20 años

BIOMETRÍA, DATOS PERSONALES Y MIGRACIÓN EN COLOMBIA

Una guía para organizaciones que trabajan con **población migrante** venezolana en Colombia

BIOMETRÍA, DATOS PERSONALES Y MIGRACIÓN EN COLOMBIA

Una guía para organizaciones que trabajan con población migrante venezolana en Colombia

Investigación: Juliana Valdés
Juan Diego Castañeda,
Joan Lopez
Juan de Brigard

Autores: Juliana Valdés
Juan de Brigard

Revisión:

Coordinación: Juan de Brigard

Diseño: Daniela Moreno

Con la colaboración de DeJusticia, Centro de Estudios de Derecho, Justicia y Sociedad y la Corporación Opción Legal.

Queremos agradecer a las organizaciones de sociedad civil que trabajan con población migrante y participaron de los talleres sobre biometría y seguridad digital organizados en 2022, en Bogotá y Medellín por la Fundación Karisma. Sus aportes hicieron posible esta investigación.

Bogotá, Agosto de 2023
Fundación Karisma

En un esfuerzo para que todas las personas tengan acceso al conocimiento, la 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 pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos.
Más información sobre el tema:
http://www.documentoaccesible.com/#que-es.

@Karisma karismacol fundacionkarismaa

karisma.org.co

CONTENIDO

INTRODUCCIÓN

Colombia no es un país acostumbrado a grandes flujos migratorios que traigan gente a su territorio. Por el contrario, a lo largo de nuestra historia la migración ha ocurrido en la dirección opuesta, con una gran diáspora de personas colombianas que han emigrado a Estados Unidos, Chile, España o Canadá. Sin embargo, el país que más colombianos ha recibido a lo largo de la historia es de lejos Venezuela, donde para 2020 se calculaba que residían más de dos millones de colombianos.[1] Recientemete, por razones políticas, económicas y sociales, el movimiento se ha invertido y un gran número de personas venezolanas han llegado a Colombia con la esperanza de hacer una nueva vida en el país o simplemente de pasar por este territorio hacia otros rumbos.

Ante esta situación, que sin duda alguna para muchas personas ha implicado inmensos retos y un gran sufrimiento humano, el gobierno colombiano ha desplegado programas y políticas que pretenden atender las necesidades de las personas que llegan, así como dar orden al proceso de movilidad humana. Podría pensarse que en este contexto profundamente marcado por vicisitudes humanas como familias separadas e intensas necesidades económicas, prestar atención a los datos personales de las personas que migran es enfocar mal los esfuerzos y concentrarse en futilidades. Pero lo cierto es que los datos, su recolección y su tratamiento están a la base de las políticas que –en muchos casos– determinan las posibilidades y la atención o inatención de las necesidades de las personas venezolanas en Colombia.

Es por esta razón que desde la Fundación Karisma hemos hecho un esfuerzo por comprender el rol que juega la identificación biométrica y, en general, la recolección y el tratamiento de datos en el proceso migratorio. Esta práctica estatal, por ocurrir en este contexto y sobre una población particularmente vulnerable, es dificil de supervisar y controlar desde la sociedad civil, pero sin duda tiene implicaciones

1. Cancillería de Colombia y Dirección de Asuntos Migratorios, Consulares y Servicio al Ciudadano, «Estudio de Caracterización de los Usuarios que atiende cada uno de los consulados de Colombia en el Exterior», noviembre de 2020.

directas para la garantía de los derechos humanos de un segmento poblacional muy grande. Personas, además, que por su condición de vulnerabilidad y apremiante necesidad de regularizar su situación jurídica, en la práctica no pueden rehusar el consentimiento cuando sus datos les son solicitados.

Las narrativas que –desde el Estado, los medios y las compaías de tecnología– se usan para justificar el gran esfuerzo institucional por recaudar datos de la población que llega desde venezuela a colombia son principalmente dos.

La primera de ellas sostiene que la recolección masiva de estos datos es indispensable para la formulación de políticas públicas adecuadas a las necesidades de las personas que arriban a Colombia. Y aunque es claro que es más fácil formular mejores políticas con mejor información, esto –sin embargo– no explica por qué razón sería necesario hacer un registro biométrico de la polución proveniente de venezuela, mucho menos uno más exhaustivo que el exigido por el Estado a la ciudadanía colombiana.

La segunda narrativa, más presente en algunos medios[2], en los discursos de las empresas de tecnología[3] y en la literatura académica[4] que en las posturas oficiales, establece un vinculo entre los datos biométricos y la presunta capacidad del Estado para vigilar, perseguir y castigar delincuentes. Aunque ciertamente el discurso de seguridad no está expresado de manera explícita por las autoridades que diseñan estas políticas y tienen como tarea recoger los datos, las justificaciones que se esgrimen para recoger los biométricos de los migrantes hacen agua frente a un simple test de necesidad o proporcionalidad: si las huellas dactilares son una tecnología más confiable que el reconocimiento facial para garantizar la identidad, ¿para qué necesitamos datos biométricos faciales de las personas que migran?

Así pues, este documento pretende ser un llamado a las organizaciones que trabajan con población migrante para preguntarse qué rol cumple la recolección de datos dentro del proceso migratorio como un todo, cómo funciona técnicamente el proceso, qué experiencias internacionales pueden compararse al caso colombiano en este sentido, cuáles son las regulaciones que rigen estas prácticas y, finalmente, cuáles son los

2. David Jojoa, «Así funciona las cámaras de reconocimiento facial que se instalarán en Bucaramanga • ENTER.CO», ENTER.CO (blog), 8 de julio de 2022, https://www.enter.co/empresas/colombia-digital/asi-funciona-las-camaras-de-reconocimiento-facial-que-se-instalaran-en-bucaramanga/; El Espectador, «Los retos del reconocimiento facial que se usa para garantizar la seguridad», El Espectador, 5 de julio de 2022, sec. Más regiones, https://www.elespectador.com/colombia/mas-regiones/los-retos-del-reconocimiento-facial-en-la-seguridad/.

3. Olimpia IT, «En menos de 15 segundos ahora es posible identificar un rostro en Colombia mediante biometría», Olimpia IT, 26 de agosto de 2021, https://olimpiait.com/tecnologia/en-menos-de-15-segundos-ahora-es-posible-identificar-un-rostro-en-colombia-mediante-biometria/.

4. María Lorena Flórez Rojas et al., «Tecnologías de reconocimiento facial en Colombia: Análisis comparativo en relación con la protección de datos», Ius et Praxis 29, n.o 1 (marzo de 2023): 3-26, https://doi.org/10.4067/S0718-00122023000100003; Isadora Neroni Rezende, «Facial Recognition in Police Hands: Assessing the 'Clearview Case' from a European Perspective», New Journal of European Criminal Law 11, n.o 3 (septiembre de 2020): 375-89, https://doi.org/10.1177/2032284420948161.

principios que deberían respetar los sistemas de datos. Además de eso, ofrecemos a modo de anexo una breve explicación de qué son y por qué son importantes los formatos de consentimiento informado y las políticas de tratamiento de datos, así como una explicación breve de qué es y cómo puede usarse la acción de tutela. Comprender estos temas y herramientas e incorporarlos en las agendas de las organizacione que trabajan con población migrante es la única manera de avanzar con una estrategia mancomunada que conduzca a la adopción de mejores prácticas en la recolección y el tratamiento de datos que son necesarios para mejorar las condiciones de estas personas, pero que deben estar suficientemente regulados como para no aumentar su exposición o vulnerabilidad.

Por último, es importante mencionar que las prácticas de datificación identificadas durante esta investigación son un primer paso necesario para el establecimiento de una política regional de vigilancia y securitización, por lo que es importante tener presente también ese horizonte. Solo así será posible garantizar que no se abuse de los datos recogidos y que las desigualdades estructurales que aquejan a la población que migra no se agraven más con el uso de la tecnología.

1. BIOMETRÍA ¿Y ESO QUÉ ES?

1.1 ¿A qué nos referimos cuando hablamos de biometría?

La biometría es la recolección, análisis y procesamiento de una serie de características que se consideran únicas para cada persona y que pueden ser biológicas, como el rostro, las huellas dactilares, el iris o el ADN, o comportamentales, como la voz, los gestos o la forma en que se mueve el cuerpo[5], entre otras. Dichas características pueden utilizarse para identificar o verificar la identidad de las personas.[6] Cuando la biometría se usa para identificar estamos usando esas características personales para responder a la pregunta de quién es alguien. En este proceso, se lleva a cabo una comparación 1:N, es decir, se compara la información de un individuo (por ejemplo su rostro) con varios o todos los registros que se tienen almacenados en una base de datos (todos los rostros registrados) para encontrar una coincidencia que permita responder la pregunta ¿quién es esa persona desconocida?.[7] Esto se da, por ejemplo, en el marco de investigaciones policiales. Por otro lado, si se utiliza para verificar la identidad lo que se busca es indagar si la persona es quien dice ser. En este proceso, se hace una comparación 1:1, en la que se compara la información recogida (por ejemplo una huella dactilar) con el registro específico almacenado en una base de datos bajo el mismo nombre para ver si ambos coinciden. Aquí se busca responder a la pregunta ¿es esta persona quien dice ser?[8]. Este procedimiento se da, por ejemplo, en la acción cotidiana de desbloquear nuestros teléfonos celulares con el rostro o la huella.

El uso de tecnologías biométricas es cada vez más popular, pues permite ligar rápidamente la identidad de una persona a un cuerpo o una característica específica y almacenarla en una base de datos

5. Btihaj Ajana, Governing through biometrics: The biopolitics of identity (Springer, 2013); Alexander S. Gillis, Peter Loshin, y Michael Cobb, «What is biometrics?», TechTarget, s. f., https://www.techtarget.com/searchsecurity/definition/biometrics.

6. David Leslie, «Understanding bias in facial recognition technologies An explainer», (The Alan Turing Institute, 2020).

7. Gillis, Loshin, y Cobb, «What is biometrics?»

8. Gillis, Loshin, y Cobb.

para utilizarla posteriormente en distintos contextos en que es necesario identificar o autenticar la identidad[9]. Así mismo, su uso se ha expandido debido a la idea de que es una tecnología más precisa, más "objetiva", menos susceptible a errar y que basa la identificación en características que son difíciles de modificar o falsificar.[10]

1.1.2 ¿Cómo funciona la biometría?

La biometría funciona en cuatro pasos[11] que se presentan en la mayoría de los sistemas de identidad.

1. Registro

En esta etapa se recolectan las características de la persona que se consideran únicas a través de una serie de sensores, o medios análogos o digitales. Por ejemplo, se toman impresiones de la huella dactilar, fotos del rostro o del iris, se le pide a la persona que firme repetidamente una planilla. Este dato que se recolecta se convertirá en una imagen de consulta.

Una vez se tienen estas imagenes de consulta, a través de un procedimiento algorítmico estas se convierten en una plantilla biométrica, es decir, en una representación digital, numérica y abstracta de esa característica que se recolectó.[12]

2. Almacenamiento

Posteriormente, esta plantilla que se ha elaborado se almacena en una base de datos. Las bases de datos son un conjunto de registros que se almacenan para su posterior uso. En el caso de la biometría, dependiendo de si es facial, dactilar, comportamental o combina varios tipos, este conjunto de información se verá de manera diferente.

Por ejemplo, mientras que en la biometría facial la base de datos tiene que ser de huellas faciales (o patrones de rostro), en la dactilar debe ser de patrones de la huella. Incluso, podemos tener bases de datos que almacenan ambos tipos de datos.

En el almacenamiento, cada registro biométrico está asociado a un nombre y, con mucha frecuencia, a otros datos como un número de identificación

9. Ajana, Governing through biometrics: The biopolitics of identity.

10. David Lyon, Identifying citizens: ID cards as surveillance (Polity, 2009).

11. Ajana, Governing through biometrics: The biopolitics of identity.

12. Danny Thakkar, «What is a biometric template? Is it secure?», s. f., https://www.bayometric.com/biometric-template-security/.

