



# BIOMETRÍA

## en el Estado colombiano

*¿Cuándo y cómo se ha justificado su uso?*

Por:  
Fundación Karisma

Investigación:  
Juan Diego Castañeda  
Joan López  
Lucía Camacho



# Fundación Karisma

Bogotá, Colombia 2019

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantallas o pantalla braille. El propósito del diseño accesible es que todas las personas puedan leer, incluidas aquellas que tienen algún tipo de discapacidad visual o de dificultad para la lectura y comprensión.

Más información sobre documentos accesibles en:  
<http://www.documentoaccesible.com/#que-es>

## Biometría en el Estado colombiano ¿Cuándo y cómo se ha justificado su uso?

**Por:**  
Fundación Karisma

**Investigación:**  
Juan Diego Castañeda  
Joan López  
Lucía Camacho

**Diseño y diagramación:**  
Daniela Moreno

**Coordinación editorial:**  
Diego Mora Bello



*Este material circula bajo una licencia Creative Commons CC BY-SA 4.0. Usted puede remezclar, retocar y crear a partir de la obra, incluso con fines comerciales, siempre y cuando dé crédito al autor y licencie las nuevas creaciones bajo mismas condiciones.*

*Para ver una copia de esta licencia visite:*

<https://creativecommons.org/licenses/by-sa/4.0/deed.es>



# Contenido

<b>1 Introducción</b> .....	5
<b>2 Situación jurídica de los datos biométricos</b> .....	6
<b>3 Bases de datos biométricos en funcionamiento</b> .....	19
Base de datos biométricos de la Registraduría Nacional del Estado Civil (decadactilar y fotos biométricas) .....	19
Base de datos biométrica de Migración Colombia BIOMIG (iris) .....	23
<b>4 Usos de la base de datos de la RNEC</b> .....	25
Operadores biométricos .....	25
Sistema Appolo de la Policía Nacional .....	27
Asobancaria .....	28
Elecciones .....	28
<b>5 Proyectos</b> .....	29
Nuevas bases de datos biométricos .....	29
Sistema Multibiométrico ABIS (Automated Biometric Identification System) .....	29
Nuevos usos para las bases existentes .....	32
Autenticación biométrica en los Servicios Ciudadanos Digitales .....	32
<b>6 Conclusiones</b> .....	34
<b>7 Bibliografía</b> .....	38



# 1 Introducción

“La biometría” dice la Registraduría Nacional del Estado Civil (en adelante, RNEC) es el “método ideal de identificación humana”<sup>1</sup>. Esta afirmación de la certeza de métodos científicos y técnicos para configurar la identidad de una persona a partir de sus características físicas está atravesada por la forma en la que entendemos al Estado y en la que la ciudadanía puede acceder a servicios públicos. En este texto exploramos las razones por las cuales se han recolectado y usado datos biométricos en el Estado colombiano para contrastarlas con la protección legal y constitucional de los datos biométricos.

En primer lugar, revisamos la situación jurídica de los datos biométricos a través de las decisiones de la Corte Constitucional y la Delegatura para la Protección de Datos. En esta revisión buscamos entender cómo se define en estas decisiones un dato biométrico, cuáles son los requisitos para su tratamiento y las justificaciones que permiten recolectar y usar datos como la huella dactilar o las imágenes del rostro de una persona.

El dato por sí mismo, como una huella en una superficie o el registro de la voz de una persona, no tiene la capacidad de revelar directamente a la persona que la produjo. La identificación se configura una vez se confronta el dato y el registro que relaciona ese dato con un nombre o un número de identificación, por ejemplo. De ahí que la segunda parte de este texto haga un seguimiento de las bases de datos biométricas que operan la RNEC, la Policía Nacional y Migración Colombia, que son las que existen actualmente en el país.

En la tercera parte nos enfocamos en los usos de esas bases de datos. En otras palabras, nos preguntamos por quiénes y según qué razones se pueden consultar estas bases de datos. Parte del análisis de la segunda parte explica los usos originales de las bases de

---

1. Registraduría Nacional del Estado Civil, “La biometría: método ideal de identificación humana”. Disponible en: <https://www.registraduria.gov.co/La-biometria-metodo-ideal-de.html>

datos biométricas. Estas preguntas nos permiten pensar en las relaciones complejas que se forman alrededor de estas bases de datos entre ciudadanía, Estado y privados.

Finalmente, hacemos un recuento de las bases de datos o usos que están en diseño o que deben entrar a operar pronto. Este análisis complementa las justificaciones actuales para el uso de datos biométricos en el Estado con discursos sobre las expectativas de las autoridades respecto a la tecnología biométrica y al funcionamiento de un Estado moderno.

Para hacer el análisis se empleó información conseguida a través de derechos de petición, artículos académicos y otros documentos disponibles al público tales como comunicados de prensa, noticias publicadas en medios de comunicación, información contractual y documentos de contratistas involucrados con el despliegue de tecnologías biométricas. El análisis legal se centró en los textos de las leyes de protección de datos vigentes en Colombia, las sentencias de la Corte Constitucional y las decisiones de la Delegatura para la Protección de Datos.



# 2

## Situación jurídica de los datos biométricos

### Aplicación de la definición de datos biométricos

La clasificación de los datos y la información en Colombia es compleja debido a que existen al menos tres leyes que pueden determinar la situación jurídica del dato: la ley de habeas data para el sector financiero, la ley de protección de datos y, finalmente, la ley de transparencia y acceso a la información pública<sup>2</sup>. Estas leyes clasifican los datos por su naturaleza y por su circulación<sup>3</sup>.

Por su naturaleza, los datos son personales o no personales. Los primeros, que son objeto de la ley de protección de datos, pueden ser clasificados como sensibles si hay en ellos el potencial de afectar la intimidad de la persona o de generar discriminación<sup>4</sup>. Justamente en esta categoría están mencionados los “datos biométricos”. La Corte Constitucional y la Delegatura para la Protección de Datos han entendido que lo sensible del dato radica en que hace parte de la intimidad<sup>5</sup> de la persona.

La Delegatura para la Protección de Datos a través de varios procesos de sanción por el incumplimiento de la ley de protección de datos ha afirmado que los datos relativos a la salud son datos sensibles.

<sup>2</sup> Respectivamente, se trata de la Ley 1266 de 2008, Ley 1581 de 2012 y Ley 1704 de 2012.

<sup>3</sup> Sobre las entidades del sector público se encuentran facultadas para acceder a datos biométricos, puede verse la siguiente tabla <https://tinyurl.com/yy7qqk2v>

<sup>4</sup> Ley 1581 de 2012, “artículo 5. Datos Sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.”

<sup>5</sup> La Sentencia C-1011 de 2008 contiene un pasaje citado en varias ocasiones por la misma Corte Constitucional y la Delegatura para la Protección de Datos para definir el dato sensible: “la información sensible,[está] relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad” Cfr. Corte Constitucional, sentencia C-1011 del 16 de octubre de 2008, M.P. Jaime Córdoba Triviño.

En la Resolución 58969 del 2014<sup>6</sup>, la SIC abordó un caso sobre el tratamiento indebido de la información que revelaba el estado de gravidez de una mujer y que habría sido obtenida por una sociedad encargada de preservar células madre del cordón umbilical para ofrecerle a estas sus servicios comerciales<sup>7</sup>. La SIC determinó, entre otras cosas, que el dato de salud relativo al estado de embarazo de la mujer era, en efecto, un dato sensible cuyo tratamiento estaba expresamente prohibido por la legislación de habeas data y que su uso indebido podría dar lugar a eventos de discriminación o afectar el derecho a la intimidad de su titular.

Dos años después, tratándose nuevamente del tratamiento de datos sensibles, la Resolución 39298 de 2016<sup>8</sup> sancionó a una aseguradora en salud, por haber permitido en su portal web la visualización al público de los datos de las consultas médicas en los cuales hacían una expresa alusión a información sobre la salud sexual y reproductiva de una de sus afiliadas.

En cuanto a los datos biométricos, solo la Delegatura de Protección de Datos ha apuntado alguna definición general. Esencialmente, el dato biométrico sería aquel que parte del reconocimiento de una característica física de una persona que resulta única en cada individuo y que permite así distinguirlo de cualquier otro<sup>9</sup>. Aunque a partir de la definición se pueden pensar en muchas especies de datos biométricos, hasta donde se pudo averiguar, la Corte Constitucional y la Delegatura han decidido casos solamente relacionados con huellas digitales y fotografías o videos.

Respecto a la huella digital, la Delegatura investigó la captura de las huellas dactilares por una entidad privada para monitorear el ingreso y salida de sus empleados<sup>10</sup>; a las administraciones de edificios que recogían las huellas de las personas que ingresaban al lugar<sup>11</sup>; así como a un gimnasio en el que las personas afiliadas usaban su huella para

---

6 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 58969 de 2014, disponible en: [http://www.sic.gov.co/sites/default/files/files/Res%20No\\_%2058969%20de%202014%20-%20BANCO%20CELULAS%20MADRE.pdf](http://www.sic.gov.co/sites/default/files/files/Res%20No_%2058969%20de%202014%20-%20BANCO%20CELULAS%20MADRE.pdf)

7 El caso: La empresa que inicialmente le practicó el examen de embarazo no le advirtió a ésta del acceso que tendrían terceros a sus datos personales, por lo que la afectada decidió reclamar contra la sociedad comercial encargada de la preservación de células madre que la había contactado telefónicamente luego de conocer ella misma su estado de embarazo, alegando que ésta compañía no tenía una autorización que le permitiera llevar a cabo el tratamiento de su información.

8 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 39298 de 2016, disponible en: [http://www.sic.gov.co/sites/default/files/files/Res%20No\\_%2039298%20del%202016%20-%20COLMEDICA.pdf](http://www.sic.gov.co/sites/default/files/files/Res%20No_%2039298%20del%202016%20-%20COLMEDICA.pdf)

9 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, conceptos C-2014-273515 y C-2018-299565

10 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 12809 de 2018, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/RE12809-2018.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE12809-2018.pdf)

11 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 29407 de 2018, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/29407-16-234117.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/29407-16-234117.pdf) y Resolución N. 43530 de 2018 disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/RE43530-2018.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE43530-2018.pdf)

entrar a las instalaciones<sup>12</sup>. Cada investigación derivó en la respectiva sanción porque en cada caso, no se satisfizo el requisito de obtención del consentimiento informado del titular de aquel dato sensible para proceder a la captura de su información y posterior tratamiento.

La Corte Constitucional, por su parte, trató la huella digital de una forma muy diferente en un caso en el que una persona reclamaba la protección de su derecho a la vida, mínimo vital y seguridad social porque la Registraduría Nacional había cometido un error en su número de identificación y su banco se negaba al reconocimiento de su pensión. En este caso, la Corte retomó otros pronunciamientos sobre el uso de la biometría en el sistema electoral –que será tratado más adelante– y apuntó la posibilidad de usar la identificación biométrica como un sustituto del documento de identidad. Esto no significa que de facto la huella digital se pueda usar como se usa el documento de identidad, pero sí muestra cómo se ha abordado de formas diferentes este dato biométrico.

La Corte Constitucional, por su parte, trató la huella digital de una forma muy diferente en un caso en el que una persona reclamaba la protección de su derecho a la vida, mínimo vital y seguridad social porque la Registraduría Nacional había cometido un error en su número de identificación y su banco se negaba al reconocimiento de su pensión. En este caso, la Corte retomó otros pronunciamientos sobre el uso de la biometría en el sistema electoral –que será tratado más adelante– y apuntó la posibilidad de usar la identificación biométrica como un sustituto del documento de identidad<sup>13</sup>. Esto no significa que de facto la huella digital se pueda usar como se usa el documento de identidad, pero sí muestra cómo se ha abordado de formas diferentes este dato biométrico.

Sobre las fotografías del rostro, la Delegatura ha dicho que son datos personales, pero no necesariamente biométricos y, por tanto, sensibles. En casos en los que la administración de un edificio tomaba fotografías a las personas que ingresaban al sitio o se había implementado un sistema de videovigilancia<sup>14</sup>, se entendió que se trataba de un dato personal de tipo privado. Esta clasificación proviene de otra línea jurisprudencial de la Corte Constitucional en la que la información se clasifica de acuerdo con su

---

12 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 55405 de 2018, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/2018055405.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2018055405.pdf)

13 Corte Constitucional, sentencia T-1000 del 26 de noviembre de 2012, M.P. Jorge Iván Palacio Palacio

14 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 60460 de 2017, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/201706046resolucion.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/201706046resolucion.pdf); Resolución N. 43530 de 2018, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/RE43530-2018.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE43530-2018.pdf); y Resolución N. 55405 de 2018, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/2018055405.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2018055405.pdf)



divulgación<sup>15</sup>. La consecuencia de clasificar así a las fotografías o videos es que solo pueden ser conocidos por una autoridad judicial o por orden judicial. La Corte Constitucional usó la misma clasificación, sin hacer referencia a datos sensibles, en un caso en el que la administración de un balneario se negaba a entregar las grabaciones en las que se registró el momento de la muerte de una persona a sus familiares porque contenían imágenes de menores de edad en vestido de baño. La Corte Constitucional sostuvo en esa ocasión que por tratarse de un lugar privado y porque aparecen menores, la información era privada y solo podía divulgarse por orden judicial<sup>16</sup>.

