. 69434 del 4 de diciembre de 2019.

Para efectos de la notificación se procederá conforme lo ordena el artículo 4[44] del Decreto Legislativo 491 del 28 de marzo de 2020.

En mérito de lo expuesto, este Despacho

---

[43] Departamento Administrativo Nacional de Estadística (DANE), en: https://sitios.dane.gov.co/cnpv/#!/. Consultada el 26 de febrero de 2019.

[44] El artículo 4 del Decreto Legislativo 491 de 2020 ordena lo siguiente: "*Notificación o comunicación de actos administrativos. Hasta tanto permanezca vigente la Emergencia Sanitaria declarada por el Ministerio de Salud y Protección Social,* ***la notificación*** *o comunicación de los actos administrativos* ***se hará por medios electrónicos****. Para el efecto en todo trámite, proceso o procedimiento que se inicie será obligatorio indicar la dirección electrónica para recibir notificaciones, y con la sola radicación se entenderá que se ha dado la autorización.*
En relación con las actuaciones administrativas que se encuentren en curso a la expedición del presente Decreto, los administrados deberán indicar a la autoridad competente la dirección electrónica en la cual recibirán notificaciones o comunicaciones."

Por la cual se resuelve un recurso de apelación

VERSIÓN ÚNICA

RESUELVE

ARTÍCULO PRIMERO: MODIFICAR LOS ARTÍCULOS PRIMERO Y SEGUNDO de la Resolución 69434 del 4 de diciembre de 2019, de conformidad con lo expuesto en la parte motiva del presente acto administrativo, los cuales quedarán así:

> *"**ARTÍCULO PRIMERO: ORDENAR** al **MUNICIPIO DE CAJIBÍO, CAUCA**, identificado con el Nit. 891.500.864-5, en su condición de Responsable del Tratamiento, proceda a evaluar si el sistema biométrico de la huella dactilar es adecuado, pertinente y no excesivo en relación con la finalidad perseguida por el ente municipal. O, por el contrario, si existen otros mecanismos menos lesivos o invasivos para los Titulares, es decir, que no requiera el procesamiento de un dato biométrico, pero que al mismo tiempo, le permitan cumplir con las obligaciones legales a las que ese ente territorial está sujeto.*
>
> *En el evento que el sistema biométrico no sea estrictamente necesario para el fin perseguido, el **MUNICIPIO DE CAJIBÍO, CAUCA,** deberá implementar un sistema menos lesivo para los derechos y libertades de las personas.*
>
> ***ARTÍCULO SEGUNDO: ORDENAR** al **MUNICIPIO DE CAJIBÍO, CAUCA**, identificado con el Nit. 891.500.864-5, en su condición de Responsable del Tratamiento, contar con una alternativa, que no requiera el tratamiento de datos sensibles, en los casos en que los empleados se rehúsen a suministrar su huella en el sistema biométrico".*

ARTÍCULO SEGUNDO: CONFIRMAR en todos sus demás aspectos la Resolución No. 69434 del 4 de diciembre de 2019, de conformidad con lo expuesto en la parte motiva del presente acto administrativo.

ARTÍCULO TERCERO: EXHORTAR al Representante Legal de la **MUNICIPIO DE CAJIBÍO, CAUCA**, señor **YOHN WILMER CAMPO FLOR**, para que adopte las medidas pertinentes, útiles, efectivas y verificables con miras a:

a) Respetar los derechos de los Titulares al acceso, actualización, rectificación o supresión de los datos personales en custodia del ente territorial, así como la revocatoria de la autorización, si aplica.

b) Hacer efectivo el pleno respeto de los principios rectores en materia de protección de datos personales.

c) Garantizar que la protección de datos personales se convierta en una parte integral de la formulación de políticas públicas del municipio.

d) Asegurar que en cualquier proyecto, propuesta, iniciativa o actividad, que involucre datos personales, se realicen los tests de necesidad y proporcionalidad, a fin de que se logre el objetivo administrativo perseguido, pero al mismo tiempo proteja los derechos a la protección de datos personales y privacidad de los Titulares de la Información.

e) Realizar evaluaciones de impacto para identificar, evaluar y gestionar los riesgos asociados al Tratamiento de los datos personales bajo custodia o posesión del ente municipal. Dicha evaluación debe estar documentada y ser permanente, a fin de determinar su nivel de eficacia en cuanto al cumplimiento de la normatividad y evitar que se vulneren los derechos de los Titulares.

f) Determinar si el sistema biométrico adquirido por el ente municipal cumple con requisitos de calidad, exactitud, seguridad y confidencialidad para proteger los datos personales procesados por esta herramienta. Adicionalmente, implementar mecanismos de auditoría para garantizar el cumplimiento de los mismos.

g) Establecer cuál es el rol que está desempeñando la Secretaría de Gobierno y Tránsito y participación Comunitaria en el Tratamiento de los datos personales bajo custodia y posesión de la alcaldía municipal, de conformidad con los conceptos de Responsables y Encargados del Tratamiento que trae el artículo 3º de la Ley 1581 de 2012.

h) Cumplir las órdenes emitidas por la Dirección de Investigación de Protección de Datos Personales, confirmadas mediante la presente resolución.

ARTÍCULO CUARTO: NOTIFICAR personalmente el contenido de la presente resolución a la **MUNICIPIO DE CAJIBÍO, CAUCA**, identificada con el Nit. 891.500.864-5, a través de su representante legal o su apoderado o quien haga sus veces, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

ARTÍCULO QUINTO: INFORMAR el contenido de la presente resolución al Director de Investigación de Protección de Datos Personales y devolverle el expediente para su custodia final.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., 31 de Julio de 2020

El Superintendente Delegado para la Protección de Datos Personales

NELSON REMOLINA ANGARITA

LAM

VERSIÓN ÚNICA

Por la cual se resuelve un recurso de apelación

NOTIFICACIÓN:

Sociedad:	**MUNICIPIO DE CAJIBÍO - CAUCA**
Identificación:	891.500.864-5
Representante Legal:	**YOHN WILMER CAMPO FLOR**
Identificación:	76.325.726
Dirección:	CALLE 5 A NO. 1-34/38 CAM
Ciudad:	CAJIBÍO, CAUCA
Correo Electrónico:	alcaldia@cajubio-cauca.gov.co despachoalcalde@cajibio-cauca.gov.co