(como la cédula), la fecha de nacimiento, la nacionalidad, la dirección de residencia o el número de teléfono, entre otros. Así quien realiza la autenticación o la identificación tiene más información sobre el individuo.

3. Adquisición

Este paso se realiza cuando una persona quiere acceder a un bien o un servicio y es necesario verificar o conocer su identidad para ello.

Aquí se toman nuevamente los datos biométricos de la persona a través de un sensor u otros medios tecnológicos. Inmediatamente, este dato se transforma en una representación numérica mediante el mismo proceso algorítmico que se utilizó durante el registro y se crea una "plantilla viva" que es comparable con el registro guardado en la base de datos.

4. Comparación

En la comparación es donde puntualmente se realizan los procesos de identificación o de verificación. Pueden ser de dos tipos:

1. Verificación/Autenticación de la identidad: la "plantilla viva" se compara con una plantilla específica en la base de datos para ver si ambas coinciden. (Comparación 1:1)

2. Identificación: la "plantilla viva" se compara con todas las plantillas que se tienen almacenadas en la base de datos para ver con cuál o cuáles coincide. (comparación 1:N)

1.1.3 ¿Para qué se usa la biometría en la actualidad?

En el mundo la biometría se utiliza para la venta de productos, la detección del crimen y el delito, el control de entrada a establecimientos e incluso para el manejo de celulares y otros equipos. Por ejemplo, es frecuente que los bancos nos exijan un registro de las huellas digitales para abrir una cuenta y que nos obliguen a autenticar nuestra identidad al retirar dinero o que nuestros teléfonos se puedan desbloquear con la huella o con el rostro. En todos estos casos, las entidades, las empresas o los equipos –según corresponda– están verificando que usted sea quien dice ser o están buscando determinar quién es usted.

Siendo más precisos, sin embargo, uno de los fines más comunes de este proceso en la actualidad es el de establecer la identidad legal de alguien y determinar si esta persona tiene o no acceso a una serie de bienes y servicios que proveen los Estados.

La identidad legal es un derecho fundamental humano que se refiere justamente al reconocimiento de las personas como sujetos de derechos y deberes frente a un Estado específico.[13] Algunos ejemplos son los procesos electorales en que es necesario autenticar la identidad mediante la huella o, como veremos más adelante, los procesos migratorios.

Para poder establecer la identidad de alguien y utilizarla para transacciones es necesario pasar por una serie de pasos que han sido llamados el "ciclo de la identidad". Estos son análogos a los cuatro que vimos anteriormente, pero más generales, pues ya no se refieren específicamente a la biometría sino a la identidad en general. El ciclo está compuesto –como se ve en la imágen 1– por[14]:

Imágen 1: ciclo de vida de la identidad[15]

13. Banco Mundial e Identificación para el desarrollo, «ID4D Practitioner's Guide» (World Bank Group, 2019).

14. Basado en: Banco Mundial y Identificación para el desarrollo; Banco Mundial, «Catalog of Technical Standards for Digital Identification Systems», 2018, https://id4d.worldbank.org/technical-standards#:~:text=Catalog%20of%20Technical%20Standards%20for%20Digital%20Identification%20Systems&text=Standards%20are%20critical%20for%20identification,identity%20lifecycle%20for%20technical%20interoperability.; Banco Mundial, «Technology Landscape for Digital Identification», 2018, https://openknowledge.worldbank.org/handle/10986/31825; Fundación Karisma, «Conceptos básicos de los sistemas de identidad», Digital ID Colombia, 7 de diciembre de 2021 https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id/.

15. Fundación Karisma, «Conceptos básicos de los sistemas de identidad».

1. La producción de la identidad. Esto ocurre en dos momentos. Primero, durante el registro cuando una persona ofrece una serie de atributos para reclamar una identidad específica a la autoridad que administra el sistema de identidad. Por ejemplo, al registrar los datos de un bebé en una partida de nacimiento. Segundo, cuando estos datos son validados frente a otras fuentes de información disponibles y almacenados en bases de datos. Por ejemplo, al cumplir la mayoría de edad y actualizar el documento de identidad, se contrasta la información y se almacena en una nueva base.

2. La emisión de las credenciales. En este proceso se crean elementos que permitan autenticar esa identidad que se creó con el registro. Estos pueden ser algo que la persona tiene (por ejemplo, el documento nacional de identificación, físico o digital), algo que la persona sabe (la clave única con la que se accede al banco) o algo que la persona es o hace (los datos biométricos como las huellas, ojos, o rostros o comportamentales como la manera en que firma o sus gestos).

3. El uso de credenciales. Es aquí cuando esa identidad que se creó en el registro y que está siendo autenticada por un mecanismo específico (por ejemplo, presentando la tarjeta, poniendo la clave o demostrando la característica física o comportamental) se utiliza y es validada en un punto de transacción para verificar la identidad y acceder a un servicio.

4. La administración del sistema. Esta etapa alude al almacenamiento de la información en una base de datos y el mantenimiento de este sistema en sentido tecnológico y financiero.

En los sistemas de identificación que hacen uso de la biometría, esta se encuentra presente en todos los momentos del ciclo de la identidad. Particularmente, porque son los atributos biológicos como las huellas, el rostro o el iris los que brindamos al momento del registro, los que quedan impresos o registrados en las credenciales, los que utilizamos para validar nuestra identidad al momento de realizar trámites, y los que quedan almacenados en las bases de datos de las entidades en las cuales los adelantamos.

Para comprenderlo revisemos el ejemplo concreto del pasaporte: para su expedición no solo se entregan datos personales (nombre, edad, fecha de nacimiento, tipo de sangre, estatura, etc.), sino que también se registran las huellas dactilares de los diez dedos de la mano, se entrega una fotografía y se firma uno (o varios) formularios. Una vez se validan estos datos, se crea una credencial física que permite a la persona autenticar su identidad: el pasaporte. Este pasaporte se le pedirá a la persona en los puestos de control fronterizo y el funcionario verificará que es quien dice ser tomando sus huellas digitales y comparando su rostro con la foto. Después dirá si está o no autorizada para

salir o entrar al territorio y si puede avanzar en su viaje. Todo este proceso es posible porque la información se encuentra almacenada en bases de datos que se mantienen y se actualizan a lo largo del tiempo.

1.1.4 ¿Qué sabrían sobre mí? ¿Qué tipo de información recolectan?

El tipo de información que se recolecta depende ampliamente del fin que se persigue y de las especificaciones del software biométrico que se ponga en funcionamiento para lograrlo. En el proceso de producción de identidad se puede recolectar información de dos tipos: biométrica y biográfica.

Cuando se recolectan datos biométricos estos pueden ser, a su vez, de dos tipos: biológicos o comportamentales. Como mencionamos más atrás, la primera se basa en la recolección de características biológicas únicas a cada persona, que persisten a lo largo del tiempo y permiten distinguirla de las demás y así identificarla o verificar su identidad. Algunos de los identificadores fisiológicos que se recolectan son:[16]

- Las huellas dactilares de las manos
- Facciones de la cara
- Posición relativa de los ojos en la cara
- Patrones del iris
- La sangre
- La voz
- El ADN

En el caso de la biometría comportamental se busca la recolección de patrones únicos de comportamiento que permitan determinar la identidad, los gustos, preferencias de una persona o favorecer formas de autenticación. Algunos de los datos que se pueden recolectar son:[17]

- La firma
- Patrones de tecleo
- La presión que se ejerce sobre el teclado al momento de escribir
- La forma en que se deslizan los dedos por el teléfono móvil
- Formas de caminar
- Expresiones faciales

16. Gillis, Loshin, y Cobb, «What is biometrics?»

17. One Span, «Biometría conductual», One Span The digital Agreements Company, s. f., https://www.onespan.com/es/topics/biometria-conductual.

Cuando se recolectan datos biográficos, los mínimo que se solicita suele ser:

- Los nombres y apellidos de la persona que entrega sus datos
- La fecha de nacimiento y/o su edad
- El sexo
- El tipo de sangre
- La estatura

Sin embargo esta lista no es exhaustiva y la recolección de información puede incluir muchos más campos, por ejemplo, el cuestionario del RUMV solicita también información del tamaño del grupo familiar e incluso de salud. Aquí es muy importante tener en cuenta que la información biográfica que se recolecta en el marco de un proceso de creación de identidad con datos biométricos queda vinculada con el dato biométrico mismo, de manera que quien acceda al registro a través del dato biométrico normalmente podrá ver también toda la información asociada a ese registro. Es decir, cuando entregamos, por ejemplo, nuestra huella, estamos ofreciendo junto con ella mínimo nuestro nombre y número de identificación, pero usualmente también toda la información biográfica que entregamos durante el proceso de producción de identidad.

1.1.5 ¿Para qué se usará esta información? ¿cómo la usarían?

Para responder esta pregunta es fundamental recalcar nuevamente que el tipo de información que se recolecta depende de los fines para los cuales se implemente el sistema biométrico. Los usos que se le ha dado a esta tecnología varían desde la seguridad, la identificación y la prevención del crimen, hasta –en el caso de la biometría comportamental– la venta de productos publicitarios específicos o la autenticación continua durante el uso de un servicio, por ejemplo, mientras el usuario permanece en la página de un banco.[18] A continuación presentamos algunos ejemplos de estos usos por parte de públicos y privados.

"Ahora con la cámara de su celular puede acceder a su documento": biometría facial en la cédula digital colombiana

La Registraduría Nacional del Estado Civil en Colombia ha desarrollado múltiples proyectos para aumentar la tecnificación de los sistemas de identificación en el país desde hace más de 50 años. Sin embargo, a finales de 2020, la entidad firmó un contrato con la multinacional IDEMIA para la implementación de una nueva cédula de ciudadanía digital. Con esto, se creó una nueva versión de la cédula física impresa en

18. One Span.

policarbonato “y una versión digital por medio de una modificación a la aplicación de reimpresión de cédulas disponible para Android y IOS que autenticaba la identidad de la persona usando reconocimiento facial en el dispositivo”.[19]

También, a través de este contrato se buscó desarrollar una plataforma de autenticación facial al servicio de entidades externas. “Este sistema requiere el número de cédula de la persona y una cámara que extraiga los patrones faciales para que una institución externa verifique que el rostro que está siendo detectado corresponda a ese número de cédula.”[20] Es decir, la registraduría busca con esto ofrecer a clientes privados el servicio de autenticación de la identidad con reconocimiento facial usando nuestros datos.

“Un momento jóven, me permite su cédula y su huella”: la utilización de biometría para el control del crimen y el delito

Uno de los sistemas que utiliza la policía en Colombia es el sistema biométrico Appolo desarrollado por la compañía Olimpia. Este sistema que fue implementando en el año 2016, permite a los miembros de la Policía Nacional autenticar la identidad de una persona y cotejar mediante su huella digital si esta tiene o no órdenes de captura a nivel nacional o internacional vigentes.[21] Appolo funciona a través de una comparación entre las huellas o la información alojada en el código de barras de la cédula de ciudadanía, con los datos que reposan en las bases de datos de la Registraduría Nacional del Estado Civil.[22] Su funcionamiento es posible gracias a un convenio entre estas dos entidades del Estado.

Las razones para la implementación de Appolo, según la Policía Nacional, obedecieron a que la autenticación biométrica permitía verificar la identidad de las personas y así tomar decisiones mucho más acertadas para la detención del crimen y el delito, y reforzar la seguridad nacional. También argumentaron que era una forma de luchar contra la suplantación y la falsificación de documentos en el país.[23]

19. Fundación Karisma, «El sistema de reconocimiento facial de la Registraduría Nacional», 1 de julio de 2021, https://digitalid.karisma.org.co/2021/07/01/sistema-reconocimiento-facial-registraduria/.

20. Fundación Karisma.

21. “Proyecto Autenticación Biométrica Policía Nacional," Policía Nacional de Colombia, June 19, 2018, https://www.policia.gov.co/noticia/proyecto-autenticacion-biometrica-policia-nacional.