Sin embargo, de acuerdo con la Delegatura para la Protección de Datos, una fotografía o video se clasifica como biométrico y, por tanto, sensible solo cuando se implementen alguna técnica para “la extracción de elementos particulares del rostro”<sup>17</sup>. Esta interpretación, que se apoya en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo<sup>18</sup>, deja dudas sobre qué tipo de técnica y conexión con otras bases de datos se requeriría para determinar el cambio de clasificación del dato para ser biométrico ya que sería necesario un repositorio con el cual contrastar el resultado de la medición de las características del rostro. En ninguno de los casos, la investigación de la Delegatura encontró que hubiera una extracción de datos o comparación con bases de datos, por lo cual no entendió que hubiera un tratamiento de datos sensibles.

---

15 Cfr. Corte Constitucional, sentencia C-1011 del 16 de octubre de 2008, M.P. Jaime Córdoba Triviño, “Respecto a estos datos personales, la jurisprudencia propone dos modos de clasificación. La primera, relacionada con el nivel de protección del derecho a la intimidad, divide los datos entre información personal e impersonal, definiéndose la segunda como aquella que no reúne los requisitos mencionados anteriormente. (...) La siguiente gran tipología divide los datos personales con base en un carácter cualitativo y según el mayor o menor grado en que pueden ser divulgados. Así, se establece la existencia de información pública, semiprivada, privada y reservada.” Estas dos clasificaciones paralelas fueron sostenidas también en la sentencia C-748 de 2011.

16 Corte Constitucional, sentencia T-114 del 3 de abril de 2018, M.P. Carlos Bernal Pulido

17 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 60460 de 2017, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/201706046resolucion.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/201706046resolucion.pdf)

18 La Delegatura cita el siguiente aparte del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo: “El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física” Cfr. Superintendencia de Industria y Comercio, Oficina Jurídica, consulta N. 297406 de 2018

## Protección de los datos biométricos

En los procesos que ha decidido la Delegatura para la Protección de Datos, en efecto, se ha sancionado a quienes realizan el tratamiento de datos sensibles y biométricos sin los requisitos legales. En esta sección revisamos las relaciones entre requisitos y límites del tratamiento y la aplicación de los principios de la ley de protección de datos como aparecen en estas sanciones. Para consultar las resoluciones proferidas por la Delegatura sobre datos biométricos y que fueron revisadas en la redacción de la sección siguiente.

### Resoluciones de la Superintendencia de Industria y Comercio SIC - Delegatura para la Protección de Datos

Año	Resolución	Datos	Decisión
2014	58969	Datos sensibles: revelaban el estado de gravidez de una mujer y que habrían sido obtenidos por terceros para ofrecer servicios de preservación de células madre	Se sanciona a la empresa que accede a la información de la mujer en tanto que no cumplió con el requisito de obtención del consentimiento informado para el tratamiento de datos sensibles
2016	39298	Datos sensibles: revelaban información sobre la salud sexual y reproductiva de la afiliada a una aseguradora en salud, cuya visualización estaba dispuesta sin restricciones en la página web de la aseguradora.	Se sanciona a la aseguradora prepagada de salud, no sólo porque la autorización de tratamiento de datos no incluyó ninguna advertencia sobre la circulación en la internet de la información sensible de los asegurados, sino porque la información podía visualizarse libremente en internet por falta de mecanismos de seguridad de la entidad.
2017	60640	Dato privado: las fotografías que se tomen sin el uso de sistemas biométricos que permitan extraer de ellas rasgos particulares de la persona, siguen siendo datos privados, no biométricos.	Se sanciona a una empresa de vigilancia privada que para identificar a visitantes, tomaba una foto de su rostro sin su consentimiento y sin prever para ello una clara política de tratamiento de datos personales.
2018	12809	Datos sensibles: captura mediante escáner de las huellas digitales de los empleados de una entidad privada para registrar ingreso y salida del turno laboral	Se sanciona a la empresa por no haber contado con el consentimiento informado para el tratamiento de información sensible de sus empleados.

Año	Resolución	Datos	Decisión
2018	29407	Datos sensibles: captura mediante escáner de las huellas digitales de visitantes de una propiedad horizontal y los empleados de la empresa encargada de validar el ingreso y salida del edificio.	Se sanciona a la empresa de vigilancia por no haber contado con un procedimiento para la obtención del consentimiento informado en la toma de datos sensibles. Afirma la SIC que los avisos de advertencia no constituyen una forma para obtener vía asentimiento la autorización en el tratamiento de esa información por parte del titular de la huella.
2018	55405	Datos sensibles: captura mediante escáner de las huellas digitales de usuarios de un gimnasio.	Se sanciona al gimnasio por no haber retirado de su base de datos, la huella digital de usuarios que estaban inactivos del servicio.
2018	11395	Datos biométricos obtenidos por la Unión del Colegiado Notariado de Colombia	En una investigación preventiva, la SIC advierte sobre la necesidad de que en la autenticación biométrica de quienes realizan trámites notariales, se efectúe la obtención del consentimiento informado, y se restrinja el acceso y administración de las bases de datos con información personal.
2018	43530	Datos sensibles: una administradora de propiedad horizontal, capturaba y almacenaba la huella digital de visitantes al edificio	Se sanciona a la administradora de la propiedad horizontal por no contar con el consentimiento informado del titular del dato, y por no contar además, con una política de tratamiento de datos sensibles.

## Requisitos del tratamiento de datos biométricos

La importancia de clasificar un dato como biométrico es que es un dato sensible y, de acuerdo con la ley de protección de datos, para su tratamiento se deben cumplir ciertos requisitos.

El primer requisito para el tratamiento de datos sensibles es el consentimiento o autorización por parte del titular. La autorización debe ser expresa y debe dejar claro cuáles son los datos sensibles que se recogen, debe informarse la finalidad para la cual se reco

gen los datos y advertirse que la persona no está obligada a entregar este tipo de datos<sup>19</sup>. Adicionalmente, se debe conservar una copia de la autorización<sup>20</sup> y desplegar un aviso de privacidad visible<sup>21</sup>, así como establecer y aprobar una política de privacidad<sup>22</sup> y un manual interno para el tratamiento de datos<sup>23</sup>.

Según las decisiones de la Delegatura, el tratamiento de datos sensibles parece tener como único límite el cumplimiento de estos requisitos. Por eso es necesario analizar si se han configurado límites al tratamiento de datos biométricos, es decir, razones por las cuales no sería legal hacer este tratamiento aun cuando se cumplan los requisitos. Dentro de estos límites debe considerarse cómo podrían aplicar los principios de la ley de protección de datos para dibujar con más precisión hasta dónde se puede pedir y usar la biometría.

## Límites y principios de la protección de datos biométricos

Aunque el tratamiento de datos sensibles está prohibido, existen unas excepciones que posibilitan el tratamiento de este tipo de datos<sup>24</sup>. Las decisiones de la Delegatura han considerado solamente la autorización del titular de los datos sensibles y se ha enfocado en verificar que efectivamente exista esa autorización en las condiciones que mencionamos anteriormente, así como el cumplimiento de los requisitos especiales de información. Sin embargo, en ninguna de las decisiones se evalúa la necesidad y la finalidad de la recolección de los datos biométricos tales como huellas y fotografías.

La Corte Constitucional interpretó el artículo sobre las excepciones a la prohibición del tratamiento de datos sensibles y estableció lo que parece ser una regla que delimita los casos en los que es posible hacer ese tratamiento, excluyendo cualquier otra finalidad:

La prohibición de tratamiento de datos sensibles es una garantía del habeas data y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana. Sin embargo, en ciertas ocasiones el tratamiento de tales datos es indispensable para la adecuada prestación de servicios –como la atención médica y la educación– o para la realización de derechos ligados precisamente a la esfera íntima de las per-

---

19 Ley 1581 de 2012, artículo 6, literal A; artículo 9; artículo 12

20 Ley 1581 de 2012, artículo 17, literal B

21 reto 1377 de 2013, artículo 14 y 15. El Decreto 1377 de 2013 está recogido en el artículo 2.2.2.25 del Decreto Único Reglamentario 1704 de 2015 pero haremos referencia en este documento a la nomenclatura del Decreto original para facilitar la lectura.

22 Decreto 1377 de 2013, artículo 13

23 Ley 1581 de 2012, artículo 17, literal K; Decreto 1377 de 2013, artículo 27

24 Ley 1581 de 2012, artículo 6

sonas –como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión. Las excepciones del artículo 6 responden precisamente a la necesidad del tratamiento de datos sensible en dichos escenarios<sup>25</sup>.

La Delegatura recoge esta posición de la Corte y afirma que solo puede hacerse el tratamiento de datos personales “cuando sea indispensable para la adecuada prestación de servicios como la atención médica, educación, o la realización de derechos ligados a la esfera íntima de las personas”<sup>26</sup>.

Esta regla, que limitaría el tratamiento de datos biométricos en la teoría, no parece ser aplicada en la práctica. En los casos donde se comprobó que la administración de un edificio o un gimnasio obligan a empleados y visitantes a dejar su huella digital o a tomarse una fotografía, la Delegatura no analizó si era necesario recoger este tipo de datos y se limitó a comprobar la existencia de una autorización en las condiciones que ya especificamos.

Esto podría indicar, por contraste, que se puede recolectar un dato biométrico siempre que una persona acepte que se tome la fotografía, el escaneo del iris o la impresión de las huellas digitales. Una interpretación así se dirige a poner el principio de libertad por encima de los demás, pues, sin importar para qué se usa el dato biométrico, lo importante sería que la persona haya consentido a su tratamiento a partir de una autorización en la que tenía claro el objetivo y el hecho de que no estaba obligada a entregar ese dato. Es necesario anotar que las decisiones de la Delegatura respecto a los datos biométricos están atadas a su competencia. De acuerdo con la ley de protección de datos, esta dependencia de la Superintendencia de Industria y Comercio –SIC– tiene competencia para investigar y sancionar “entidades de naturaleza privada”.

Es necesario anotar que las decisiones de la Delegatura respecto a los datos biométricos están atadas a su competencia. De acuerdo con la ley de protección de datos<sup>27</sup>, esta dependencia de la Superintendencia de Industria y Comercio –SIC– tiene competencia para investigar y sancionar “entidades de naturaleza privada”. En el sector público, la Procuraduría General de la Nación es la encargada de investigar a sancionar a los servidores públicos por presuntas violaciones a la ley de protección de datos, pero hasta el momento no se conocen

---

25 Corte Constitucional, sentencia C-748 del 6 de octubre de 2011, M.P. Jorge Ignacio Pretelt Chaljub

26 Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos, Resolución N. 58969 de 2014, disponible en: [http://www.sic.gov.co/sites/default/files/files/Res%20No\\_%2058969%20de%202014%20-%20BANCO%20CELULAS%20MADRE.pdf](http://www.sic.gov.co/sites/default/files/files/Res%20No_%2058969%20de%202014%20-%20BANCO%20CELULAS%20MADRE.pdf); consulta N. 13-2733515 de 2014; y Resolución N. 60460, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/201706046resolucion.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/201706046resolucion.pdf)

27 Ley 1581 de 2012, artículo 23, parágrafo: “Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva”.

procesos de este tipo. Al revisar la constitucionalidad del artículo que asigna estas competencias, ni la Corte Constitucional ni la misma Procuraduría hicieron algún comentario.

En opinión de tres magistrados de la Corte Constitucional<sup>28</sup>, este arreglo institucional tiene varios problemas pues no considera que el derecho a la protección de datos no sólo afecta relaciones económicas y comerciales sino también las “relaciones entre el individuo y el Estado” que aparecen, por ejemplo, en las bases de datos del Sistema de Selección de Beneficiarios de Programas Sociales –SISBEN– y otras similares.

Por un lado, hay muchas bases de datos que administran organismos en la rama judicial, en la rama legislativa y los organismos de control establecidos en la Constitución. La potencial competencia de la SIC entraría en tensión con la independencia de estos poderes y deja sin aplicación efectiva el derecho de protección de datos en las bases de datos que allí se creen o usen. Además, habría un problema en la rama ejecutiva pues la SIC, que es parte de esta rama, sería “juez y parte” en posibles casos de violación de la ley de protección de datos.