22. Juan Castañeda, Joan López Solano, y Lucía Camacho, Biometría en el Estado colombiano ¿Cuándo y cómo se ha justificado su uso?, 2019, https://doi.org/10.13140/RG.2.2.21018.08646.

23. Juan Castañeda, Joan López, y Lucía Camacho, Biometría en el Estado colombiano ¿Cuándo y cómo se ha justificado su uso?, 2019, https://doi.org/10.13140/RG.2.2.21018.08646.

¿Cómo te está yendo en las clases? Reconocimiento facial y comportamental en algunas escuelas en China

Desde hace varios años el gobierno chino ha apostado por la modernización tecnológica del Estado y de su relación con los ciudadanos en diversas esferas. En este proceso, en el año 2018 una escuela en Hangzhou recibió bastante atención internacional al conocerse el hecho de que estaba utilizando biometría facial y comportamental al interior de sus instalaciones.

En un primer momento la biometría de reconocimiento facial se utilizó para autorizar la entrada de estudiantes al plantel educativo, pagar el almuerzo y solicitar libros de la biblioteca.[24] Mientras tanto, la biometría comportamental, a través de cámaras se escaneaba permanentemente los gestos y las emociones expresadas en el rostro y los movimientos de los estudiantes. El análisis de estos datos se usó para que, según lo que arrojara el software, los maestros supervisaran el desempeño de sus alumnos.[25]

1.1.6 ¿Los sistemas biométricos se equivocan?

Ninguno de estos usos, sin embargo, está exento de polémica. En los casos colombianos, la incorporación de biometría facial en la cédula se ha dado sin que haya una discusión democrática al respecto y el uso del sistema APPOLO por parte de la Policía Nacional confiere a la entidad unas facultades de vigilancia masiva que no necesariamente son deseables. Por su parte, el uso en el contexto de los colegios en China ha levantado múltiples voces de protesta que se cuestionan sobre los riesgos a la privacidad y la vigilancia permanente que implican estos sistemas sobre la vida cotidiana de los estudiantes. Se cuestionan si estos datos debería o no tenerlos una escuela y las implicaciones que esta hipervigilancia puede tener sobre lo derechos humanos de los estudiantes.[26] Así mismo, no es claro que un sistema automatizado de reconocimiento facial gestual sea capaz de inferir, adecuadamente y sin errores, variables asociadas al desempeño escolar de los niños.

24. Tara Francis Chan, «A school in China is monitoring students with facial-recognition technology that scans the classroom every 30 seconds», Insider, 20 de mayo de 2018 https://www.businessinsider.com/china-school-facial-recognition-technology-2018-5.

25. CRI, «Facial recognition used to analyze students' classroom behaviors», en.people.cn, 19 de mayo de 2018, http://en.people.cn/n3/2018/0519/c90000-9461918.html.

26. «What is facial recognition - and how sinister is it? | Biometrics | The Guardian», accedido 12 de julio de 2023, https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it.

En términos generales, la identificación a través de la biometría, al igual que cualquier otro procedimiento, tiene la posibilidad de fallar pues no solo depende del cuerpo de las personas que va cambiando de manera constante, sino también de las personas que programan los algoritmos, desarrollan los sensores y operan las máquinas, de las máquinas mismas, así como de las condiciones ambientales en las que operan. En la literatura internacional se han encontrado varias **fallas de los sistemas de identificación biométricos. Las fallas de estos sistemas a nivel técnico general** son:

1. El sistema tiene una posibilidad de falsos positivos (le adjudica una identidad que no le corresponde a una persona) y falsos negativos (niega su identidad al individuo, aunque esta sí le corresponda). Esto se debe a que los sistemas de autenticación biométrica se basan en probabilidades.[27] Por ejemplo, es frecuente que un software de reconocimiento facial "se confunda" entre dos personas gemelas, o incluso entre madres e hijas o padres e hijos, pues el porcentaje de probabilidad de que el software reconozca los mismos rasgos en dos personas distintas pero fisiológicamente parecidas es alto. Para convencerse de esto, basta con ver ejemplos de cómo –con frecuencia– parientes cercanos pueden desbloquear los teléfonos de unos y otros con su rostro. Además, a quienes desarrollan los softwares no les conviene hacerlos excesivamente restrictivos porque, si lo fueran, un simple cambio en el ángulo de la cara o en la posición de la huella sobre el lector podría evitar que el software encuentre una coincidencia. Es decir: el equilibrio entre evitar falsos negativos y evitar falsos positivos es demasiado estrecho y deja lugar a error.

2. Algunos sistemas biométricos no evitan la suplantación al 100%, existen muestras de que con reproductores de huellas o máscaras -en el caso de la biometría facial- estos pueden ser burlados.[28]

3. Existen una serie de comunidades que no pueden ser identificadas a través de estos sistemas debido a sus características corporales, por ejemplo, personas que han sufrido accidentes, parálisis o amputaciones, entre otras.[29] Esto implica que los sistemas biométricos también puedan ser un factor de exclusión social para dichos grupos.

4. Además de lo anterior están las vulnerabilidades de seguridad digital: en primer lugar los datos biométricos están almacenados en una base de datos cuya seguridad depende de quien la custodie, pero nunca es infalible. Ya se han presentado casos en que las bases de datos biométricas son vulneradas y los datos quedan expuestos.[30]

27. AEPD, «14 equívocos con relación a la identificación y autenticación biométrica», 2020, https://www.aepd.es/sites/default/files/2020-06/nota-equivocos-biometria.pdf.

28. AEPD.

29. AEPD.

30. "Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms," The Guardian (Guardian News and Media, August 14, 2019), https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

En segundo lugar, dado que los lectores deben conectarse a una base de datos que, con frecuencia, es remota, la capacidad del sistema de autenticar la identidad de las personas depende de la fiabilidad de la conexión. Si hay errores de conexión, como sucedió por ejemplo durante las elecciones de 2022, la autenticación se hace imposible.

Las fallas que se han encontrado alrededor de los **sistemas biométricos dactilares** son:

1. Es frecuente que haya fallas en la identificación de las personas como consecuencia de la imposibilidad de leer las huellas dactilares. Las causas son diversas. Por ejemplo, los trabajos manuales pueden comprometer las huellas dactilares[31], haciendo que personas campesinas, artesanas u obreras, entre otras, usualmente tengan más dificultad para utilizar estos servicios de identificación. El mismo fenómeno se puede dar por condiciones médicas subyacentes como la dermatitis[32] o –como se vió en el caso de Eurodac– por el daño intencional y premeditado de las huellas por parte de las personas con la intención de evitar ser identificadas por este medio.[33]

2. En el caso de los sistemas biométricos dactilares, el potencial de falsos positivos o negativos depende de elementos como la luminosidad de los sensores, la precisión para la captura de datos y su limpieza, entre otros.[34]

Las fallas encontradas alrededor de los **sistemas biométricos faciales[35]** son:

1. Los algoritmos de biometría se entrenan usando grandes bases de datos de referencia para que el sistema "aprenda" a reconocer distintos patrones, en el caso de la biometría facial, se usan los rostros de muchas personas. Sin embargo, dado que con frecuencia estos sistemas han sido desarrollados en el norte global, la

31. Vindu Goel, «"'Big Brother' in India Requires Fingerprint Scans for Food, Phones and Finances."», The New York Times, 7 de abril de 2018, https://www.nytimes.com/2018/04/07/technology/india-id-aadhaar.html.

32. Martin Drahansky et al., «Influence of Skin Diseases on Fingerprint Recognition», BioMed Research International 2012 (2012), https://www.hindawi.com/journals/bmri/2012/626148/.

33. Chloe Lyneham, «EU's migrant fingerprinting system Eurodac under review», DW, 9 de noviembre de 2017, https://www.dw.com/en/eus-migrant-fingerprinting-system-eurodac-under-review/a-41311572.

34. AEPD, «14 equívocos con relación a la identificación y autenticación biométrica».

35. Para más información sobre estas fallas véase Fundación Karisma, «Qué es y cómo funciona el reconocimiento facial», 1 de julio de 2021, https://digitalid.karisma.org.co/2021/07/01/que-es-reconocimiento-facial/#fn:9.

mayoría de los rostros que se han utilizado son de personas blancas, especialmente hombres.[36] Lo anterior implica que son mucho menos eficientes detectando los rasgos faciales de mujeres y personas racializadas, pues tienen menos entrenamiento y están menos "refinados" para operar con estos grupos. Es decir, son sistemas tecnológicos que reproducen desigualdades estructurales graves como los prejuicios raciales o de género.[37]

2. Como señalamos más arriba, se han abierto múltiples procesos de estudio e investigación por casos en los que estos sistemas de reconocimiento e identificación biométrica han confundido la identidad de gemelos y gemelas o de familiares cercanos.[38]

3. Al igual que con la biometría dactilar, los accidentes o algunas condiciones médicas como la neurofibromatosis, pueden comprometer la capacidad de los sistemas de reconocer rostros diversos. Si el sistema en cuestión exige el reconocimiento facial, esta puede convertirse en una dificultad ineludible para algunas personas usuarias.

Más adelante, en la sección 1.2.2 exploramos algunos riesgos adicionales, ya no desde el punto de vista técnico, sino social.

1.2 ¿Cuál es la relación entre biometría y migración? Un acercamiento a las políticas de seguridad de los Estados

1.2.1 El papel de la biometría en los procesos migratorios

La verificación de la identidad y la vigilancia de los movimientos de las personas para entrar o salir de un país son mecanismos de control migratorio que fueron emergiendo alrededor del mundo con la conformación de los estados nacionales. Su principal objetivo era hacer más visibles para los Estados los movimientos de personas, mercancías y productos que se movían a través de las fronteras que definían su territorio[39]. De manera paralela a estos sistemas de control fronterizo, se comenzaron a desarrollar mecanismos para identificar tanto a quienes hacían parte de la comunidad

36. Simone Browne, Dark Matters: On the Surveillance of Blackness (Duke University Press, 2015), https://doi.org/10.1215/9780822375302.

37. Leslie, «Understanding bias in facial recognition technologies An explainer»,.

38. AEPD, «14 equívocos con relación a la identificación y autenticación biométrica».

39. Huub Dijstelbloem, Albert Meijer, y Michiel Besters, «The Migration Machine», en Migration and the new technological borders of europe (Plagrave: Mcmillan., 2011).

nacional –los ciudadanos–, como a aquellos que no –los extranjeros– en busca de tener una visión mucho más amplia de sus movimientos[40]. Este es el marco en que documentos de identificaciones transnacionales (pasaportes modernos) empezaron a aparecer, después de la primera guerra mundial.[41]

Con el aumento de la globalización y tras la caída del muro de Berlín varios académicos establecieron que nos encontrábamos en un mundo en el que las fronteras nacionales serían cada vez más porosas y el movimiento de personas sería cada vez más libre. Sin embargo, en contraposición a un mayor movimiento de bienes y mercancías entre fronteras, se establecieron controles cada vez más fuertes para el movimiento de personas, específicamente de aquellas provenientes de los países occidentales menos prósperos[42].

Aunque los mecanismos de identificación ya estaban abasteciéndose alrededor del mundo, los acontecimientos del 11 de septiembre de 2001 en los Estados Unidos generaron preocupaciones sobre cómo asegurar la seguridad del Estado y de sus ciudadanos de aquellas personas no ciudadanas cuya presencia en el territorio nacional podría resultar peligrosa o no deseada[43]. Durante esta época comenzaron a desarrollarse diversas narrativas sobre los peligros que podría traer sobre la seguridad de los territorios nacionales el paso de personas, mercancías y movimientos no identificados a través de las fronteras de manera no controladas[44].

En este contexto fue el espacio perfecto para que las compañías tecnológicas presentarán sus diversos avances como un mecanismo para solucionar estos problemas de seguridad que aquejan a los Estados[45]. Una de las soluciones brindadas por estas compañías fue la identificación biométrica. Al estar basada en la captura, análisis y procesamiento de elementos únicos para cada cuerpo, prometía generar una forma de identificación (en principio) poco invasiva, estable, difícil de falsear o de engañar, y que podía ser utilizada en diversos contextos.[46]

40. David Lyon, «Chapter 5: the border is everywhere: ID cards, surveillance and the other», en Global Surveillance and Policing: border, security and identity (Portland, Oregon: William Publishing, 2005).

41. National Geographic. 2017. A History of the Passport. [online] Available at: <https://www.nationalgeographic.com/travel/article/a-history-of-the-passport> [Accessed 23 September 2022].

42. Dijstelbloem, Meijer, y Besters, «The Migration Machine».

43. Lyon, Identifying citizens: ID cards as surveillance.

44. Dijstelbloem, Meijer, y Besters, «The Migration Machine».

45. Lyon, Identifying citizens: ID cards as surveillance.

46. Lyon, «Chapter 5: the border is everywhere: ID cards, surveillance and the other».

La mirada histórica nos permite asociar este fenómeno con formas más antiguas de biometría, como la antropometría criminal o la frenología, pseudociencias de origen europeo que comenzaron a aplicarse en América a comienzos del siglo XX. Estas técnicas, basadas también en la medición corporal, buscaban garantizar el control y la vigilancia de individuos considerados peligrosos o potencialmente peligrosos para la sociedad como enfermos mentales, migrantes o delincuentes.[47] La biometría contemporánea, aunque más sofisticada y tecnificada es, en buena medida, la continuación histórica de estas herramientas de control social.

Por otra parte, aunque la biometría comenzó a implementarse en búsqueda de disminuir las amenazas de seguridad que podrían generarse en estos contextos, es clave señalar que hoy en día también se utiliza desde un enfoque de prevención.[48] En pocas palabras, ya no solo se usa para la detección de un peligro claro, sino también en aras de mitigar una amenaza o situación posible que pueda afectar la seguridad en un sentido amplio.

Esta ampliación de la función de los sistemas de identificación biométrica ha llevado a que cada vez más se desdibuje aquello que se considera un riesgo o aquello que puede afectar la seguridad, al tiempo que se permite ampliar los límites de la recolección de la información, la vigilancia y la intervención sobre la vida de las personas[49]. En ese sentido, la expansión del uso de datos biométricos en contextos migratorios se da en el marco de una masificación de la vigilancia. Así mismo, este sistema pasa a tener un papel protagónico en la definición de la situación jurídica de las personas en un territorio, pues las define y permitir que se las incluya o se las excluya de los bienes y servicios que el Estado ofrece.[50]

1.2.2 La aplicación de la biometría en procesos migratorios: una mirada a algunos ejemplos internacionales

1.2.2.1 El sistema dactiloscópico Europeo (Eurodac)

Uno de los usos de los sistemas de identificación biométrica para procesos migratorios más notorios en el mundo es el sistema de dactiloscopia europea o Eurodac. Eurodac es un sistema de información que se utiliza en toda la Unión Europea desde 2003 para la recolección, análisis y procesamiento de las huellas dactilares de los solicitantes

47. Hering Torres, Max S. 2018. 1892: Un Año Insignificante. Pgs 59-61. Bogotá, Colombia: Universidad Nacional de Colombia.

48. Lyon, Identifying citizens: ID cards as surveillance.

49. Lyon.

50. Dijstelbloem, Meijer, y Besters, «The Migration Machine».

de asilo y ciertas categorías de migrantes irregulares[51]. Así mismo, es uno de los principales mecanismos a través de los cuales se implementa la Regulación de Dublín. Con esta regulación se determina qué Estado miembro de la Unión Europea tendrá la responsabilidad de examinar una solicitud de protección internacional presentada en uno de ellos por un ciudadano de un tercer país[52]. Aunque Eurodac es parte de un sistema migratorio mucho más complejo, su función es clara: facilitar la vigilancia y el rastreo de los movimientos de los solicitantes de asilo y de los migrantes irregulares en la Unión Europea.

Para hacer este proceso posible, la regulación de Eurodac obliga a todos los Estados miembros a recolectar las huellas digitales de toda persona que llegue a la Unión Europea solicitando asilo, que sea mayor de 14 años; al igual que la de todas las personas de terceros países que hayan sido aprendidas en procesos relacionados con cruces fronterizos irregulares o ilegales –sean estos por mar, tierra o aire–[53]. Una vez las huellas son recolectadas a través de un sistema AFIS, estas son transmitidas para su almacenamiento a una base de datos centralizada a la que tienen acceso todos los países miembros y las entidades de policía.

La centralización de esta información funciona de la siguiente manera. Supongamos que una persona está solicitando asilo o es encontrada cruzando de manera irregular en Grecia, cuando se tomen sus huellas dactilares se revisará contra esa base de datos central. En este punto, el agente migratorio revisa si las huellas de esta persona ya se encuentran registradas en la base de datos y a qué responde esta situación, es decir, si la persona había ya realizado una solicitud internacional de protección en otro país de la Unión Europea o si había sido detenido intentando ingresar de manera irregular a alguno de estos países.

En caso de que sus datos no se encuentren, sus huellas digitales son recolectadas y almacenadas en el sistema. Sin embargo, si se encuentra una coincidencia en el sistema se pueden presentar dos situaciones. Si la persona ya había solicitado asilo en otro país, se le negará la entrada en Grecia y se conducirá su caso al otro país para que se adelante la solicitud pertinente –en caso de que esta no haya sido previamente

51. Niovi Vavoula, «Transforming Eurodac from 2016 to the New Pact: From the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration», 2021, https://www.ecre.org/wp-content/uploads/2021/01/ECRE-Working-Paper-Transforming-Eurodac-from-2016-to-the-New-Pact-January-2021.pdf.

52. ACNUR, «El Reglamento de Dublín: asilo en Europa ahora está en tus manos», 2010 https://www.acnur.org/fileadmin/Documentos/Publicaciones/2010/7364.pdf.

53. Vavoula, «Transforming Eurodac from 2016 to the New Pact: From the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration».

denegada–. Por otro lado, si la persona ya había sido sorprendida cruzando de manera irregular la frontera, se negará su entrada y se aplicará la sanción correspondiente.

¿Cuáles son los riesgos en materia de derechos humanos asociados a la implementación de Eurodac?

Los problemas asociados con Eurodac podrían dividirse en dos grandes grupos. En el primer grupo se encuentran las situaciones problemáticas relacionadas con el proceso de recolección de las huellas digitales de las personas que migran a Europa. En este grupo se ven casos en donde se denuncia:

1. Hay una recolección excesiva de datos de la población que solicita asilo o que ha sido encontrada en condición irregular en las fronteras europeas que no se aplica a ningún otro tipo de migrante.[54]

2. Se le brinda la posibilidad a las autoridades de policía de descargar y acceder a estas bases de datos a discreción, sin un control o una razón específica. Según organizaciones defensoras de derechos humanos, esto lleva a una asimilación de esta población con la criminalidad y el delito, al permitir una vigilancia constante y no justificada sobre personas solicitantes de asilo o que han sido encontradas migrando en condiciones irregulares.[55]

3. Se han evidenciado casos y procedimientos que niegan la posibilidad de las personas solicitantes de asilo o que migraron en condición irregular de negar la recolección de sus datos personales. Dentro de la normatividad se sostiene la posibilidad de utilizar formas "no amigables" para la recolección de las huellas dactilares de las personas que se niegan a brindarles a las autoridades migratorias de los países de la Unión Europea. Entre ellas se encuentra la posibilidad de detener a la persona[56] y -según relatan activistas- de recolectar sus huellas de maneras que pueden llegar a ser violentas.[57]

54. Andrea Dernbach y Der Tagesspiegel, «Eurodac fingerprint database under fire by human rights activists», trad. Erika Körner, Euractiv, 15 de julio de 2015, https://www.euractiv.com/section/justice-home-affairs/news/eurodac-fingerprint-database-under-fire-by-human-rights-activists/.

55. Dernbach y Tagesspiegel.

56. European Comission, «On Implementation of the Eurodac Regulation as regards the obligation to take fingerprints», 27 de mayo de 2015, https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2015)150&lang=es.

57. Euractive, «The curious tale of the French prime minister, PNR and peculiar patterns», 23 de octubre de 2016.

4. Entre las reformas que se proponen a Eurodac, se busca implementar mecanismos de recolección de información que permitan subsanar los casos de personas migrantes y solicitantes de asilo que se niegan a dar sus huellas dactilares. Para obligar el cumplimiento de la ley se ha propuesto la implementación de biometría facial[58], una forma de recolección sigue funcionando aunque se dañen las huellas dactilares o la persona se niegue a suministrarlas.

En el segundo grupo se encuentran los casos relacionados con lo que se hace con las huellas digitales una vez estas son almacenadas en la base de datos general y se encuentran en poder de las autoridades migratorias y de policía. En el segundo caso, algunas problemáticas que se han denunciado son:

1. Las personas migrantes y solicitantes de asilo, son categorizadas de manera arbitraria en el sistema pues este proceso se realiza, con frecuencia, según los criterios del oficial de migración[59]. Esta categorización arbitraria afecta las posibilidades de las personas migrantes y solicitantes de asilo de movilizarse o desarrollar determinados procesos al interior de la Unión Europea.

2. La categorización arbitraria y las diferencias en las condiciones de acogida de algunos de los países miembros de la Unión Europea no garantizan el examen justo y eficiente de las solicitudes de asilo[60].

3. El derecho a la protección de datos y la corrección de información personal no está garantizado para las personas migrantes encontradas en condición irregular ni a solicitantes de asilo, pues no se les permite verificar si sus datos se encuentran o no en el sistema, ni rectificarlos[61]. Esto aumenta las posibilidades de identificación errónea o de que estos errores afectan los procesos de las personas solicitantes.

4. El sistema de Eurodac de manera general restringe la posibilidad de movilidad de las personas solicitantes de asilo o encontradas migrando de manera irregular, puesto que se ven obligadas a quedarse en el país en que fueron abordadas por la autoridad migratoria hasta que se tenga una resolución sobre su caso.

58. Lyneham, «EU's migrant fingerprinting system Eurodac under review».

59. Las categorías que se manejan con Eurodac son las siguientes: categoría 1 para solicitantes de protección internacional; categoría 2 para personas encontradas cruzando la frontera de algún estado miembro de la Unión Europea de manera irregular, o categoría 3 para personas encontradas permaneciendo de manera irregular en un estado miembro de la Unión Europea.

60. Blanca Garcés-Mascareñas, «Por qué Dublín "no funciona"», CIDOB (blog), 1 de noviembre de 2015, https://www.cidob.org/es/publicaciones/serie_de_publicacion/notes_internacionals/n1_135_por_que_dublin_no_funciona/por_que_dublin_no_funciona.

61. Valeria Ferraris, «Economic Migrants and Asylum Seekers in Ten Fingers: Some Reflections on Eurodac and Border Control», Faculty of Law Blog, University of Oxford (blog), 8 de mayo de 2017, https://blogs.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2017/05/economic-migrants.

5. No hay libertad para las personas migrantes o solicitantes de asilo sobre en qué país desean adelantar su proceso o construir su vida debido a los postulados de la Reglamentación de Dublín.

6. Se vienen desarrollando propuestas que harán que Eurodac ya no sea una base de datos anonimizada[62]. De manera adicional a la recolección de huellas dactilares, se está proponiendo la recolección de datos biográficos, personales, huellas y fotografías faciales, estas propuestas podrían llegar a afectar el derecho a la privacidad de las personas migrantes en condición irregular y solicitantes de asilo.