Finalmente, la SIC es una entidad dedicada a la protección del consumidor y la vigilancia de la competencia<sup>29</sup>, por lo cual podría haber una tensión entre su naturaleza y el control de la aplicación de la ley de protección de datos en casos que no tienen que ver con este tipo de temas. En el país aún no ha surgido un debate en el que se haya tenido en cuenta estos argumentos, por lo que los problemas de la protección de datos dentro de la actividad estatal siguen sin respuesta.

## Implicaciones para bases de datos del Estado

El análisis sobre los requisitos, límites y principios de la protección de datos ha partido de las decisiones de la Delegatura en casos donde un particular es el responsable del tratamiento de los datos, pues esta autoridad no tiene competencia para investigar y sancionar los casos en los que pueda estar involucrada una autoridad pública. Los problemas para entender cómo opera la protección de datos en el sector público pueden verse en el análisis de las excepciones a la autorización para el tratamiento de datos, y en los casos donde se crean bases de datos y registros por orden legal.

---

*28 Salvamento de voto de los magistrados María Victoria Calle Correa, Jorge Iván Palacio Palacio y Luis Ernesto Vargas Silva en la sentencia C-748 del 6 de octubre de 2011, M.P. Jorge Ignacio Pretelt Chaljub.*

*29 Decreto 2153 de 1990.*

Los principios de la ley de protección de datos aplican para todos los casos de tratamiento de datos personales, de acuerdo con la Corte Constitucional<sup>30</sup>. Sin embargo, hay una lista de actividades en las cuales las reglas específicas de la protección de datos no aplican. Estas actividades, para el argumento que nos interesa presentar acá, son las bases de datos de inteligencia, control de lavado de activos, financiación del terrorismo y las relacionadas con la información estadística oficial. La interpretación de la Corte Constitucional en cada caso ha defendido que existe un objetivo legítimo protegido por la Constitución para el levantamiento y uso de ese tipo de información que, en todo caso, debe respetar el principio de proporcionalidad.

Para el caso de información estadística oficial, la Corte Constitucional entiende que es necesario mantener un nivel de reserva sobre datos con los cuales se toman decisiones para políticas públicas y programas sociales. Otras bases de datos o registros en los que se ha entendido que existe un fin constitucional legítimo son, por ejemplo, las listas de personas que no pueden contratar con el Estado<sup>31</sup>, los registros de antecedentes penales<sup>32</sup>, órdenes de captura<sup>33</sup>, y las bases de datos de afiliados al sistema de salud<sup>34</sup>. Si bien en estos casos no necesariamente están involucrados datos biométricos, se ha admitido que la creación de bases de datos o registros por sí misma no es una actividad desprotegida por la Constitución. Estas bases pueden incluir datos biométricos, especialmente en los casos en que se usa la biometría para verificar la identidad de las personas, pero no necesariamente se ha aplicado la ley de protección de datos.

En otras palabras, verificar la identidad de una persona en las bases de datos de la RNEC a través de la biometría es una forma de tratamiento de datos biométricos. Sin embargo, en casos donde por mandato legal la biometría sirve para establecer la identidad, se puede producir una situación en la que solo pueden negarse a entregar estos datos bajo la condición de renunciar al servicio o beneficio, haciéndose inaplicable lo establecido en el Decreto 1377 de 2013, en el sentido de que ninguna actividad estará condicionada a la entrega de datos sensibles.

Los casos de uso de biometría para verificar la identidad de una persona entonces muestran un contraste entre el régimen de protección de datos y la creación y uso de bases de datos biométricas estatales. Por tanto, es necesario investigar cómo y por qué se hacen estas bases de datos y de acuerdo a qué justificaciones. El marco de la protección de da-

---

*30 Ley 1581 de 2012, artículo 2, parágrafo. Adicionalmente, la Corte Constitucional en la Sentencia C-748 de 2011 dijo "(...) tal como se hizo en la sentencia C-1011 de 2008, la Sala se permite recordar que aunque en principio es constitucional la consagración de algunas excepciones a la aplicación de algunas disposiciones de la ley, ello no significa que aquellos ámbitos, así como todos los demás en los que se lleva a cabo tratamiento de datos personales, estén excluidos de las garantías básicas del derecho al habeas data, así como de las garantías de otros derechos fundamentales que en cada caso puedan resultar lesionados con el tratamiento de datos personales".*

*31 Corte Constitucional, sentencia T-1031 del 30 de octubre de 2003, M.P. Eduardo Montealegre Lynett*

*32 Corte Constitucional, sentencia T-020 del 27 de enero de 2014, M.P. Luis Guillermo Guerrero*

*33 Corte Constitucional, sentencia T-531 del 267 de septiembre de 2016, M.P. Gabriel Eduardo Martelo*

*34 Corte Constitucional, sentencia T-1038 del 14 de diciembre de 2010, M.P. Jorge Iván Palacio Palacio*

tos en estos casos es sólo una parte de los elementos que hay que considerar, mientras que los fines del Estado, la razón de ser y la configuración de programas de salud o subsidios se hacen más relevantes.

## La huella digital como sinónimo de identidad

En otras ocasiones, la huella digital ha sido considerada por las Cortes no como un dato biométrico sensible, sino como una forma alternativa de probar la identidad para el acceso a servicios de salud o beneficios de programas sociales.

La Corte Suprema de Justicia, en un caso de falso rechazo en la autenticación biométrica de la huella digital de un ciudadano al momento de efectuar un trámite de tipo notarial, decide tutelar los derechos del accionante, poniendo de presente que el error de autenticación con la huella se presentó en varias notarías a la que este recurrió. Deduce que no se trató de una falla en el sistema de biometría de dichas entidades, sino en una inconsistencia en los datos o en la transmisión de estos de la RNEC hacia las notarías.

El juez del caso terminó ordenando a la Registraduría, como entidad encargada de realizar la caracterización e individualización de la ciudadanía, a hacer lo necesario para corregir la autenticación biométrica del tutelante. Para esto, la tarea debía hacerse con la Unión Colegiada del Notariado para permitirle al ciudadano el ejercicio de su derecho a la identificación que “reconoce al ciudadano su individualidad, su condición de ser humano único y diferente a todos sus pares”<sup>35</sup>.

Por su parte, la Corte Constitucional se ha pronunciado en varios casos en donde la huella digital se usa para suplir la falta del documento de identidad. En un caso, una persona pide la protección del derecho a la vida y la salud frente a la decisión de su empresa prestadora de salud de negarse a entregar los medicamentos que necesita para la enfermedad de Parkinson. Para reclamar el medicamento, la empresa de salud exige que se verifique la identidad del beneficiario con su huella digital. En la práctica, esto resulta en la negación del acceso al servicio de salud porque la persona no podía desplazarse hasta el lugar donde entregaban el medicamento por el estado avanzado de la enfermedad y, en su lugar, enviaba a una persona de confianza para reclamarlo. En esa ocasión, dijo la Corte:

Para la Sala es factible que SaludCoop E.P.S. exija que fármacos como los relacionados en el presente caso, sean reclamados por la persona directamente afectada, pues así se evitan fraudes, malos usos o destinación indebida. Sin embargo, dichas reglas de cuidado no pueden aplicarse desconociendo las circunstancias del caso concreto, como quiera que en ocasiones como la

---

<sup>35</sup> Corte Suprema de Justicia de Colombia, Sala de Casación Laboral, rad. 69577, sentencia del 9 de noviembre de 2016, M.P. Jorge Luis Quiroz Alemán



actual, la persona aún necesitando los medicamentos no puede reclamarlos personalmente viéndose impelida a autorizar a un tercero para que, en su representación, exija su entrega a la E.P.S. respectiva<sup>36</sup>.

En otro caso, una persona pidió protección a sus derechos a la igualdad, al mínimo vital y a la vida digna pues no cuenta con el documento nacional de identificación y la entidad financiera se niega a desembolsar el auxilio que le reconoce el Departamento para la Prosperidad Social por ser reconocida como víctima de desplazamiento forzado. La Corte Constitucional le dio la razón a la reclamante, mencionando el uso de la biometría una de las alternativas para verificar la identidad de la beneficiaria:

A manera de ejemplo, la pluralidad de certificaciones aportadas en el asunto que se revisa; la presentación de documentos que presenten características de seguridad similares a las de la cédula de ciudadanía junto con aquellos que acreditan que la cédula se encuentra en trámite; el establecimiento de comunicación directa entre el Banco y la Registraduría Nacional del Estado Civil; o sistemas de identificación por biometría, deberían ser considerados como medidas para que las personas víctimas de desplazamiento accedan a sus recursos. No corresponde a la Sala indicar cuál de esos medios es el adecuado, pero las órdenes de prevención a adoptar se encaminarán a contribuir en la creación de tales mecanismos<sup>37</sup>.

La Corte reconoció que es legítimo y necesario exigir una prueba de la identidad para evitar comprometer “la seguridad del sistema financiero, (...) la confianza de los usuarios en el mismo y, muy especialmente, la protección de los recursos de la población desplazada”<sup>38</sup>.

Finalmente, en una decisión que sintetiza las relaciones entre identidad y biometría frente a distintos registros estatales, la Corte Constitucional consideró que ser titular de un derecho es distinto a la forma de acreditar la identidad. Por esto, se deben flexibilizar las formas para realizar esa acreditación en el marco de la modernización, simplificación y eliminación de trámites y también teniendo en cuenta los “avances científicos y tecnológicos” en relación con la identidad. Concretamente, dice la Corte:

Los medios de identificación personal no son sistemas estáticos. Por el contrario, estos deben actualizarse en consonancia con los avances científicos y tecnológicos sobre la materia para lograr mayor seguridad, fiabilidad y eficacia en los procesos de individualización, guardando siempre respeto por la dignidad humana y demás garantías constitucionales<sup>39</sup>.

---

36 Corte Constitucional, sentencia T-312 del 4 de abril de 2008, M.P. Rodrigo Escobar Gil

37 Corte Constitucional, sentencia T-561 del 17 de julio de 2012, M.P. María Victoria Calle

38 *Ibidem*.

39 Corte Constitucional, sentencia T-1000 del 26 de noviembre de 2012, M.P. Jorge Iván Palacio Palacio

En estas decisiones se reflejan dos justificaciones para el uso de la biometría que están conectadas. La primera es que la biometría funciona para identificar a una persona para permitirle, en consecuencia, el reconocimiento de sus derechos por terceros. Este reconocimiento se concreta en un subsidio o ayuda económica. Segundo, la identificación y autenticación de la identidad de una persona es necesaria para evitar fraudes y evitar el desperdicio de recursos públicos. Las decisiones de las Cortes en estos casos provienen de una visión garantista de los registros estatales, pues le restan importancia a los documentos de identidad cuando ellos son un obstáculo para el reconocimiento de derechos y beneficios en programas sociales. En su lugar, advierten que se deben usar formas alternativas de verificación de la identidad, dentro de las que se cuenta la biometría, cuando no se puede acceder al documento de identidad.

Como se verá en los capítulos siguientes, la biometría ha sido incorporada en algunas bases de datos estatales bajo la idea de que es una forma más segura de verificar la identidad de las personas. Un Registrador Nacional, citado por la Corte Constitucional, imagina muchos usos distintos para la biometría:

La identificación por medio de huellas digitales es hoy en día la forma más representativa de utilización de la biometría: Tiene usos tan variados como permitir el acceso a computadoras y redes, controlar horarios de ingreso, restringir el acceso físico a un área restringida, hacer seguimiento a migrantes en puntos fronterizos y para mejorar la seguridad en los cajeros automáticos, entre otros<sup>40</sup>.

### Qué entidades están facultadas legalmente para acceder a datos biométricos en Colombia

Año	Norma	Art	Entidad facultada	Tipo de dato al que accede
2011	Ley 1450	227	<p>Las entidades que desarrollen actividades financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos de captación del público.</p> <p>Las administradoras del sistema de seguridad social integral en pensiones, salud y riesgos laborales</p> <p>Las entidades públicas o particulares con funciones públicas que quieran verificar la plena identidad de los ciudadanos</p>	Datos biométricos de los afiliados al sistema general de seguridad social, salud y pensiones y en general, los que administra la RNEC

<sup>40</sup> *Ibidem*.

Año	Norma	Art	Entidad facultada	Tipo de dato al que accede
2012	Ley 1581	10 (a)	Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial sin necesidad de requerir autorización del titular del dato	No se restringe el tipo de dato al que pueden acceder
2012	Decreto 019	18	En los trámites y actuaciones que se cumplan ante las entidades públicas y los particulares que ejerzan funciones administrativas; el Instituto Nacional Penitenciario y Carcelario INPEC;	Datos biométricos
2015	Ley 1753	159	Las entidades que desarrollen actividades financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos de captación del público.  Las administradoras del sistema de seguridad social integral en pensiones, salud y riesgos laborales  Las entidades públicas o particulares con funciones públicas que quieran verificar la plena identidad de los ciudadanos	Datos biométricos de los afiliados al sistema general de seguridad social, salud y pensiones y en general, los que administra la RNEC
2016	Res. 5633	14	Las entidades interesadas en acceder y consultar los datos y la base de datos con la información biográfica y biométrica que produce y administra la Registraduría Nacional del Estado Civil	Datos biométricos
2017	Decreto 1413	2.2.1 7.2.2.4 // 2.2.1 7.3.1	Entidades públicas y particulares que ejercen función pública	Datos biométricos



# 3

## Bases de datos biométricos en funcionamiento

### Base de datos biométricos de la Registraduría Nacional del Estado Civil (decadactilar y fotos biométricas)

Colombia inició el proceso de recolección de datos biométricos de la ciudadanía en dos esfuerzos diferenciados que terminaron confluyendo en el siglo XXI. Por un lado, tenemos la base de datos criminal que, al igual que otros países del mundo, inició a principios del siglo XX tomando huellas dactilares, medidas antropométricas y fotografías de los criminales<sup>41</sup>. Por otro lado, el Departamento Nacional de Identificación, en un intento por luchar contra los fraudes electorales, empezó a proveer Cédulas de Ciudadanía que incluían datos antropométricos, una fotografía y la huella del índice derecho en 1934<sup>42</sup>.

En 1948, en medio de una crisis de institucionalidad y violencia partidista, se expidió la Ley 89 de 1948 para reformar el sistema electoral, creando un organismo independiente de los partidos para administrar las elecciones. En esta Ley se incluyó el requerimiento de contratar una misión extranjera de países del Norte global para que ayudara en “dictaminar acerca de los sistemas que deban emplearse en la identificación y cedulación”<sup>43</sup>.

Así, en 1950 llegó una misión canadiense que hizo una serie de recomendaciones que incluían la adopción del sistema dactiloscópico Henry e iniciar un archivo centralizado microfilmado de las huellas dactilares. Curiosamente, Canadá no contaba con un sistema de identificación nacional. A partir del informe de la misión canadiense, en 1951 se adoptó el Decreto 2628 para iniciar la impresión de las nuevas cédulas<sup>44</sup>. El proceso de

---

41 Alzate, Juan David, *Entre rostros y huellas. Una aproximación a los procedimientos aplicados a la investigación judicial por homicidio en Medellín-Colombia (1900-1930)*. TRASHUMANTE | Revista Americana de Historial Social, (2013): 32-55.

42 Decreto 944 de 1934

43 Ley 89 de 1948

44 Decreto 2628 de 1951

consolidación de la base de datos de identidad nacional se daría con la Ley 39 de 1961, que convirtió a la Cédula en un requerimiento para “todos los actos civiles, políticos, administrativos y judiciales”<sup>45</sup>. Con esta Ley inició un proceso que mezcló el registro de la ciudadanía para reclamar sus derechos con la recolección y clasificación de sus datos biométricos.

En 1970, con el Decreto 1260, la RNEC quedó a cargo de la producción de las cédulas y la recolección de datos. El cambio del archivo a formato digital iniciaría en 1997 con el Proyecto de Modernización Tecnológica que trató de aumentar los estándares de seguridad de las cédulas anteriores y buscó digitalizar los datos de la Registraduría y las bases de datos<sup>46</sup> biométricas. El procedimiento se realizó en dos fases y la RNEC lo hizo con apoyo de la multinacional francesa Morpho SAFRAN (actualmente, IDEMIA)<sup>47</sup>.

La primera fase, entre 1997 y 2005, implicó la preparación de los datos de la Registraduría para instalar un Sistema Automatizado de Identificación Dactilar (AFIS, por sus siglas en inglés). En ese sentido, en 1999, se adquirió software y hardware necesario para iniciar el proceso de digitalización de los registros y la consolidación de un sistema AFIS. En 2000, se arrancó la producción de la nueva cédula con hologramas que requería la recolección de los datos antropométricos, las huellas dactilares, la fotografía y el grupo sanguíneo. Este documento incluyó un código de barras que tiene datos alfanuméricos con los patrones que permiten determinar la unicidad de la huella en la cédula<sup>48</sup>.

En la segunda fase, entre 2005 y 2010, se extendió la base de datos a las personas que tenían los anteriores modelos de la cédula y se terminó el sistema AFIS con un servicio web que permitía su implementación en los sectores público y privado<sup>49</sup>. Igualmente, en 2008 se inició la producción de la tarjeta de identidad biométrica a menores de edad para incluirlos en las bases de datos de la Registraduría<sup>50</sup>. A partir de 2008, la empresa francesa arrancó la transferencia del sistema a la Registraduría. En 2010, los antiguos formatos perdieron validez y se completó la transferencia del sistema, consolidando la base de datos biométricos más grande del país con un índice de indocumentación de 10%<sup>51</sup>.

---

45 Ley 39 de 1961

46 Decreto 1260 de 1970

47 Martins, Alexandre, *The Colombian Identification System Implementation and technological advancement of the civil identification and registration systems*. *Keesing Journal of Documents & Identity*, (2013): 25-28.

48 Martins, “*The Colombian Identification System*”

49 *Ibidem*.

50 Registraduría Nacional del Estado Civil. «Historia de nuestra cédula de ciudadanía.» *Nuestra huella - Revista Electrónica Mensual*, (2012)

51 Banco Interamericano de Desarrollo, *Inventario de los registros civiles e identificación de América Latina y el Caribe*. (Washington: BID, 2010), 14

Como se mencionó, la historia de la base biométrica de registro civil estaba apartada de la base de datos de registro criminal. En 1998, como una donación de los Estados Unidos mediante el Plan Colombia<sup>52</sup>, la Policía Nacional implementó el sistema AFIS Printrak de la firma Motorola. En 2009, la Policía Nacional buscó construir una base de datos interoperable con los registros civiles de la base de datos de la Registraduría. Para esto, se contrató a la multinacional francesa que se había encargado de la base de datos de la Registraduría<sup>53</sup>.

Para este momento, existían otras bases de datos biométricas de personas con algún tipo de investigación judicial como la del Departamento Administrativo de Seguridad (DAS)<sup>54</sup> y la de la Dirección de Investigación Criminal e INTERPOL (DIJIN)<sup>55</sup> también implementadas por Morpho. En 2010, cuando Morpho completó el traslado del sistema a la Registraduría, también se generaron interconexiones entre estas bases de datos de registro biométrico de criminales<sup>56</sup>.

En 2011, con el Decreto 4057 de 2011, se suprimió el DAS y se le entregaron las funciones de registro a la Policía<sup>57</sup>. Finalmente, ese mismo año, por medio del convenio interadministrativo No. 3, se suscribió un acuerdo de cooperación entre la RNEC y la Policía que permitiría el uso del servicio web para reducir el tiempo de consulta. De esta forma, los registros criminales terminaron confluyendo con los registros civiles en la base de datos biométrica de la Registraduría.

Después de la consolidación de la base de datos biométricos de la Registraduría, inició un proceso de automatización e interoperabilidad de la identidad digital en el Estado. Así, con el Decreto 019 de 2012, con el propósito de hacer más eficiente al Estado, se permitió el uso de la verificación electrónica de la huella dactilar para los trámites y actuaciones frente a entidades y particulares en actividades administrativas<sup>58</sup>. Este decreto abrió la posibilidad de utilizar la base de datos biométrica de la Registraduría para identificar a una persona en cualquier relación con el Estado.

---

52 El Plan Colombia es un acuerdo bilateral firmado en 1999 entre los gobiernos de Estados Unidos y Colombia para apoyar económicamente la lucha contra el narcotráfico.

46 Decreto 1260 de 1970

53 Fondo Rotatorio de la Policía Nacional de Colombia, Estudio y documentos previos con objeto “adquisición, instalación, implementación, licenciamiento, prueba, puesta en servicio, garantía, soporte y mantenimiento de un sistema biométrico facial, palmar y dactilar para la Policía Nacional”. (Ministerio de Defensa Nacional, 2017)

54 El DAS fue el organismo estatal de inteligencia y contrainteligencia en Colombia que fue suprimido después de una serie de escándalos de interceptaciones ilegales.

55 La DIJIN es una dirección de la Policía Nacional encargada de la investigación penal y que, a partir de la eliminación del DAS, comenzó a encargarse de los convenios con la INTERPOL

56 Martins, “The Colombian Identification System”

57 Decreto 4057 de 2011

58 Decreto 019 de 2012, artículo 18

Posteriormente, con la Ley 1753 de 2015, se ampliaron los espacios en que se requeriría la verificación biométrica y se consolidó el camino para interoperar la base de datos biométrica de la RNEC y convertirla en un requisito básico de la vida ciudadana. Por un lado, convirtió en obligatoria la verificación biométrica de las personas dentro del sistema de seguridad social (salud, pensión y riesgos laborales). Además, la Ley instó a cualquier entidad pública y a privados con funciones públicas a verificar la identidad ya fuese por medio de su propia infraestructura o utilizando uno de los operadores seleccionados por la Registraduría para este fin<sup>59</sup>. Por otro lado, la Ley abrió la posibilidad de que las instituciones financieras y aseguradoras utilizaran la base de datos para identificar a personas, pagando un monto determinado por la Registraduría<sup>60</sup>.

Las tendencias que dejó esta Ley se institucionalizaron con la Resolución 5633 de 2016, que reglamentó las condiciones y procedimientos para el acceso a las bases de datos de la Registraduría. En primer lugar, cualquier entidad y particular que cumpla funciones públicas puede pedir acceso a la base de datos por medio de una solicitud y cumpliendo con los requerimientos técnicos para utilizarla. En segundo lugar, se reguló la posibilidad de que los privados suscriban acuerdos con la Registraduría para acceder a la autenticación biométrica por medio de pagos a la RNEC. En tercer lugar, se determinaron los requisitos técnicos para que los operadores pueden cobrar para ofrecer los servicios tecnológicos a entidades o particulares interesados en la autenticación de las personas<sup>62</sup>.

Con los movimientos recientes de la RNEC es claro que la concepción de la identificación está cambiando. Por una parte, en un intento por hacer más seguro y moderno el proceso de identificación, se está recogiendo datos biométricos cada vez más sensibles de la población, mientras que se contratan costosos sistemas automatizados de identificación. Así, la relación de la ciudadanía con el Estado se vuelve más dependiente de la plena identificación, obligando a todas las instituciones públicas a implementar costosas tecnologías o una contratación con un tercero, inclusive, en zonas sin infraestructura para su funcionamiento.

Por otra parte, la RNEC se está convirtiendo en un administrador de la identidad biométrica de la población que cobra a los privados interesados en tener la certeza de individualidad (en su mayoría compañías financieras) por los datos personales sensibles de la ciudadanía.

---

<sup>59</sup> Ley 1753 de 2015

<sup>60</sup> Ley 1753 de 2015, artículo 159

<sup>61</sup> Resolución N. 5633 de 2016, artículo 33

<sup>62</sup> Resolución N. 5633 de 2016

La base de datos biométricos de la Registraduría es la más grande, pero, más allá de su tamaño, también representa una serie de cambios en términos de los niveles individualización y las lógicas que sostienen ese proceso.

En primer lugar, una base de datos biométricos pensada para la identificación de votantes solo para las elecciones se convirtió en un registro civil requerido para que la ciudadanía se relacione con el Estado al reclamar sus derechos, ampliando la base de sujetos susceptibles al proceso de recolección de datos biométricos. En segundo lugar, la base de datos biométricos que, a principios del siglo, estaba reservada para “poblaciones indeseadas” como las personas con procesos criminales se terminó uniendo con los registros civiles. En tercer lugar, la base de datos reservada para registro civil frente al Estado se convirtió en un prerrequisito para acceder a los derechos básicos de la ciudadanía –como se detalló también en la sección sobre la situación jurídica–, en una herramienta de la fuerza pública y un mecanismo de individualización e identificación frente a los privados.

### Base de datos biométrica de Migración Colombia BIOMIG (iris)

A finales de 2017, la Autoridad de Control Migratorio y de Extranjería del Estado Colombiano (en adelante, Migración Colombia) empezó a utilizar el sistema de Migración Biométrica (BIOMIG). Un sistema identificación automática fronteriza que utiliza datos biométricos del iris para identificar a las personas nacionales mayores de 12 años en su ingreso al país a través del Aeropuerto el Dorado de Bogotá (el más importante de Colombia). El sistema en la actualidad cuenta con 10 terminales y la inscripción es voluntaria con la cédula de ciudadanía, el pasaporte y un análisis de las treinta terminales para recolectar la información biométrica de las personas<sup>63</sup>.