1.2.2.2 Migration information and data analysis system (MIDAS): el sistema biométrico desarrollado por la Organización Internacional para las Migraciones (OIM)

El sistema de información y análisis de datos sobre migración (MIDAS, en inglés) fue desarrollado por la OIM en 2009 como un sistema de utilización sencilla, de alta calidad que pudiera ser usado por aquellos estados que requieren una solución integral efectiva y a bajo costo.[63] MIDAS es un sistema de entrada-salida con el cual es posible recopilar, procesar, archivar y analizar la información de las personas en tiempo real. Estos datos que se toman de la persona pueden ser contrastados con bases nacionales e internacionales disponibles para los Estados, pero también son almacenados en una base de datos central.

El funcionamiento de MIDAS consiste en la captura de la información biográfica y biométrica de las personas a través de la lectura de los documentos de viaje e identificación, lectores de huellas digitales y cámaras web equipadas para la toma de fotografías.[64] En todos los casos el sistema recolecta: datos biográficos (nombre, apellidos, fecha de nacimiento, etc.); datos biométricos (huellas dactilares y faciales); imágenes de los documentos de identificación examinados bajo luz infrarroja; datos de entrada y salida del país; datos sobre visados que pueda tener la persona y medio a través del cual se ingresa al país[65]. Aunque actualmente este sistema se encuentra en varias partes del mundo, ha sido mayoritariamente adquirido por países africanos.

62. Ferraris.

63. Samuel Singler, «Biometric statehood, transnational solutionism and security devices: The performative dimensions of the IOM's MIDAS», Theoretical Criminology 25, n.o 3 (2021): 454-73, https://doi.org/10.1177/13624806211031245.

64. Organización Internacional para las Migraciones, «MIDAS. A COMPREHENSIVE AND AFFORDABLE BORDER MANAGEMENT INFORMATION SYSTEM», s.f, https://www.iom.int/sites/g/files/tmzbdl486/files/documents/midas-brochure18-v7-en_digitall.pdf.

65. Organización Internacional para las Migraciones.

¿Cuáles son los riesgos en materia de derechos humanos asociados a la implementación de MIDAS?

Algunos de los principales riesgos en materia de derechos humanos que se asocian las sistema MIDAS son:

1. En algunos lugares como Nigeria se ha encontrado que hay una falta de consentimiento informado por parte de las personas migrantes para la recolección de sus huellas dactilares. Esta situación se debe a que muchas de las personas migrantes no hablan el idioma de los oficiales migratorios. En casos como el de Nigeria, se ha evidenciado como algunos de los oficiales solamente le muestran a las personas cómo colocar sus dedos sobre los sensores para realizar la captación de datos personales, pero no explican en otras formas el procedimiento, sus objetivos o sus alcances[66].

2. MIDAS permite la extensión de la vigilancia sobre los migrantes africanos, incluso fuera de África. En casos como el nigeriano se ha encontrado la suscripción de contratos con Agencia de Control Fronterizo y Marítimo de la Unión Europea (FRONTEX, por sus siglas en francés) para el análisis de la información que recopila el sistema MIDAS a través del África Frontex Risk Analysis Cell (AFIC). Según declaraciones de funcionarios de la OIM y de la agencia misma el uso de información del AFIC permite expandir la capacidad de información que puede tener la agencia para determinar dentro de la Unión Europea la procedencia exacta de los migrantes africanos.

3. En varios países de África se ha firmado el protocolo de la Comunidad Económica de Estados de África Occidental (ECOWAS, por sus siglas en inglés) que permite el libre movimiento de bienes y personas a través de las fronteras de los Estados miembros. Sin embargo, se ha evidenciado que esta movilidad es restringida por el sistema de control migratorio MIDAS, resultando no solo en reducción de la movilidad sino también en la detención de las personas que realizan un movimiento entre países para trabajar o estudiar.[67]

66. Florence Boyer y Harouna Mounkaila, «LA FABRIQUE DE LA POLITIQUE MIGRATOIRE AU NIGER: LES APPROCHES SÉCURITAIRES ET HUMANITAIRES AU SERVICE DE LA FERMETURE D'UN COULOIR MIGRATOIRE», Routes et pauses des parcours migratoires : Afrique-Amérique, n.o 3 (2018), https://horizon.documentation.ird.fr/exl-doc/pleins_textes/divers21-02/010077535.pdf.

67. Kamal Donko, Uli Beisel, y Martin Doevenspeck, «Security and Trade in African Borderlands: migration Control, the Local Economy and Violence in the Burkina Faso and Niger Borderland», Journal of Borderlands Studies 37, n.o 2 (2022): 235-51.

2. Y EN COLOMBIA ¿CÓMO HA FUNCIONADO LA BIOMETRÍA? ¿CÓMO PASÓ A SER UN REQUISITO PARA LAS PERSONAS MIGRANTES VENEZOLANAS?

2.1. Antecedentes: el aumento de la migración colombo venezolana y la expedición del Estatuto Temporal de Protección al Migrante venezolano (ETPMV)

Durante varias décadas Colombia se caracterizó más por ser un país expulsor de población foránea que uno de recepción de flujos migratorios o de acogida[68]. Sin embargo, recientemente, por el desmejoramiento de las condiciones sociales, económicas y políticas de Venezuela, Colombia se convirtió en uno de los principales destinos para personas venezolanas -o que vivían en este país- y comunidades indígenas69. Aunque la movilidad entre las fronteras de Colombia y Venezuela para el desarrollo de actividades comerciales, educativas y laborales era constante, y en décadas pasadas hubo un flujo importante de Colombianos hacia Venezuela, en la segunda década del S.XXI se evidenció una inversión en esta dinámica.

68. María Teresa Palacios Sanabria y Beatríz Londoño Toro, eds., Migración y derechos humanos: el caso colombiano, 2014-2018, Primera edición, Jurisprudencia (Bogotá: Universidad del Rosario, 2019).

69. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, «CONPES 3950 Estrategia para la atención de la migración desde Venezuela», 23 de noviembre de 2018, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3950.pdf.

Para el año 2015 el presidente Nicolás Maduro anunció el cierre de fronteras con Colombia y su Gobierno inició un proceso de deportación de personas colombianas.[70] Durante este año también comienzó a aumentar la migración de personas venezolanas a Colombia, ya no solo en relación con las actividades en las zonas de frontera, sino también para establecerse en diversos puntos. Por su posición estratégica en el continente, el territorio colombiano, cuando no es el destino final, es también una espacio de paso hacia diversos destinos migratorios incluidos Estados Unidos, Ecuador y Perú, entre otros. Una de las rutas más utilizadas y peligrosas para quienes se desplazan hacia el norte del continente es la del Tapón del Darien[71].

Es así como a partir de esta fecha el número de personas venezolanas en Colombia tendió a aumentar y alcanzó un pico en el año 2018. Si en 2014 se contabilizaban 23.573 personas en el país, en 2015 las cifras ascenderían a 31.471[72]. Así mismo, aunque en 2017 se registraron 403.702 personas venezolanas en el país, para 2018 había aproximadamente 1.174.743 y en 2021 el número cerró en 1.742.927[73] según las cifras de Migración Colombia.

Ante esta migración acelerada, el gobierno nacional de Colombia desplegó alternativas para la identificación, caracterización y regularización de la población migrante venezolana –véase imagen 1–. El Gobierno también expidió el CONPES 3950 de 2019 en que formuló una estrategia de política pública para enfrentar la crisis migratoria y ofrecer soluciones en relación con la salud, vivienda, educación, trabajo y acceso a servicios básicos, entre otros, para la población venezolana que llegaba a Colombia.

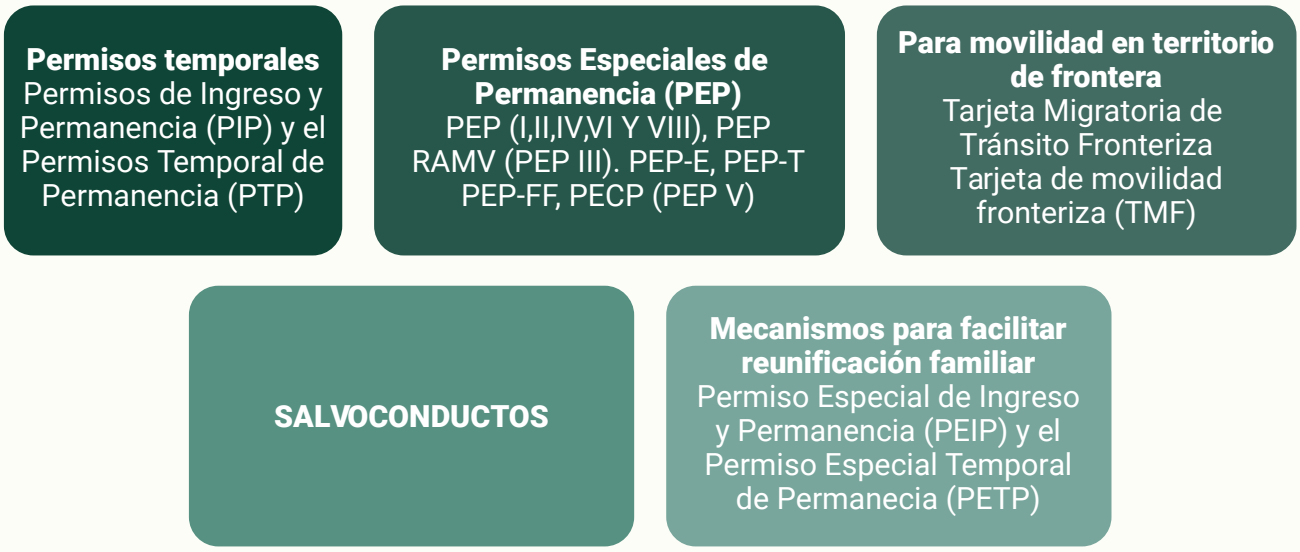
70. OCHA, «Colombia: Situación humanitaria en frontera colombo- venezolana Informe de situación No. 12», 2015, https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/151015_informe_de_situacion_no_12_situacion_de_frontera_final.pdf.

71. «Ruta migratoria del Darién 2023: todo lo que debés saber sobre los peligros de la selva entre Colombia y Panamá», Médicos Sin Fronteras Argentina, 5 de mayo de 2023, https://www.msf.org.ar/actualidad/ruta-migratoria-darien-todo-lo-que-debes-saber.

72. Unidad Administrativa Especial de Migración Colombia, «Distribución de venezolanos en Colombia», 31 de enero de 2021, 2.

73. Unidad Administrativa Especial de Migración Colombia, 2.

Imagen 2: mecanismos desarrollados por el Gobierno colombiano para atender la situación de la población migrante venezolana en el país[74]



Aunque los mecanismos de regulación de la situación migratoria de las personas venezolanas fueron de utilidad en su momento, con el paso del tiempo mostraron su alcance limitado y horizontes temporales muy cortos. Por un lado, seguían llegando personas venezolanas al país que, aunque entraban de manera regular con su pasaporte o por corredores humanitarios, permanecían en Colombia sin tener los permisos para ello y debían acceder a alguno de los mecanismos temporales brindados por el Gobierno. Por otro lado, la migración de personas en condición irregular fue aumentando sin que hubiera mecanismos adecuados para contribuir su regularización[75].

En busca de solucionar la situación, el gobierno nacional propuso el desarrollo de un Estatuto Temporal de Protección al Migrante Venezolano (ETPMV) en cabeza de la Unidad Administrativa Especial de Migración Colombia (Migración Colombia). El ETPMV

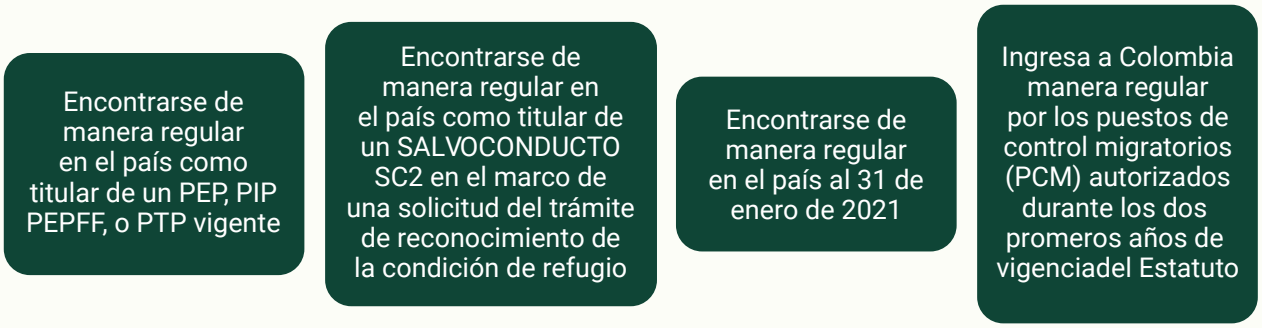
74. Elaborado por los autores (2022) con base en Presidencia de la República, «Decreto 1770 "Por el cual se declara el Estado de Emergencia Económica, Social y Ecológica en parte del territorio nacional."» (2015), https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=66171; Unidad Administrativa EspecialMigración Colombia, «Resolución 1220» (2016), https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/resolucion_uaemc_1220_2016.htm#:~:text=Ministerio%20de%20Relaciones%20Exteriores%20%2D%20Normograma,Unidad%20Administrativa%20Especial%20Migraci%C3%B3n%20Colombia%5D&text=Por%20la%20cual%20se%20establecen,Fronterizo%20en%20el%20territorio%20nacional.; CONPES, «Documento CONPES 3950 Estrategia para la atención de la migración desde Venezuela»; Ministerio de Relaciones Exteriores y Presidencia de la República, «Decreto 216 Por medio del cual se adopta el Estatuto Temporal de Protección para Migrantes Venezolanos Bajo Régimen de Protección Temporal y se dictan otras disposiciones en materia migratoria» (2021), https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20216%20DEL%201%20DE%20MARZO%20DE%202021.pdf.

75. Ministerio de Relaciones Exteriores y Presidencia de la República, Decreto 216 Por medio del cual se adopta el Estatuto Temporal de Protección para Migrantes Venezolanos Bajo Régimen de Protección Temporal y se dictan otras disposiciones en materia migratoria.

se planteó como un mecanismo jurídico de protección temporal para las personas venezolanas migrantes que se encontraban en el país al 31 de enero de 2021 y para aquellas que ingresaran de manera regular al país hasta el 24 de noviembre de 2023.[76]

A través de este mecanismo se busca "(...) generar el registro de información de esta población migrante y posteriormente otorgar un beneficio temporal de regularización"[77] a aquellos migrantes que cumplan con las condiciones establecidas en el decreto 216 de 2021 -véase imagen 2-.

Imagen 3: Requisitos establecidos en el decreto 216 de 2021 para acceder al Estatuto Temporal de Protección al Migrante Venezolano (ETPM)[78]



El beneficio temporal de regularización para las personas migrantes se materializa en el Permiso por Protección Temporal (PPT). El PPT es un documento de identidad que autoriza a la persona a ejercer cualquier ocupación legal en el país y permite "acreditar (...) su permanencia en Colombia para los efectos de la acumulación del tiempo requerido para aplicar a una Visa Tipo R"[79].[80]

76. Unidad Administrativa Especial de Migración Colombia, «ABC Estatuto temporal de Protección, Resolución 0971 de 2021», 8 de junio de 2021, https://www.migracioncolombia.gov.co/infografias-visibles/abc-estatuto-temporal-de-proteccion-resolucion-0971-de-2021.

77. Ministerio de Relaciones Exteriores y Presidencia de la República, Decreto 216 Por medio del cual se adopta el Estatuto Temporal de Protección para Migrantes Venezolanos Bajo Régimen de Protección Temporal y se dictan otras disposiciones en materia migratoria, 15.

78. Elaborado por los autores (2022) con base en el Ministerio de Relaciones Exteriores y Presidencia de la República, Decreto 216 Por medio del cual se adopta el Estatuto Temporal de Protección para Migrantes Venezolanos Bajo Régimen de Protección Temporal y se dictan otras disposiciones en materia migratoria.

79. Visa de residente, puede darse para quienes quieren establecer su residencia en colombia pues son padres de un nacional, renunciaron a su nacionalidad por la colombiana, han acumulado un tiempo de permanencia o por inversión extranjera. Para más información véase Cancillería, «Tipos de visa en Colombia», 2020, https://www.cancilleria.gov.co/tt_ss/1-tipos-visas-colombia.

80. Ministerio de Relaciones Exteriores y Presidencia de la República, Decreto 216 Por medio del cual se adopta el Estatuto Temporal de Protección para Migrantes Venezolanos Bajo Régimen de Protección Temporal y se dictan otras disposiciones en materia migratoria, 18.

Para que se otorgue el PPT, además de cumplir con lo que se enuncia en la imagen 3, la persona debe completar el Registro Único de Migrantes Venezolanos (RUMV). El RUMV está compuesto por tres etapas: i) completar el formulario de pre-registro en la página de Migración Colombia ii) diligenciar la encuesta de caracterización socio-económica; y iii) asistir a la toma de datos biométricos en los centros determinados para ello por Migración Colombia.

2.1.1 Una vez cumplidos los requisitos, ¿cuáles son los pasos a seguir para obtener el Permiso por Protección Temporal (PPT)?

Una vez la persona migrante se ha asegurado de que cumple con los requisitos para acogerse al estatuto, debe desarrollar en su totalidad las tres etapas del Registro Único de Migrantes Venezolanos (RUMV). El RUMV es administrado por Migración Colombia y tiene como objetivo la recolección de información biográfica, socioeconómica y biométrica de la población migrante venezolana que se encuentra en el país y que cumple con los requisitos para acogerse al ETPMV[81]. Para el Gobierno colombiano la recolección de los datos que contiene en RUMV es un paso necesario para identificar a la población migrante venezolana que se encuentra en el país y las condiciones en las que se encuentra, pues, según la narrativa oficial, con estos datos se puede formular políticas y programas adecuados. Cabe anotar, sin embargo, que la recolección de estos datos –en especial los datos biométricos– busca servir también una función de securitización, en tanto sirven para vigilar a las personas migrantes y pueden ser usados en contextos judiciales.

El RUMV se divide en tres etapas sucesivas: i) pre-registro; ii) diligenciamiento de la encuesta de caracterización socioeconómica y iii) registro biométrico presencial. En primer lugar, para que la persona migrante pueda realizar el pre-registro deberá crear un usuario y contraseña en la página de Migración Colombia, autenticarse y llenar los datos que le pide el sistema –véase el cuadro 1–.

81. Ministerio de Relaciones Exteriores y Presidencia de la República, Decreto 216 Por medio del cual se adopta el Estatuto Temporal de Protección para Migrantes Venezolanos Bajo Régimen de Protección Temporal y se dictan otras disposiciones en materia migratoria.

Cuadro 1: datos que se le solicitan a las personas migrantes durante el pre-registro en la página web de Migración Colombia[82]

1	**Datos de registro**	Tipo y número de documento, nacionalidad, nombres y apellidos, fecha de nacimiento. Estos datos son recuperados automáticamente por el sistema.
2	**Registro de hoja de vida**	Tipo de operación (solo brinda una opción, Permiso por Protección Temporal), género, fecha de vencimiento del documento, profesión/ocupación, lugar de nacimiento con su estado o departamento y ciudad o municipio.
3	**Datos de domicilio y contacto**	
4	**Información del grupo familiar**	
5	**Adjunto de documentos**	Fotografía tipo documento, fotografía del documento de identificación y prueba sumaria (solo para personas que se encontraban en el país en situación irregular antes del 31 de enero de 2021).

Una vez se ha realizado el pre-registro, la segunda etapa que debe completar la persona migrante es el diligenciamiento de la encuesta de caracterización socio-económica en su totalidad, consignando todos los datos que se solicitan –véase cuadro 2–. En caso de que no se conteste toda la encuesta, el proceso se toma como incompleto y no será posible que la persona obtenga un turno para asistir a la tercera etapa del proceso, es decir, a la recolección presencial de los datos biométricos en el espacio establecido por Migración Colombia.

Cuadro 2: datos que se solicitan a las personas migrantes en la encuesta de caracterización socio-económica[83]

1	**Reconocimiento y pertenencia**	Indicar si se está solicitando o no la condición de refugiado ante el Ministerio de Relaciones Exteriores y cuál fue su intención al momento de ingresar al país.

82. Elaborado por los autores (2022) con base en Unidad Administrativa Especial de Migración Colombia, «Tutorial para contestar la encuesta de caracterización socioeconómica.», 23 de mayo de 2021, https://www.migracioncolombia.gov.co/rumv/tutorial-para-contestar-la-encuesta-de-caracterizacion-ocieconomica.

83. Elaborado por los autores (2022) con base en Unidad Administrativa Especial de Migración Colombia; Unidad Administrativa Especial de Migración Colombia, «Respuesta Solicitud de información con radicado No. 202124115098821», 12 de enero de 2022.

2	**Documentos de identificación nacional, pertenencia étnica e identidad**	Documentos con los que se cuenta (PEP, TMF, PFT, pasaporte o salvoconducto), identidad de género, pertenencia a un grupo étnico, orientación sexual.
3	**Grupo familiar**	Lugar de nacimiento, familiares que aún se mantienen en Venezuela e intenciones de migración de estos, envío de remesas y medios por los cuales se realiza a Venezuela, indicar si se tienen relaciones de parentesco en Colombia que otorguen ciudadanía, o si hubo intentos o intenciones de acceder a ciudadanía colombiana.
4	**Condición de vida**	Programas de alimentación o subsidio a los que actualmente tiene acceso, niños y adolescentes a cargo y datos generales de estos, indicar si los niños y adolescentes a su cargo se encuentran estudiando, actividades al aire libre realizan y si se tiene un lugar destinado para su cuidado, indicar si alguna vez se quedó sin vivienda por uno o más días o hubo problemas para satisfacer las necesidades alimenticias de los niños y adolescentes a su cuidado.
5	**Estudios y ocupación**	Acceso a alimentación y transporte escolar en Colombia, acceso a entidades educativas en el país, último grado de escolaridad obtenido en Colombia, indicar si sabe leer y escribir, experiencia laboral certificada (en Colombia o Venezuela), actividad que desempeña actualmente y cómo llegó a ella, en que sector se localiza esta actividad, ingresos mensuales y tipo de contrato. Respecto al trabajo en Venezuela, se solicitan cuál era el empleo, en qué sector, cuál era la remuneración mensual del mismo, o si se tenía empresa.
6	**Seguridad y protección social**	Indicar si está o no afiliado a un sistema de protección social en el país, si lo está especificar a cuál, si no lo está especificar por qué no.
7	**Salud**	Enfermedades crónicas, infectocontagiosas, enfermedades de transmisión sexual (si tiene alguna indicar cuál), indicar si se tiene o no acceso a medicamentos para el tratamiento de la enfermedad, embarazo, lactancia, indicar si asiste a controles prenatales, si se es gestante o lactante indicar si consume suplementos, indicar si se ha contagiado de COVID-19.

8	**Motivos de migración**	Indicar motivos que lo motivaron a migrar de Venezuela a Colombia.
9	**Percepción de integración**	Indicar si se ha sentido discriminado en Colombia, en qué lugares y que tan fácil o difícil considera el acceso a determinados bienes.
10	**Vulnerabilidad**	Indicar si ha sido víctima de un delito o tipo de violencia en Colombia e indicar de qué tipo.

Una vez se ha completado la encuesta de caracterización socioeconómica, la persona migrante recibe a su correo electrónico una constancia de realización de estas dos etapas. Esta constancia le permite a la persona agendar una fecha para la recolección presencial de datos biométricos en alguno de los centros designados por Migración Colombia. En esta cita se recolectan: fotografía de la persona, huellas dactilares y firma. Una vez completado este proceso se analiza cada caso de manera individual. Si la persona cumple con lo dispuesto en el parágrafo 1 del artículo 15 de la Resolución 971 del 28 de abril de 2021, se otorga la protección del ETPMV y se brinda el Permiso por Protección Temporal (PPT)[84].