Una vez se ha hecho el registro, la persona que ingresa al país debe digitar su número de identidad nacional en una pantalla táctil conectada a una barrera automática y colocarse a una distancia adecuada para que se realice la autenticación siguiendo los patrones del iris y se abran las puertas. Por esto, BIOMIG es un sistema fronterizo automatizado como los que hay en Europa y los Estados Unidos, pero es el primero en utilizar patrones biométricos del iris para autenticar a una persona<sup>64</sup>. Según informó el Director de Migración Colombia a la prensa, el terminal durante el proceso migratorio “se conecta automáticamente con diferentes bases de datos tanto nacionales como internacionales

---

<sup>63</sup> Presidencia de Colombia, «Migración Colombia empezó a usar sistema de inmigración de colombianos por medio de reconocimiento del iris.» (25 de Febrero de 2018).

<sup>64</sup> GEMALTO, *Los ojos son la solución - La solución de reconocimiento de iris de Gemalto acelera la inmigración en Colombia.* (GEMALTO, 2018)



[INTERPOL] para poder verificar si esta persona tiene algún impedimento u orden de captura”<sup>65</sup>.

La compra de los equipos se realizó a través del contrato número 117 de 2017 con la Unión Temporal de Control Fronterizo INCOMELEC-GEMALTO. La primera fase del contrato costó más de dos mil cien millones de pesos colombianos (675 mil dólares aproximadamente). A pesar de la Unión, la empresa encargada del sistema es la multinacional holandesa Gemalto que desarrolló un software para usar las terminales EF-45 de reconocimiento biométrico facial y de iris de la empresa CMI Tech<sup>66</sup>. El contratista tiene amplio historial y relaciones con el Gobierno colombiano y Migración Colombia<sup>67</sup>. En la actualidad, el sistema ya cuenta con terminales en cuatro aeropuertos de Colombia y hay planes de implementarlo en unidades móviles migratorias por conexión satelital<sup>68</sup>.

Migración Colombia señala que “la recolección [es] de más de 150 patrones biométricos entre los que se incluye el iris”. Igualmente, la descripción comercial de las terminales menciona la posibilidad de recoger patrones biométricos del rostro, incluidos el iris. En ese sentido, el sistema es capaz de recoger mucha más información que solamente la del iris<sup>70</sup>.

Según Migración Colombia, el sistema tiene varias justificaciones como la mejora de la percepción de seguridad a nivel internacional, la optimización de los procesos migratorios, la eficiencia financiera, la modernización de la entidad y la seguridad nacional<sup>71</sup>. En ese sentido, el sistema BIOMIG se presenta como una solución para todos los problemas de la entidad en términos de seguridad nacional y eficiencia en la atención al viajero. Igualmente, la idea inicial del sistema es centrarse en la población nacional colombiana para ampliarse a otros tipos de personas<sup>72</sup>.

De acuerdo a la información que nos fue entregada por Migración Colombia sobre la justificación jurídica del sistema, la entidad considera que puede hacer tratamiento de

---

65 Caracol Televisión, «Con solo una mirada, colombianos podrán ingresar en segundos al país.» Caracol Televisión, (27 de Febrero de 2018): <https://noticias.caracol.com/colombia/con-solo-una-mirada-colombianos-podran-ingresar-en-segundos-al-pais>.

66 Migración Colombia, Contrato No 117 de 2017 con la Unión Temporal de Control Fronterizo INCOMELEC-GEMALTO, (2017)

67 GEMALTO, *Los ojos son la solución*,

68 Becerra, Laura, «Cuatro aeropuertos del país ya cuentan con sistema de migración automática.» *La República*, (5 de Abril de 2018).

69 Migración Colombia, «Comunicado Oficial Biomig.» <http://migracioncolombia.gov.co/index.php/es/prensa/comunicados/comunicados-2018/febrero-2018/6539-en-menos-de-25-segundos-y-con-solo-una-mirada-los-colombianos-podran-ingresar-al-pais-migracion-colombia>, (25 de febrero de 2018)

70 Migración Colombia, “Contrato No 117 de 2017”

71 Migración Colombia, *Estudios Previos para el Contrato No 117 de 2017 con la Unión Temporal de Control Fronterizo INCOMELEC-GEMALTO*, (2017), 1-4

72 *Ibidem*, 6

datos biométricos<sup>73</sup>. A pesar de que Migración Colombia reconoce que los datos biométricos son sensibles y que deben mantenerse en reserva bajo la Ley 1581 de 2012, su tratamiento no requiere de una autorización previa dada la naturaleza misional de sus funciones. Considerando que Migración Colombia es una autoridad civil de seguridad del Estado, la Ley les permite hacer tratamiento de datos biométricos, a pesar de su naturaleza sensible, por razones de seguridad y defensa nacional<sup>74</sup>.

La base de datos biométricos BIOMIG es pionera en el uso de la identificación por iris en el control fronterizo automatizado, pero la pregunta que surge detrás su implementación subyace en el principio de proporcionalidad y la prioridad de proteger los datos sensibles de la ciudadanía. A pesar de que Migración Colombia pretende hacer más ágil y eficiente el proceso migratorio, la primera respuesta que ofrece el Estado al problema no puede ser un sistema que utiliza datos personales sensibles de la ciudadanía sin cuidado de los riesgos para los derechos humanos que este tipo de sistema representa. Igualmente, a pesar de que se plantea la necesidad de “optimizar los recursos financieros de la entidad”, no parece que implementar un sistema de esta naturaleza sea la respuesta lógica.

---

<sup>73</sup> Oficina de Asesoría Jurídica de Migración Colombia, «Memorando Concepto Jurídico: Autenticación biométrica.» (2017)

<sup>74</sup> Oficina de Asesoría Jurídica de Migración Colombia, “Memorando Concepto Jurídico”



# 4

## Usos de la base de datos de la RNEC

### Operadores biométricos

Como se mencionó, a partir de la publicación del Plan Nacional de Desarrollo 2010-2014, se abrió la posibilidad de utilizar las bases de datos generadas por entidades públicas y particulares en ejercicio de funciones públicas de forma “permanente y gratuita” por otras entidades que lo requieran para los programas y proyectos de ese Gobierno<sup>75</sup> Ahora bien, el proceso de cambiar la lógica de las bases de datos biométricas de la Registraduría no se daría hasta la publicación del Decreto 019 de 2012, que introdujo el uso de medios electrónicos para autenticar a la ciudadanía en procedimientos que llevan a cabo entidades públicas o quien ejerza funciones públicas de diversa índole: financieros, pensionales, registros públicos, la expedición de pasaportes y visas, entre otros<sup>76</sup>.

Las siguientes regulaciones de la Registraduría pusieron a disposición de las entidades públicas y los particulares que prestan servicios públicos la base de datos biométricos de la RNEC<sup>77</sup>. De nuevo, dicho acceso estaba enmarcado en la lógica de luchar contra la suplantación y el fraude. Así mismo, el acceso está condicionado al envío de un escrito que indicara el tipo de información requerida por la entidad interesada, los propósitos y razones en que se fundamenta la necesidad de tal información. Igualmente, se requiere de la presentación de una prueba técnica para analizar el desempeño de la plataforma tecnológica de la entidad solicitante; habilitando tres modalidades de acceso a la base de

---

<sup>75</sup> Ley 1450 de 2011, artículo 227

<sup>76</sup> Ley 1450 de 2011, artículo 17 y 18

<sup>77</sup> Resolución N. 3341 de 2013 y Resolución N. 5633 de 2016

datos de la Registraduría: el hosting dedicado<sup>78</sup>, el housing o collocation<sup>79</sup>, y la infraestructura propia<sup>80</sup>.

Con lo anterior, aparecieron los “aliados tecnológicos”, que son operadores de la infraestructura tecnológica que le permite a las entidades y a los particulares acceder a la base de datos de la Registraduría si cumplen con los requisitos determinados por esta. En la práctica, son quienes disponen los lectores de huella digital y la conexión con la base de datos de la RNEC. Entre los requisitos está la experiencia certificada en autenticación biométrica de al menos tres años, infraestructura tecnológica, capacidad financiera y superar la prueba técnica realizada por la Registraduría.

A partir de ahí, los actores que quieran utilizar la base de datos de la RNEC dependen de los aliados tecnológicos para poder ejercer sus funciones. En cuanto a los particulares, que incluyen prestadores de servicios financieros de entidades públicas, fondos de pensiones, operadores bursátiles, aseguradoras y notarías, deben pagar unos montos por consulta establecidos por la Registraduría anualmente. De esta forma, la base de datos biométricos de la Registraduría se convirtió en un negocio impulsado desde la RNEC para que privados presten servicios tecnológicos al Estado y particulares que cumplan funciones públicas<sup>81</sup>.

## Sistema Appolo de la Policía Nacional

Desde 2018, la Policía Nacional comenzó a utilizar una herramienta tecnológica fabricada por la empresa Olimpia, que utiliza un dispositivo parecido a un móvil que, por medio de internet, accede a la base de datos de la Registraduría para autenticar a una persona y cotejar si existen órdenes nacionales o internacionales de captura.

Según la Policía Nacional, este procedimiento toma alrededor de cinco segundos y cuenta con un sistema de seguridad que utiliza la geolocalización para asegurar que sea utiliza-

---

78 Resolución N. 3341 de 2013, art. 18, a. “Hosting dedicado. La Entidad Pública o el tercero autorizado por esta, podrá contratar el servicio de Hosting dedicado (plataforma de hardware, software y licenciamiento) con el proveedor del Data Center, en donde la Registraduría ha dispuesto la base de datos biométrica para consulta. El servicio de Hosting contempla el arrendamiento del uso de la plataforma tecnológica definida e implementada por la Registraduría Nacional del Estado Civil (...)”

79 Resolución N. 3341 de 2013, art. 18 b. “Housing o Collocation. La Entidad Pública o el tercero autorizado por esta, podrá contratar el servicio de Housing o Collocation con el proveedor del Data Center en donde la Registraduría ha dispuesto la base de datos biométrica para consulta, con el fin de instalar, o alojar, en él su propia infraestructura necesaria para el acceso a la base de datos de información biométrica de la Registraduría Nacional del Estado Civil (...)”

80 Resolución 3341 de 2013, art. 18 c. “Infraestructura propia. La Entidad Pública o el tercero autorizado por esta, deberá instalar en un data center Tier 3, bajo su cuenta y riesgo, la plataforma tecnológica completa (sistema de almacenamiento, hardware, software y licenciamiento) definida por la Registraduría Nacional del Estado Civil (...)”

81 La RNEC ha publicado una lista de las entidades públicas o que prestan funciones públicas con las cuales hay un convenio vigente para la consulta del Archivo Nacional de Identificación que está disponible en: <https://www.registraduria.gov.co/-Consultas-ANI-.html>

do por el personal autorizado<sup>82</sup>. Además de la consulta en las bases de datos de órdenes de captura, el dispositivo permite cotejar los datos de la Cédula de Ciudadanía (presentes en el código de barras) con los de la base de datos de la Registraduría, lo que asegura que el documento es original<sup>83</sup>. Adicionalmente, la Policía espera que estos dispositivos puedan ser utilizados con nuevas características como reconocimiento facial y de iris<sup>84</sup>.

El proceso para adquirir y construir el sistema de biometría móvil Appolo comenzó en 2016 y costó 895 millones de pesos (287 mil dólares aproximadamente)<sup>85</sup>. Para su funcionamiento, fue necesario un convenio con la RNEC para tener un acceso directo a las bases de datos biométricas basados en la Resolución 3341 de 2013.

De acuerdo con la Policía, este sistema parte de tres preocupaciones. Primero, una necesidad de innovación en la investigación criminal. Segundo, una preocupación por la seguridad nacional, pues la identificación plena de las personas permitiría tomar acciones más efectivas y confiables para la seguridad nacional<sup>86</sup>. Para la Oficina de Telemática de la Policía, “es de suma importancia el cotejo biométrico de ciudadanos en diligencias de control y vigilancia, que permitan la identificación de los colombianos como un tema de seguridad nacional”<sup>87</sup>. En tercer lugar, el dispositivo permitiría facilitar la validación de la identidad en cualquier momento para luchar contra la falsificación de documentos y la suplantación<sup>88</sup>.

## Asobancaria

Con las posibilidades que dejó la legislación, las instituciones financieras y bancarias empezaron un proceso de integración de la autenticación biométrica a la provisión de sus servicios. De esta forma, mediante el Contrato 027 de 2016, la Registraduría suscribió un solo convenio con la Asociación Bancaria y de Entidades Financieras de Colombia (en

---

82 Policía Nacional, «Proyecto autenticación biométrica Policía Nacional.» (19 de Junio de 2018), disponible en: <https://www.policia.gov.co/noticia/proyecto-autenticacion-biometrica-policia-nacional>.

83 El País, «Los nuevos gadgets de la Policía con los que verifican identidad y antecedentes en segundos.» *El País.com.co*, (9 de Mayo de 2018), disponible en: <https://www.elpais.com.co/judicial/los-nuevos-gadgets-de-la-policia-con-los-que-verifican-identidad-y-antecedentes-en-segundos.html>.

84 Camacho, Laura, «La Policía ahora revisará sus antecedentes judiciales con la huella.» *El Tiempo*, (21 de Mayo de 2018), disponible en: <https://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/policia-implementa-la-identificacion-biometrica-en-sus-procedimientos-214926>.

85 Oficina de Telemática de la Policía Nacional, «Estudios previos para Contrato de Compraventa 06-7-10081-16: Sistema de Biometría Móvil.» (2016), disponible en: <https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=16-1-157976>

86 *Ibidem*.

86 *Ibidem*.

87 *Ibidem*,2

88 *Ibidem*.

adelante, Asobancaria)<sup>89</sup>. Es decir, este contrato permite a todas las instituciones financieras y bancarias acceder a las bases de datos de la Registraduría.

Igualmente, el convenio les permite tener acceso no solo a los datos biométricos, sino también a la información biográfica. Este acceso se hace a través de un aliado tecnológico llamado CertiCámaras, que presta su infraestructura para la recolección de la información biométrica que luego se coteja con la base de datos de la Registraduría<sup>90</sup>. Así, las instituciones financieras deben pagar unos montos determinados por la Registraduría para acceder a las bases de datos.

De acuerdo con Asobancaria, la autenticación biométrica en el sistema financiero colombiano trae beneficios tanto para las personas como para las entidades financieras. Para este gremio, esto representa una modernización que hace más rápida las transacciones, mitiga el riesgo de suplantación y hace una transformación digital aplicando la política de “cero papel”. Igualmente, la autenticación biométrica representa una posibilidad para las entidades de ofrecer servicios de forma automatizada y asegurar la identificación de los datos financieros de cada cliente<sup>91</sup>.

## Elecciones

Hace diez años la RNEC utilizó por primera vez la autenticación biométrica en procesos electorales atípicos. Según la Registraduría, se planeaba implementar tres nuevos controles en el proceso de votación: la identificación del votante en la base de datos del censo electoral, la entrega del documento de identidad y la autenticación mediante suhuella dactilar. Dichos procedimientos permitirían evitar la suplantación o la doble votación en las elecciones atípicas<sup>92</sup>. De hecho, la RNEC argumentó que los nuevos procedimientos eran una respuesta al fallo del Consejo de Estado en 2005, que constató que había más votos que votantes para las elecciones al Congreso de la República de 2002<sup>93</sup>. A partir de ahí, la Registraduría ha masificado gradualmente el uso de la biometría en los procesos electorales hasta utilizarlo en cerca de 33 comicios<sup>94</sup>.

---

89 Asobancaria . «Autenticación biométrica para usuarios del sistema financiero colombiano.» (2016), disponible en: <https://www.asobancaria.com/biometria/>

90 *Ibidem*.

91 Asobancaria, «Biometría: conveniente y segura.» *Semana Económica* 2018 (2018).

92 Registraduría Nacional del Estado Civil, «Suplantación de electores: un fraude más recurrente en el mapa de riesgo electoral.» *Nuestra Huella*, (2009), disponible en: <https://www.registraduria.gov.co/Edicion-No-34-Ano-V-diciembre-de.html#01>.

93 Registraduría Nacional del Estado Civil, *ESTE DOMINGO LOS HABITANTES DE SALAZAR DE LAS PALMAS (NORTE DE SANTANDER) Y BELÉN DE LOS ANDAQUÍES (CAQUETÁ) ELEGIRÁN SUS NUEVOS ALCALDES*, (2009), disponible en: <https://www.registraduria.gov.co/ESTE-DOMINGO-LOS-HABITANTES-DE.1563.html>

94 Registraduría Nacional del Estado Civil, «La huella dactilar: la base del sistema de identificación en Colombia.» *Nuestra Huella*, (2012), disponible en: [https://www.registraduria.gov.co/rev\\_electro/2012/rev\\_elec\\_noviembre/revista\\_noviembre2012.html#10](https://www.registraduria.gov.co/rev_electro/2012/rev_elec_noviembre/revista_noviembre2012.html#10).



# 5

## Proyectos

### Nuevas bases de datos biométricos

#### Sistema Multibiométrico ABIS (Automated Biometric Identification System)

Entre los proyectos que plantean utilizar nuevos datos biométricos está la contratación de un sistema de identificación biométrica de rostros y palmas para la Policía Nacional de Colombia. En 2017, la Policía Nacional presentó un proyecto para “la adquisición, instalación, implementación, prueba, puesta en servicio, garantía, soporte y mantenimiento de un sistema biométrico facial, palmar y dactilar” para reforzar la política “Vigilancia Comunitaria por Cuadrantes”. Para su financiación, la Policía Nacional aportó 6,120 millones de pesos y el Ministerio del Interior otros 6 mil millones de pesos. El ganador del concurso fue la Unión Temporal Tecnom<sup>95</sup>. De acuerdo a los informes del proyecto, todavía no está terminado, pero se espera que se concluya a finales de marzo del 2019<sup>96</sup>.

De acuerdo con los Estudios Previos del Contrato, la necesidad del sistema biométrico se sustenta en la Ley 62 de 1993, la cual establece la razón de ser de la Policía Nacional como la responsable de la ejecución de la policía judicial. Además, se argumenta que la adquisición de un sistema como este representaría un aporte “significativo e importante a la administración de la justicia” porque brinda análisis científicos y técnicos que ayudan a la individualización del crimen. Igualmente, según la Policía, en términos técnicos representa la mejora del sistema biométrico que se tiene en la actualidad, el cual presenta problemas en el almacenamiento y tiempos de respuesta. En este sentido, hay una necesidad de que “la labor policial sea mucho más eficiente y efectiva”<sup>97</sup>.

<sup>95</sup> Policía Nacional de Colombia, «Estudios previos para la adquisición, instalación, implementación, prueba, puesta en servicio, garantía, soporte y mantenimiento de un sistema biométrico facial, palmar y dactilar.», (Bogotá, 2017).

<sup>96</sup> Policía Nacional de Colombia, «Prórroga No. 5 al contrato de compraventa No. 203-1-2017.», (Bogotá, 2018).

<sup>97</sup> Policía Nacional de Colombia, “Estudios previos para la adquisición”, 4

El discurso de la modernización de la lucha contra el crimen es una constante en el contrato, pues, según la Policía, es necesario cambiar la plataforma AFIS por una más moderna que permita el cotejo de información dactilar, facial y palmar, como un Sistema Automático de Identificación Biométrica (ABIS). Esto con el fin de lograr la “interconectividad con plataformas biométricas”<sup>98</sup>. Así mismo, esta nueva tecnología permitiría la individualización e identificación de personas por medio del uso de “imágenes extraídas de videos de cámaras de seguridad localizadas en puntos estratégicos”<sup>99</sup>. La Policía argumenta que este sería un procedimiento no invasivo, el cual estaría basado en datos como la localización y características faciales o un análisis global de la cara.

En términos prácticos, la construcción del sistema dependerá de las bases de datos de personas con investigaciones criminales con las que cuenta la Policía Nacional de la DIJIN-INTERPOL y del suprimido DAS. Dichas bases de datos guardan “casos criminales (latentes y fragmentos de huella) y fotografías”<sup>100</sup>. Las dos bases de datos cuentan con una plataforma tecnológica que fue instalada en 2008 para AFIS-DAS y en el 2009 para AFIS-DIJIN por la multinacional IDEMIA.

La Policía Nacional espera que el sistema funcione como un apoyo al Modelo Nacional de Vigilancia Comunitaria por Cuadrantes. Por un lado, uno de los retos es lograr analizar videos para la extracción e identificación de rostros en hechos criminales. Por otro lado, el sistema debería funcionar con 163 dispositivos comprados fabricados por la empresa IDEMIA llamados Morpho RapID que permiten la identificación facial y dactilar. Sin embargo, los dispositivos solo funcionaban con el sistema AFIS y no para los datos faciales porque la Policía no cuenta con el software necesario para cotejar las características únicas de los rostros. Por esto, un objetivo del contrato es que el sistema ABIS pueda utilizar las fotografías de las bases de datos criminales para buscar patrones faciales utilizando los Morpho RapID. Con esto, se estima una “mejora en la gestión, asegurando el máximo rendimiento, efectividad y desempeño misional”<sup>101</sup>, por medio de la individualización rápida.

Si el proyecto se concreta y efectivamente puede realizarse la identificación de rostros a partir de videos, sería necesario analizar la aplicación de la ley de protección de datos de acuerdo con lo que ha decidido la Delegatura de Protección de Datos. De acuerdo con la interpretación que se explicó en el primer aparte de este documento, las fotografías no son datos biométricos sino hasta que se hace un procedimiento de análisis para usar las características físicas para identificar a una persona. En este caso, no se ha hecho un análisis sobre las justificaciones para exceptuar la aplicación de la ley de protección de datos o, si es jurídicamente inviable esta excepción, el riesgo de quienes instalan cámaras en establecimientos privados.

---

<sup>98</sup> *Ibidem*, 6

<sup>99</sup> *Ibidem*, 6

<sup>100</sup> Policía Nacional de Colombia, “Estudios previos para la adquisición”, 3

<sup>101</sup> *Ibidem.*, 3



En cuanto al desarrollo del contrato, se encontraron cinco prórrogas, pues el contratista no pudo cumplir con los tiempos del contrato por dificultades técnicas en la migración de las bases de datos. Así, la Unión Temporal se vio obligada a subcontratar con empresas con experiencia para desarrollar el sistema ABIS como IDEMIA para encargarse de los registros decadaclares y de palmas, y HERTA para encargarse de los sistemas de reconocimiento facial<sup>102</sup>. Como se mencionó, IDEMIA se había encargado del antiguo sistema AFIS, ahora debía hacer la migración del sistema para unificarlo con las nuevas características del sistema ABIS. En cuanto a HERTA, fue necesario realizar la migración de cerca de 44,000 fotografías para incluirlas en la base de datos y la instalación de sus aplicativos en el sistema de la Policía<sup>103</sup>. Los aplicativos de HERTA que fueron adquiridos por la Policía fueron Biodatabase para la migración de bases de datos, Biogenerator para generar un modelo 3D de los rostros de una base de datos de fotografías y el Biofinder para análisis forense de videos para identificar e individualizar<sup>104</sup>.

A pesar de las promesas del sistema, las bases de datos de imágenes parecen ser en ocasiones de baja calidad o sin datos personales<sup>105</sup>. Así que será difícil que el sistema sea funcional para los intereses de la Policía Nacional de utilizar sus sistemas de cámaras y sus dispositivos Morpho RapID. Sin embargo, lo que se puede extraer del análisis de los contratos es el afán de la fuerza pública para contar con sistemas de identificación biométrica más modernos, sin tener una justificación funcional y social.

Hace apenas diez años, la Policía había hecho una gran inversión en un sistema AFIS. Hace seis creó un convenio con la Registraduría y hace dos contrató el sistema Appolo para masificar el uso de ese sistema. Sin embargo, la Policía había comprado dispositivos que podían usar reconocimiento facial, como los Morpho RapID, sin tener la infraestructura para ello. Por esto, la Policía busca crear un sistema que reemplace el AFIS para poder utilizar reconocimiento facial en unos dispositivos que, en algunos casos, ya son obsoletos para el sistema que quiere instaurar. En otras palabras, la Policía Nacional adquiere sistemas bajo el argumento de la modernización para los que no cuenta con el soporte y que, posteriormente, terminan justificando nuevas adquisiciones para hacerlos funcionales. Con esto, el Estado queda atrapado en el discurso de las soluciones tecnológicas a problemas sociales: si ocurre un hecho en el que puedan emplearse estos sistemas, hay una razón para gastar más. Si las condiciones de seguridad se mantienen estables o mejoran, hay una justificación para lo que se está gastando. Esta forma de analizar el problema de la vigilancia y el uso de datos biométricos es, como dice Hayes, un “argumento [que] amenaza con afianzar los gastos en seguridad hasta el infinito”<sup>106</sup>.