En este punto es clave mencionar que aunque la vinculación al ETPMV es voluntaria, si la persona migrante desea acceder al PPT no puede negarse a completar ninguna de las tres etapas que componen el RUMV, pues todos los datos exigidos durante estas etapas son requeridos para continuar el trámite de expedición del permiso según la Resolución 0971 de 2021[85]. En pocas palabras, si alguna de las tres etapas aquí mencionadas no se cumple, incluida la recolección de datos biométricos, el trámite de la persona en cuestión se verá estancado y tendrá pocas posibilidades de acceder al Permiso por Protección Temporal.

2.1.2 ¿Qué tipo de biometría usa el gobierno colombiano en el ETPM? ¿Cómo justifica la recolección de estos datos?

Desde Migración Colombia, la recolección, análisis y almacenamiento de datos sensibles, biométricos, demográficos, movimientos migratorios y documentos administrativos de la población nacional y migrante se realiza en busca de cumplir con la misión institucional de la entidad. Esta misión se resumen en[86]:

84. Unidad Administrativa Especial de Migración Colombia, «ABC Estatuto temporal de Protección, Resolución 0971 de 2021».

85. Unidad Administrativa Especial de Migración Colombia, «Resolución 0971 "Por la cual se implementa el estatuto temporal de protección para migrantes venezolanos adoptado por medio del decreto 216 de 2021» (2021) Artículo 3 y parágrafo del artículo 9.

86. Unidad Administrativa Especial de Migración Colombia, «Estudio previo: licitación pública», 27/072020, 1; Presidencia de la República, «Decreto 4062 "Por el cual se crea la Unidad Administrativa Especial Migración Colombia, se establece su objetivo y estructura"» (2011).

1. Realizar las labores de vigilancia y control migratorio y de extranjería del Estado colombiano.

2. Contribuir a la seguridad nacional.

3. Controlar el registro, ingreso, permanencia y salida de nacionales y extranjeros en territorio colombiano.

4. Desarrollar los demás trámites y documentos relacionados con los procesos migratorios asignados a la entidad por el Gobierno Colombiano.

Aunque Migración Colombia ya tiene entre sus objetivos la recolección de datos de personas nacionales y extranjeras a través de procesos de registro, según la entidad, en el país existían muchas personas migrantes venezolanas aún no registradas. Por esta razón, era fundamental contar con una herramienta como el ETPMV.

Una de las peculiaridades del estatuto es que recoge varias características físicas de las personas migrantes venezolanas, las utiliza para procesos de identificación biométrica y las condensa en el Permiso por Protección Temporal (PPT). Aunque Migración Colombia ya contaba con métodos de autenticación biométrica tanto para nacionales como extranjeros –por ejemplo, Biomig o el reconocimiento dactilar, respectivamente– desde la perspectiva de la entidad contar con un sistema de recolección, encriptación y validación biométrica de las imágenes de huellas, fotografía y firma de personas migrantes venezolanas representa una ayuda para el cumplimiento de varios puntos que son claves para la entidad:

1.Tener procesos más seguros, rápidos y eficientes, reduciendo los tiempos de atención y agilizando los procesos que requiere la Entidad.

2. Identificar de manera más precisa a las personas migrantes venezolanas.

3. Incluir las innovaciones tecnológicas en la institución.

4. Fortalecer y perfeccionar los procesos de recolección de la información de personas nacionales y extranjeras para garantizar la seguridad nacional y una migración ordenada, segura y regular.

5. Desarrollar de manera especializada, eficiente y oportuna el registro único e identificación de migrantes venezolanos que se acojan al Estatuto Temporal de Protección.

Sin embargo, es importante resaltar que la información que recoge Migración Colombia en marco del ETPM a través, por ejemplo, de la encuesta de caracterización, es más cuantiosa, detallada e invasiva que la que recoge para migrantes de otras nacionalidades o que la que tendría a su disposición el Estado tratándose incluso de

sus propios ciudadanos. Por ejemplo, la información sobre la orientación sexual o la salud de las personas caracterizadas, que es especialmente sensible, se recoge bajo la prerrogativa de formular políticas públicas que atiendan necesidades específicas de estas poblaciones que, sin embargo, son difíciles de exigir posteriormente. Esto puede significar, para las personas migrantes, que el estado colombiano conserve su información personal sin que medie ningun proceso de anonimización de datos para su uso estadístico y sin la garantía de que este ofrecerá los servicios sociales que justificarían, en primer lugar, la recolección de dichos datos.

2.1.3 ¿Cómo están regulados actualmente los datos biométricos en Colombia?[87]

El Estado colombiano se rige actualmente por un marco nacional de protección de los datos personales que se utiliza a nivel general –véase cuadro 3–, al igual que una serie de conceptos que se han brindado desde la Superintendencia de Industria y Comercio (SIC) –véase cuadro 4–.

Cuadro 3: normatividad a nivel nacional que debe respetar el Estado colombiano en el manejo de datos personales

Normativa	¿Qué regula en relación con datos personales?
Artículo 15 de la Constitución Política de Colombia	Establece el derecho a la intimidad personal, familiar y al buen nombre de los individuos y la labor del Estado de respetarlos y hacerlos respetar. De igual modo, establece el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.
Ley 1266 de 2008	Establecen las disposiciones generales de Habeas data y derechos del usuario para rectificar y conocer la información que se haya recolectado sobre ellas.
Ley Estatutaria 1581 de 2012	La ley de protección de datos personales establece los tipos de datos y su correcto tratamiento, los principios rectores de los procesos de recolección de datos personales, los derechos y condiciones de legalidad para su recolección, los deberes y derechos de las personas responsables del manejo de los datos y los mecanismos de vigilancia y sanción ante el incumplimiento de la ley.

87. Esta sección es una actualización del capítulo 1 : situación jurídica de los datos biométricos en Juan Castañeda, Joan López, y Lucía Camacho, Biometría en el Estado colombiano ¿Cuándo y cómo se ha justificado su uso?, 2019, https://doi.org/10.13140/RG.2.2.21018.08646.

Decreto 1377 de 2013	Modifica parcialmente la ley 1581 de 2012. Aquí se desarrolla el derecho constitucional de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.
Ley 1712 de 2014	La ley de transparencia y acceso a la información pública.

Cuadro 4: Resoluciones de la Superintendencia de Industria y Comercio (SIC) alrededor del uso de datos personales.

Resoluciones de la SIC	¿Cuál fue el caso que suscitó la decisión?	¿Qué decisión se tomó?
Resolución 58969 de 2014 de la SIC	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.
Resolución 39298 de 2016 de la SIC	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.
Resolución 60640 de 2017 de la SIC	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

Resolución 12809 de 2018 de la SIC	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.
Resolución 29407 de 2018 de la SIC	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.
Resolución 55405 de 2018 de la SIC	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.
Resolución 11395 de 2018 de la SIC	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.
Resolución 43530 de 2018 de la SIC	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.

De manera conjunta a este marco, también se encuentran una serie de medidas y recomendaciones que se han formulado por organizaciones internacionales y ONGs que trabajaban en la atención y protección de la población migrante que se plantean como buenas prácticas que se recomiendan a los Estados, como se ve en el cuadro 5.

Cuadro 5: normatividad, disposiciones y recomendaciones a nivel internacional que brindan pautas al Estado colombiano sobre el manejo de datos personales de las personas migrantes

Normativa	¿Qué regula en relación con el uso de datos personales de las personas migrantes?
Manual de la OIM para la protección de datos personales	Guía para la recopilación, almacenamiento y el procesamiento de datos personales de las personas migrantes en busca de respetar su intimidad, su dignidad y sus derechos fundamentales.
Política sobre la protección de datos personales de las personas de interés de ACNUR	Establece los principios de necesidad y proporcionalidad para la recolección de datos de personas migrantes desde ACNUR, cuáles son los criterios de uso, transferencia, manejo y almacenamiento de la información. También define las maneras en que se comparte la información con terceros.
Proyecto sobre protección de datos en la acción humanitaria, CICR.	Una guía para personas u organizaciones trabajando con protección de datos o personas que trabajan en el asesoramiento para la construcción de normas relacionadas con este tema. Contiene lineamientos y prácticas ya establecidas que se realizan en contextos complejos y volátiles para garantizar el beneficio y la protección de datos de las personas vulnerables.

2.1.4 ¿Qué regulaciones establece MICOL para mis datos?

En la labor que se le fue asignada a la Unidad Administrativa Especial de Migración Colombia por medio del decreto 4062 de 2011, la unidad recolecta, almacena, maneja y utiliza datos de personas nacionales y extranjeras que entren, transiten, tengan intención o permanezcan dentro del territorio nacional. Para llevar a cabo el manejo de esta información Migración Colombia se ciñe a la normativa ya enunciada en el apartado anterior, y a varias leyes y principios constitucionales –véase cuadro 6–.

Cuadro 6: normatividad en la que se basa Migración Colombia para el manejo de datos personales de las personas migrantes[88]

Normativa	¿Qué regula en relación con los datos personales?
Artículo 15 de la Constitución Política de Colombia	Establece el derecho a la intimidad personal, familiar y al buen nombre de los individuos y la labor del Estado de respetarlos y hacerlos respetar.
Ley 1266 de 2008	Establecen las disposiciones generales de Habeas data y derechos del usuario para rectificar y conocer la información que se haya recolectado sobre ellas.
Sentencia C-748 de 2011	Proyecto de Ley Estatutaria de habeas data y protección de datos personales.
Ley 1712 de 2014	La ley de transparencia y acceso a la información pública.
Ley Estatutaria 1581 de 2012	Ley de datos personales establece los tipos de datos y su correcto tratamiento, los principios rectores de los procesos de recolección de datos personales, los derechos y condiciones de legalidad para su recolección, los deberes y derechos de las personas responsables del manejo de los datos y los mecanismos de vigilancia y sanción ante el incumplimiento de la ley.
Decreto 1377 de 2013	Modifica parcialmente la ley 1581 de 2012. Aquí se desarrolla el derecho constitucional de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.

88. Unidad Administrativa Especial de Migración Colombia, «Adopción de la política tratamiento de datos personales de la Unidad Administrativa Especial Migración Colombia», 23 de julio de 2019, https://www.migracioncolombia.gov.co/planeacion/politica-de-tratamiento-de-datos-personales.

Decreto 1067 de 2015 Decreto único reglamentario del Sector de Relaciones exteriores	Define los datos que se recolectan para los distintos tipos de pasaportes y la necesidad de los y las funcionarias de mantener la confidencialidad de la información.
Decreto 1074 de 2015 Decreto único del Sector Comercio, Industria y Turismo.	Señala la labor de vigilancia y protección de la Superintendencia de Industria y Comercio (SIC) sobre el correcto uso de los datos personales de las personas.
Directiva 007 de 2019	Expedida por la Cancillería de Colombia con el fin de disponer los parámetros para que la Unidad Administrativa especial Migración Colombia adopte una política de tratamiento de datos personales
Decreto 216 de 2021	Establece los datos que serán recolectados en cada uno de los pasos del Estatuto Temporal de Protección de Migrantes Venezolanos.
Ley 2136 de 2021	Política integral migratoria del Estado colombiano (PIM). Establece en su artículo 76 una serie de parámetros a cumplir en el tratamiento de datos personales.

En el caso del ETPMV la regulación de datos personales se rige por la tabla anteriormente mostrada. En este caso, con los datos biométricos, la recolección de estos es autorizada por el usuario al momento de crear su usuario en la página de Migración Colombia y su manejo se hace conforme a los principios de la Ley 1581 de 2012, no hay aún una normativa especial de nivel nacional para su manejo.
Ahora respecto a quién tiene o no acceso a la información recolectada por Migración Colombia, en el caso del ETPMV, en el proceso de creación de clave el usuario autoriza a Migración Colombia para compartir los datos recolectados con entidades públicas y privadas para la adopción de políticas públicas en conformidad con el Decreto 216 de 2021. Sin embargo, es necesario mencionar que si bien estas leyes protegen la

recolección, uso y manejo de los datos personales por parte de Migración Colombia, también existen normas a nivel nacional que facultan el intercambio de información entre entidades públicas, privadas y aquellas que ejercen una facultad legal o administrativa de otras entidades del Estado –véase cuadro 7–.