---

102 Policía Nacional de Colombia, «Prórroga No. 1 al contrato de compraventa No. 203-1-2017.», (Bogotá, 2017)

103 Policía Nacional de Colombia, «Prórroga No. 3 al contrato de compraventa No. 203-1-2017.», (Bogotá, 2017)

104 *Ibidem*.

105 Policía Nacional de Colombia, «Prórroga No. 3 al contrato de compraventa No. 203-1-2017.», (Bogotá, 2017)

106 Hayes, Ben. «The surveillance industrial complex.» En *Routledge handbook of surveillance studies*, de Kirstie Ball, David Lyon y Kevin Haggerty. (Routledge, 2012)

El proceso de inclusión de las tecnologías de identificación facial parece seguir la misma lógica de la identificación dactilar. De la misma manera que la recolección de datos decadaclulares arrancó con las poblaciones carcelarias, la identificación facial apunta a recoger los datos de las personas con investigaciones criminales en un esfuerzo por la modernización de la Policía Nacional. Asimismo, mientras que la Policía trata de construir un sistema de identificación facial<sup>107</sup>, la Registraduría ha estado, desde 2016, organizando un sistema multibiométrico que incluye la identificación facial. Continuando con el patrón de los datos dactilares, Asobancaria y las Notarías han pedido a la Registraduría que comience a desarrollar el servicio de autenticación facial para particulares en funciones públicas<sup>108</sup>. Ahora bien, la Registraduría no ha informado a la opinión pública del avance de este proyecto y no ha publicado contratos o estudios previos al respecto.

## Nuevos usos para las bases existentes

### Autenticación biométrica en los Servicios Ciudadanos Digitales

Desde 2014, el Gobierno colombiano tenía proyectos para crear un espacio de almacenamiento de la información de la ciudadanía que facilitara la comunicación entre las entidades del Estado y los trámites de la ciudadanía<sup>109</sup>. El proyecto denominado “Carpeta Ciudadana” buscaba crear un Estado más eficiente y moderno a través de la utilización de tecnologías de la información<sup>110</sup>.

En 2017, el MinTIC unió el proyecto de “Carpeta Ciudadana” a otros proyectos que ya estaban en marcha en un sistema denominado “Servicios Ciudadanos Digitales” o SCD<sup>111</sup>. Con esto se buscaba darle solidez a Carpeta Ciudadana fusionándola con otros proyectos en curso como partes integrales: autenticación biométrica, autenticación electrónica e interoperabilidad. En primer lugar, la autenticación biométrica se encargará de enrollar a las personas en el sistema con patrones biométricos dactilares de la base de datos de la RNEC. En segundo lugar, la autenticación electrónica otorgará certificación digital de los datos que circulan en el sistema; la interoperabilidad se encargará de que los datos de una entidad puedan ser compartidos a otra dentro del sistema. Finalmente, el

---

107 *El Tiempo*, «La identificación por biometría facial, lo que viene para 2019.» *El Tiempo*, (4 de Diciembre de 2018), disponible en: <https://www.eltiempo.com/politica/gobierno/la-identificacion-por-biometria-facial-lo-que-viene-para-2019-301504>.

108 *El Heraldo*. «Notarios del país pedirán a Registraduría adoptar la biometría facial.» *El Heraldo*, (6 de Julio de 2018), disponible en: <https://www.elheraldo.co/colombia/notarios-del-pais-pediran-registraduria-adoptar-la-biometria-facial-515470>.

DataIFX, «En 2019, bancos comenzarán a implementar la biometría facial en el país.» DataIFX, (19 de Septiembre de 2018), disponible en: <http://www.dataifx.com/noticias/en-2019-bancos-comenzaran-implementar-la-biometria-facial-en-el-pais>.

109 Ministerio de las Tecnologías de la Información y las Comunicaciones, *Carpeta Personal: sus documentos en un solo lugar*. (Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones, 2014)

110 Ley 1753 de 2015

111 Decreto 1413 de 2017

componente básico es que la Carpeta Ciudadana que se encargará de almacenar los datos de la ciudadanía para que circulen dentro del ecosistema de SCD.

En el diseño final del sistema, el centro del modelo es el “Articulador” cuya función es administrar y establecer los acuerdos entre las empresas que pueden operar alguna de las partes del sistema. Así, en 2018, se creó la Agencia Nacional Digital, una asociación público-privada que se va a encargar de la administración, monitoreo, vigilancia y la selección de los operadores de SCD. El mismo año se publicaron los manuales para establecer los requisitos para selección de las empresas operadoras de cada uno de los componentes. De esta forma, se espera que en lo corrido de este año se seleccionen las empresas que podrán ser operadoras de alguna parte del sistema<sup>112</sup>.

---

<sup>112</sup>Ministerio de las Tecnologías de la Información y las Comunicaciones, *Estudio del Sector para Servicios Ciudadanos Digitales*, (Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones, 2018)



# 6 Conclusiones

El análisis de la situación jurídica de los datos biométricos no es suficiente para ver las justificaciones del uso de datos biométricos por dos razones. En primer lugar, las leyes de protección de datos y las decisiones judiciales o administrativas que parten de ellas se han aplicado en su mayoría a las relaciones entre personas particulares y empresas, no a la relación entre las personas y el Estado. Aunque estas decisiones son una guía para determinar qué se entiende en Colombia por dato biométrico, las limitaciones y los requisitos para su uso por parte del Estado aún no han sido discutidas con el mismo nivel de profundidad que en el ámbito privado y comercial. La dificultad de determinar las justificaciones para el uso de datos biométricos en el sector público también deriva de la falta de competencia de la Delegatura para la protección de datos de sancionar a funcionarios y entidades públicas por el incumplimiento de la ley de protección de datos. Esta competencia corresponde a la Procuraduría General de la Nación, pero, hasta donde se ha podido indagar, no se ha hecho ninguna investigación por el incumplimiento de la ley de protección de datos en el sector público. En segundo lugar, las leyes de protección de datos colombianas autorizan el conocimiento o tratamiento de datos personales sin autorización del titular a autoridades de la rama judicial, ejecutiva y a los organismos de control cuando se hace con fines “históricos, estadísticos o científicos” o cuando son datos relacionados con el registro civil. En ese sentido, para el tratamiento de datos sensibles no se requiere autorización del titular. Esta excepción ha sido aplicada directamente, por ejemplo, para la conformación de la base de datos biométrica de Migración Colombia. Los criterios para determinar la legitimidad de la conformación de una base de datos estatal no son sofisticados. El límite más importante para la creación de una base de datos biométrica, como se puede interpretar de las decisiones de la Delegatura para la Protección de Datos y teniendo en cuenta solo la naturaleza del dato biométrico es que responda a un fin constitucionalmente admisible. Este criterio no ofrece mucha certeza sobre qué es “admisible”, especialmente si queremos aplicarlo, por ejemplo, a la base de datos de Migración Colombia o a los proyectos en curso. Por esto, valdría la pena hacer énfasis en la precisión que hizo la Corte Constitucional en el sentido de que el tratamiento de datos

---

113 Ley 1266 de 2008 artículo 5; Ley 1581 de 2012 artículo 10

sensibles solo puede ser exigido para prestar servicios esenciales.

Las leyes de protección en Colombia están basadas en la idea de libertad de decisión para consentir el tratamiento de datos biométricos. Sin embargo, dicha suposición puede ser problemática cuando analizamos la relación entre el Estado y la ciudadanía. El consentimiento será difícilmente libre e informado cuando la ciudadanía dependa del Estado para el acceso a un servicio esencial.

Las limitaciones de las leyes de protección de datos nos obligan a buscar vías alternativas para abordar el problema del tratamiento de datos biométricos. Por esta razón, este texto apostó por deconstruir las prácticas de producción de las bases de datos biométricas en búsqueda de sus justificaciones y transformaciones. De esta forma, es posible determinar las lógicas que sustentan la construcción de estas bases de datos y pensar modelos alternativos de la relación Estado-ciudadanía.

En este documento exploramos tres bases de datos biométricas estatales a cargo de la Registraduría Nacional del Estado Civil –RNEC–, la Policía Nacional y Migración Colombia.

La base de datos de la RNEC fue construida desde principios del siglo XX para autenticar la identidad del votante, sin embargo, sus usos se ampliaron a través de la conexión con otras bases de datos, con la posibilidad de que otras entidades públicas o empresas privadas pudieran consultar dicha base de datos, o a través de la automatización del reconocimiento de huellas dactilares. De esta forma, la relación del Estado y la ciudadanía estaba mediada por la recolección de datos biométricos y la confianza en individualidad de estos datos, lo que convirtió a esta base en un prerrequisito para acceder a los derechos básicos de la ciudadanía, una herramienta de la fuerza pública y un mecanismo de individualización e identificación frente a los privados.

El movimiento hacia la tercerización y universalización de la biometría en la relación ciudadanía-Estado se potencia con la autenticación biométrica de Servicios Ciudadanos Digitales. Otro ejemplo de uso externo de la base de datos de la RNEC es el sistema Appollo. La Policía Nacional y el antiguo servicio de inteligencia –DAS– comenzaron a principios del siglo XX a recoger datos biométricos para apoyar investigaciones criminales, pero su automatización solo se dio hasta los años noventa con el apoyo de los Estados Unidos. Esta base se interconectó con la de la RNEC y hoy incluso se busca usar dispositivos portátiles para autenticar con la huella a la ciudadanía en espacios públicos por requerimiento de los oficiales de policía.

La segunda base de datos biométricos explorada en este texto fue la de Migración Colombia, que cuenta con registros de iris de población nacional colombiana que viajan al exterior. Este sistema se construyó sobre la idea de la necesidad de automatizar el control migratorio y asegurar un control de seguridad nacional.

Las bases de datos decadactilares no son las únicas en Colombia. Desde 2017, la Policía Nacional, con apoyo del Gobierno nacional, inició el proceso de construcción de una base de datos biométricos para reconocimiento facial. Para eso, se contrató multinacionales y nuevos aplicativos para utilizar las fotografías de personas con investigaciones criminales de las bases de datos de la Policía. Sin embargo, las fotografías a duras penas llegan a 44.000 registros. El objetivo de modernizar las bases de datos se relaciona con la necesidad de hacer funcionar dispositivos de reconocimiento facial previamente adquiridos sin un sistema que los respalde. Asimismo, la Registraduría también está en un proceso de construcción de una base de datos para reconocimiento facial que pueda interoperar con la que construye la Policía.

En la construcción de las bases de datos analizadas en este texto encontramos patrones que se deben señalar. En primer lugar, la historia de la construcción de las bases de datos hace visible un proceso de paulatina universalización de la identificación biométrica basado en un sueño de automatizar cualquier tipo de actuación pública. Así, el contrato social basado en la confianza del Estado en la ciudadanía se empieza a diluir poniendo la biometría como requisito y la tecnología automatizada de identificación como intermediario de su relación.

En segundo lugar, el proceso de universalización de la biometría ha mostrado un cambio de propósito de los datos recogidos que no cumple con los principios de finalidad y proporcionalidad. Por esto, los datos biométricos recogidos para escenarios únicos como las elecciones o una investigación criminal se empiezan a universalizar para utilizarse en cualquier tipo de actuación. Incluso, como ejemplifica la RNEC, el Estado comienza a comportarse como una empresa al ofrecer un servicio de autenticación de la identidad del ciudadano para cualquier privado que lo considere necesario.

De esta forma, justificaciones como la eficiencia del gasto, la modernización del Estado o la seguridad nacional permiten recoger cualquier tipo de dato en cualquier condición y usarlo para diversos fines, sin importar el daño que pueda significar en el ejercicio de los derechos por parte de la ciudadanía. Si en los usos de las bases de datos biométricas se materializa la relación entre los principios de protección de datos y los límites y requisitos del tratamiento, es necesario analizar con más detalle estas justificaciones y explorar empíricamente su impacto en la seguridad o en la prevención de fraudes en casos concretos.

En tercer lugar, el Estado hace grandes gastos en sistemas de identificación biométrica, como el caso de la Policía o Migración Colombia, para los que no cuenta con la tecnología

o el personal capacitado. Sin embargo, esos gastos no se justifican a partir de análisis de los costos que puede generar su mantenimiento, actualización o del impacto de usar estos sistemas en la relación con la ciudadanía. Igualmente, los nuevos sistemas y el afán por modernizar no se detienen para analizar si la posible afectación a los derechos humanos es proporcional respecto a los fines que persigue. En ese sentido, el afán por modernizar el Estado termina siendo menos eficiente para el gasto y para los intereses públicos de la protección de los derechos ciudadanos.

Para determinar si la conformación y uso de bases de datos biométricas en el Estado cumple con los principios de la ley de protección de datos y es necesaria y proporcional respecto a la forma en la que afecta derechos humanos, es necesario pensar en un marco que permita evaluar distintos aspectos de dichos principios. Hasta el momento, las autoridades se limitan a citar fallos de la Corte Constitucional y la ley misma, pero no existe una herramienta que permita cuestionar aspectos concretos del cumplimiento de los principios de la ley de protección de datos.

Finalmente, es necesario hacer descripciones más densas de los aspectos técnicos de la biometría para ver dónde y cómo se materializan los discursos que justifican la implementación de este tipo de tecnologías, así como este análisis debe complementarse con las prácticas de construcción del dato biométrico.



# 7

## Bibliografía

Álzate, Juan David. «Entre rostros y huellas. Una aproximación a los procedimientos aplicados a la investigación judicial por homicidio en Medellín-Colombia (1900-1930).» TRASHUMANTE | Revista Americana de Historial Social, 2013: 32-55.

Asobancaria . «Autenticación biométrica para usuarios del sistema financiero colombiano.» <https://www.asobancaria.com/biometria/>, 2016.

Asobancaria. «Biometría: conveniente y segura.» Semana Económica 2018 (Semana económica 2018), 2018.

Banco Interamericano de Desarrollo. Inventario de los registros civiles e identificación de América Latina y el Caribe. Washington: BID, 2010.

Becerra, Laura. «Cuatro aeropuertos del país ya cuentan con sistema de migración automática.» La República, 5 de Abril de 2018.

Camacho, Laura. «La Policía ahora revisará sus antecedentes judiciales con la huella.»

El Tiempo, 21 de Mayo de 2018: <https://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/policia-implementa-la-identificacion-biometrica-en-sus-procedimientos-214926>.

Caracol Televisión. «Con solo una mirada, colombianos podrán ingresar en segundos al país.» Caracol Televisión, 27 de Febrero de 2018: <https://noticias.caracoltv.com/colombia/con-solo-una-mirada-colombianos-podran-ingresar-en-segundos-al-pais>.

Congreso de la República de Colombia. “Ley 89 de 1948”, 1948.

Congreso de la República de Colombia. “Ley 39 de 1961”, 1961.

Congreso de la República de Colombia. “Ley 1266 de 2008”, 2008.



Congreso de la República de Colombia. “Ley 1451 de 2011”, 2011.

Congreso de la República de Colombia. “Ley 1581 de 2012”, 2012.

Congreso de la República de Colombia. “Ley 1704 de 2012”, 2012.

Congreso de la República de Colombia. “Ley 1753 de 2015”, 2015.

Corte Constitucional de Colombia. “Sentencia T-1031 del 30 de octubre de 2003, M.P. Eduardo Montealegre Lynett”, 2003.

Corte Constitucional de Colombia. “Sentencia C-1011 del 16 de octubre de 2008, M.P. Jaime Córdoba Triviño”, 2008.

Corte Constitucional de Colombia. “Sentencia T-312 del 4 de abril de 2008, M.P. Rodrigo Escobar Gil”, 2008.

Corte Constitucional de Colombia. “Sentencia T-1038 del 14 de diciembre de 2010, M.P. Jorge Iván Palacio Palacio”, 2010.

Corte Constitucional de Colombia. “Sentencia C-748 del 6 de octubre de 2011, M.P. Jorge Ignacio Pretelt Chaljub”, 2011.

Corte Constitucional de Colombia. “Sentencia T-1000 del 26 de noviembre de 2012, M.P. Jorge Iván Palacio Palacio”, 2012.

Corte Constitucional de Colombia. “Sentencia T-561 del 17 de julio de 2012, M.P. María Victoria Calle”, 2012.

Corte Constitucional de Colombia. “Sentencia T-020 del 27 de enero de 2014, M.P. Luis Guillermo Guerrero”, 2014.

Corte Constitucional de Colombia. “Sentencia T-531 del 26 de septiembre de 2016, M.P. Gabriel Eduardo Martelo”, 2016.

Corte Constitucional de Colombia. “Sentencia T-114 del 3 de abril de 2018, M.P. Carlos Bernal Pulido”, 2018.

Corte Suprema de Justicia de Colombia. Sala de Casación Laboral. “Radicado 69577, sentencia del 9 de noviembre de 2016, M.P. Jorge Luis Quiroz Alemán”, 2016.

DataIFX. «En 2019, bancos comenzarán a implementar la biometría facial en el país.»

DataIFX, 19 de Septiembre de 2018: <http://www.dataifx.com/noticias/en-2019-bancos-comenzarán-implementar-la-biometría-facial-en-el-país>.

Departamento Administrativo de Seguridad de Colombia. “Decreto 4057 de 2011”, 2011.  
Departamento Administrativo de la Función Pública. “Decreto 019 de 2012”, 2012

El Heraldo. «Notarios del país pedirán a Registraduría adoptar la biometría facial.» El Heraldo, 6 de Julio de 2018: <https://www.elheraldo.co/colombia/notarios-del-pais-pedirán-registraduría-adoptar-la-biometria-facial-515470>. El País. «Los nuevos gadgets de la Policía con los que verifican identidad y antecedentes en segundos.» El País.com.co, 9 de Mayo de 2018: <https://www.elpais.com.co/judicial/los-nuevos-gadgets-de-la-policia-con-los-que-verifican-identidad-y-antecedentes-en-segundos.html>.

El Tiempo. «La identificación por biometría facial, lo que viene para 2019.» El Tiempo, 4 de Diciembre de 2018: <https://www.eltiempo.com/politica/gobierno/la-identificacion-por-biometria-facial-lo-que-viene-para-2019-301504>.

Fondo Rotatorio de la Policía Nacional de Colombia. Estudio y documentos previos con objeto “adquisición, instalación, implementación, licenciamiento, prueba, puesta en servicio, garantía, soporte y mantenimiento de un sistema biométrico facial, palmar y dactilar para la Policía Nacional”. Ministerio de Defensa Nacional, 2017.

GEMALTO. Los ojos son la solución - La solución de reconocimiento de iris de Gemalto acelera la inmigración en Colombia. GEMALTO, 2018.

Hayes, Ben. «The surveillance industrial complex.» En Routledge handbook of surveillance studies, de Kirstie Ball, David Lyon y Kevin Haggerty. Routledge, 2012.

Martins, Alexandre. «The Colombian Identification System Implementation and technological advancement of the civil identification and registration systems.» Keesing Journal of Documents & Identity, 2013: 25-28.

Migración Colombia. «Comunicado Oficial Biomig.» <http://migracioncolombia.gov.co/index.php/es/prensa/comunicados/comunicados-2018/febrero-2018/6539-en-menos-de-25-segundos-y-con-solo-una-mirada-los-colombianos-podran-ingresar-al-pais-migracion-colombia>, 2018.

Migración Colombia. «Contrato número 117 de 2017 con la Unión Temporal de Control Fronterizo INCOMELEC-GEMALTO.» 2017.

Ministerio de Gobierno de Colombia. “Decreto 944 de 1934”, 1934.

Ministerio de Gobierno de Colombia. “Decreto 2628 de 1951”, 1951.

Ministerio de las Tecnologías de la Información y las Comunicaciones. Carpeta Personal: sus documentos en un solo lugar. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones, 2014.

Ministerio de las Tecnologías de la Información y las Comunicaciones. “Decreto 1413 de 2017”, 2017.

Ministerio de las Tecnologías de la Información y las Comunicaciones. Estudio del Sector para Servicios Ciudadanos Digitales. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones, 2018.

Oficina de Asesoría Jurídica de Migración Colombia. «Memorando Concepto Jurídico: Autenticación biométrica.» 2017.

Oficina de Telemática de la Policía Nacional. «Estudios previos para Contrato de Compraventa 06-7-10081-16: Sistema de Biometría Móvil.» <https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=16-1-157976>, 2016.

Policía Nacional de Colombia. «Estudios previos para la adquisición, instalación, implementación, prueba, puesta en servicio, garantía, soporte y mantenimiento de un sistema biométrico facial, palmar y dactilar.» Bogotá, 2017.

Policía Nacional de Colombia. «Prórroga No. 1 al contrato de compraventa No. 203-1-2017.» Bogotá, 2017.

Policía Nacional de Colombia. «Prórroga No. 3 al contrato de compraventa No. 203-1-2017.» Bogotá, 2017.

Policía Nacional de Colombia. «Prórroga No. 5 al contrato de compraventa No. 203-1-2017.» Bogotá, 2018.

Policía Nacional. «Proyecto autenticación biométrica Policía Nacional.» 19 de Junio de 2018: <https://www.policia.gov.co/noticia/proyecto-autenticacion-biometrica-policia-nacional>.

Presidencia de la República de Colombia, “Decreto 1260 de 1970”, 1970.

Presidencia de la República de Colombia, “Decreto 1377 de 2012”, 2012.

Presidencia de Colombia. «Migración Colombia empezó a usar sistema de inmigración de colombianos por medio de reconocimiento del iris.» 25 de Febrero de 2018.

Registraduría Nacional del Estado Civil. Este Domingo los habitantes de Salazar de las Palmas (Norte de Santander) y Belén de los Andaquíes (Caquetá) elegirán sus nuevos alcaldes. <https://www.registraduria.gov.co/ESTE-DOMINGO-LOS-HABITANTES-DE,1563.html>, 2009.

Registraduría Nacional del Estado Civil. “Resolución 3341 de 2013”, 2013.

Registraduría Nacional del Estado Civil. “Resolución 5633 de 2016”, 2016.

Registraduría Nacional del Estado Civil. «Historia de nuestra cédula de ciudadanía.» Nuestra huella - Revista Electrónica Mensual, 2012.

Registraduría Nacional del Estado Civil. «La huella dactilar: la base del sistema de identificación en Colombia.» Nuestra Huella, 2012: [https://www.registraduria.gov.co/rev\\_elec/2012/rev\\_elec\\_noviembre/revista\\_noviembre2012.html#10](https://www.registraduria.gov.co/rev_elec/2012/rev_elec_noviembre/revista_noviembre2012.html#10).

Registraduría Nacional del Estado Civil, “La biometría: método ideal de identificación humana”. Disponible en: <https://www.registraduria.gov.co/La-biometria-metodo-ideal-de.html>

Registraduría Nacional del Estado Civil. «Suplantación de electores: un fraude más recurrente en el mapa de riesgo electoral.» Nuestra Huella, 2009: <https://www.registraduria.gov.co/Edicion-No-34-Ano-V-diciembre-de.html#01>.

Registraduría Nacional del Estado Civil, “La biometría: método ideal de identificación humana”. Disponible en: <https://www.registraduria.gov.co/La-biometria-metodo-ideal-de.html>

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Resolución N. 58969 de 2014”, disponible en: [http://www.sic.gov.co/sites/default/files/files/Res%20No\\_%2058969%20de%202014%20-%20BANCO%20CELULAS%20MADRE.pdf](http://www.sic.gov.co/sites/default/files/files/Res%20No_%2058969%20de%202014%20-%20BANCO%20CELULAS%20MADRE.pdf)  
[Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Consulta N. 13-2733515 de 2014”, 2014.](http://www.sic.gov.co/sites/default/files/files/Superintendencia_de_Industria_y_Comercio,_Delegatura_para_la_Proteccion_de_Datos._%20Consulta_N._13-2733515_de_2014%20-%20.pdf)

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Concepto C-2014-273515”, 2014.

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Resolución N. 39298 de 2016”, disponible en: [http://www.sic.gov.co/sites/default/files/files/Res%20No\\_%2039298%20del%202016%20-%20COLMEDICA.pdf](http://www.sic.gov.co/sites/default/files/files/Res%20No_%2039298%20del%202016%20-%20COLMEDICA.pdf)

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Resolución N. 12809 de 2018”, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/RE12809-2018.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE12809-2018.pdf)

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Resolución N. 29407 de 2018”, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/29407-16-234117.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/29407-16-234117.pdf)

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Resolución N. 43530 de 2018”, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/RE43530-2018.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE43530-2018.pdf)

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Resolución N. 55405 de 2018”, disponible en: [http://www.sic.gov.co/sites/default/files/files/Proteccion\\_Datos/actos\\_administrativos/2018055405.pdf](http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2018055405.pdf)

Superintendencia de Industria y Comercio, Delegatura para la Protección de Datos. “Concepto C-2018-299565”, 2018.

Superintendencia de Industria y Comercio, Oficina Jurídica. “Consulta N. 297406 de 2018”, 2018.



# BIOMETRÍA

en el Estado colombiano

*¿Cuándo y cómo se ha justificado su uso?*

Por:

Fundación

**Karisma**

Investigación:

Juan Diego Castañeda

Joan López

Lucía Camacho

[karisma.org.co](http://karisma.org.co)

**Twitter:** @Karisma

**Facebook:** @fundacionkarismaa

**Instagram:** @karismacol