Cuadro 7: Entidades que están facultadas legalmente para acceder a datos biométricos en Colombia

Norma y artículo	Entidad facultada	Tipo de datos a los que puede acceder
Artículo 10 a de la Ley 1581 de 2012	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.
Artículo 18 del Decreto 019 de 2018	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
Artículo 159 de la Ley 1753 de 2015	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.
Artículos 2.2.1, 7.2.2.4, 7.3.1 del Decreto 1413 de 2017.	Entidades públicas y particulares que ejercen función pública	Datos biométricos.

Vale la pena señalar que aunque la SIC es la autoridad responsable de la protección de datos personales y sensibles, esto aplica cuando quien está haciendo el tratamiento es una entidad privada. Cuando el tratamiento está en manos de una entidad pública es la Procuraduría General de la Nación la competente para ello. En este caso, si hubiera lugar a una acción de protección de datos de personas migrantes recogidos por Migración Colombia, sería la Procuraduría quien tendría que intervenir.

2.2 ¿Qué barreras hemos identificado alrededor del uso del ETPMV?

La expedición del ETPMV supone un avance del Estado colombiano en la forma de abordar la migración de las personas venezolanas y su integración socio-económica en el país, pues supone un mecanismo de regularización migratoria temporal que permite a la persona trabajar de manera legal en Colombia. Sin embargo, a pesar de sus ventajas, existen una serie de dificultades, barreras y vacíos que aún deben ser mejorados.

Las dificultades y barreras que se presentan a continuación fueron identificadas por personas de la comunidad de migrantes venezolanos en el país en el espacio de los talleres participativos realizados por la Fundación Karisma, en las ciudades de Bogotá y Medellín. Lo que aquí se presenta parte de lo que las personas migrantes han experimentado en su propio proceso de acogida al Estatuto Temporal de Protección al Migrante, o de su acompañamiento al proceso de otras personas a través de organizaciones sociales o redes de colaboración.

Al ver la tabla 1 vemos cómo las dificultades alrededor del proceso se han organizado en tres grandes grupos: i) las barreras geográficas y económicas de acceso al mecanismo por parte de la población migrante; ii) las fallas en el proceso de recolección, uso, manejo e intercambio de información que hace desde los funcionarios y desde la entidad Migración Colombia para garantizar el acceso de la población migrante al ETPMV; y ,finalmente, iii) la xenofobia y la discriminación.

Tabla 1: Principales problemas asociados al proceso de acogida del ETPMV por personas migrantes venezolanas representantes de organizaciones sociales

Problemas asociados al proceso de acogida al ETPMV por parte de la población migrante venezolana		
Barreras	**Situación actual**	**Dificultades asociadas a la situación actual según la población migrante.**
Barreras geográficas y económicas de acceso al mecanismo por parte de la población migrante	Amplias distancias y limitaciones monetarias para acceder al estatuto	i) El primer desafío es la ubicación geográfica, por ejemplo, todo se concentra en las ciudades grandes. ii) Otro desafío ha sido el problema monetario, ya que los traslados entre ciudades, municipios y veredas implican un costo alto que la población no puede asumir, puesto que no tienen los recursos y la accesibilidad no es la mejor.
	Falta de control efectivo por parte de Migración Colombia a la recepción del documento por personas en zonas de difícil acceso.	i) En algunas partes del país, permiten que a las personas que viven en zonas difíciles les permitan que otras personas recojan el PPT por ellas. Cuando se entrega este documento a otras personas, la entidad da por hecho que esta persona efectivamente recibe el documento sin constatar que realmente lo tenga ella.

Fallas en el proceso de recolección, uso, manejo e intercambio de información que hace desde los funcionarios y desde la entidad Migración Colombia para garantizar el acceso de la población migrante al ETPM	Fallas en los procesos de uso, recolección y manejo de la información recolectada de la población migrante.	i) En la recolección de datos no relacionan bien la información y muchas veces piden a las personas repetir el proceso o emiten documentos con errores ii) Se percibe una falta de cuidado con el almacenamiento de la información biométrica, ya que ha ocurrido casos donde las personas se ven obligadas a repetir el proceso de recolección de estos datos, a veces en más de una ocasión. Los funcionarios presentan excusas para no admitir la pérdida de la información. iii) Si la persona solicita una corrección sobre un PPT emitido, éste suele volver a llegar con el error, lo cual quiere decir que no está funcionando el sistema de corrección de datos.
	Desarticulación entre entidades para el manejo y uso de la información de la población Migrante	i) No se están cruzando adecuadamente las bases de datos por ejemplo para servicios de salud o registro del SISBEN, por lo cual se les niegan los servicios a las personas aun cuando legalmente tienen acceso a los mismos.
	No se brinda información clara y completa por parte de los funcionarios de Migración Colombia	i) Hay bastante desinformación incluso entre funcionarios de las entidades. Los funcionarios no entregan información clara a las personas frente a los procesos del Estatuto ni de corrección del PPT.
Discriminación y xenofobia	Tratos desobligantes, barreras y dificultades de acceso al ETPV	i) En ocasiones el trato en la entidad de Migración es indigno para la población migrante. ii) Las comunidades pertenecientes a la población LGBTI sufren de discriminación y en ocasiones no pueden acceder al registro biométrico.

En primer lugar, un problema de larga data que ya se había identificado con mecanismos como el Registro Administrativo de Migrantes Venezolanos (RAMV), era el establecimiento de los puestos para llevar a cabo el registro en cabeceras municipales o ciudades principales. En su momento, entidades como Humans Right Watch y OCHA[89] mencionaban la dificultad de las personas en espacios rurales y rurales dispersos para acceder al registro por los desplazamientos y gastos económicos que esto implicaba, lo que fomentaba que las personas simplemente no se acercaran a los centros de recolección de información.

Aunque el ETPM se realiza de manera virtual subsiste la barrera geográfica y económica, pues las personas de las zonas dispersas aún deben desplazarse a cabeceras municipales o ciudades principales para atender a la cita de recolección presencial de datos biométricos, y -posteriormente- a la recolección de su documento. Esto llevaba a una situación que puede truncar los procesos de inclusión de la población migrante, ya que aquellas personas que no puedan costear los desplazamientos, simplemente no podrán cumplir con la cita biométrica o a la recolección del documento, y –en consecuencia– no podrán acceder a las estrategias de regularización promovidas por el Estado colombiano.

Atado a este problema, parece estar surgiendo uno igualmente grave. Como contaban algunas personas participantes de los talleres, ante el desplazamiento y gasto que supone para las personas de zonas rurales dispersas recoger su documento, algunas personas adscritas a Migración Colombia parecen estar entregando el documento a terceros para su entrega al titular, sin verificar la recepción del mismo. Aunque, no aún no existen denuncias formales sobre esto, es una situación a la que tanto la comunidad migrante como Migración Colombia deben estar atentos para exigir una solución adecuada. Particularmente, porque esta forma de entrega del documento puede dar paso a la suplantación y a la utilización por parte de terceros de los documentos que no les pertenecen.

En segundo lugar, otro gran problema se refiere al proceso de recolección, uso, manejo e intercambio de información que hace desde los funcionarios y desde la entidad Migración Colombia para garantizar el acceso de la población migrante al ETPMV. Por un lado, en relación con la información que manejan los funcionarios de la entidad, las personas migrantes asistentes a los talleres mencionaron cómo muchas veces estos también tienen vacíos en su capacitación y no saben cómo han de abordarse ciertos trámites y requerimientos. Esta falta de capacitación y de información que tienen algunos funcionarios deja a las personas migrantes sumidas en procesos de duda y sin saber cómo actuar frente a determinados procedimientos.

89. Human Rights Watch, «LA GUERRA EN EL CATATUMBO: Abusos de grupos armados contra civiles colombianos y venezolanos en el noreste de Colombia», 2019, https://www.hrw.org/sites/default/files/report_pdf/colombia0819sp_web_0.pdf; OCHA, «Colombia: Doble afectación en la subregión del Catatumbo (Norte de Santander) (conflicto armado y Flujos Migratorios Mixtos) 25 al 29 de Septiembre 2018», https://www.refworld.org.es/cgi-bin/texis/vtx/rwmain?page=search&docid=5c5080cc4&skip=0&query=RAMV.

Por otro lado, respecto al manejo de información que se hace desde la entidad, el CONPES 4100 de 2022 señala que aún subsisten varias fallas alrededor del manejo de la información que se recolecta sobre la población migrante venezolana, aún está dispersa entre diversas entidades, instituciones e instrumentos, lo que impide su correcta utilización para el bien de la población migrante.

Además de las implicaciones que esto tiene para el desarrollo de la política pública y de la estrategia de regularización migratoria en sí, es necesario evidenciar que fallas en la recolección de datos biográficos y biométricos, o brindar información incompleta o nula, puede suponer para las personas migrantes. Estos fallos pueden consolidarse en una barrera importante en el acceso a bienes y servicios del Estado, desencuentros con las autoridades y problemas de coherencia entre sus documentos para el acceso al empleo. Es una falla anclada en la falta de información, responsabilidades y convenios claros, en la duplicación de esfuerzos y en la falta de sinergia entre todas las escalas y niveles de atención de esta población.

Finalmente, un problema grave señalado durante los talleres es la xenofobia y la discriminación que enfrentan las personas migrantes venezolanas por su condición de migrantes, pero –en algunos casos– también por pertenecer a la comunidad LGBTI+. Particularmente, en los talleres se mostró cómo algunos funcionarios de Migración Colombia tratan con agresividad y de manera displicente a las personas migrantes, y se relacionan con ellas de manera desobligante durante la realización de sus trámites. Así mismo, se mencionó cómo a pesar de lo establecido por el gobierno alrededor de la comunidad LGBTI+ en relación con el ETPM aún algunas personas de la comunidad trans tienen problemas para el registro biométrico o para cumplir las condiciones establecidas para acceder al estatuto. Estas dos situaciones son bastante alarmantes pues muestran cómo una estretgia de regulación que está planteada desde la inclusión, puede estar siendo empañada por actitudes que favorecen la discriminación y la violencia hacia poblaciones en condiciones de vulnerabilidad y marginalidad altas.

2.3 Y todos estos datos, ¿para qué se usan?

La pregunta que nos queda por resolver es para qué van a usarse estos datos que se recolectan a través del proceso de acogida al Estatuto Temporal de Protección al Migrante Venezolano. Los datos que se recolectan serán utilizados –según la normatividad vigente– para dos cosas. Por un lado, para brindar un documento de identificación a la población migrante, que actúa como mecanismo de regularización temporal de la situación migratoria, y que le permite a la persona trabajar en el país. Por otro lado, los datos que se recolectan también se utilizarán para la formulación de políticas públicas adecuadas para atender las necesidades de la población migrante venezolana que favorezcan su integración socio-económica en el país.

Como ya hemos visto, los procesos de recolección de la información a través del RUMV, la encuesta de caracterización socio-económica y la cita biométrica no están exentos de fallas y problemas que aún deben solucionarse. Así, aunque las intenciones sean buenas, es necesario que las personas migrantes y de las entidades, ongs, organizaciones de la sociedad civil y personas aliadas a estos procesos tengan presentes los alcances de estas políticas y se cuestionen de manera continua ciertos aspectos:

1. El acceso real del documento a bienes y servicios del Estado: ¿a qué tipo de bienes y servicios puedo yo acceder? ¿Se me ha negado el acceso en algún momento con el documento PPT? ¿Por qué? ¿Es esto legal? ¿De qué mecanismos puedo valerme para hacer cumplir mis derechos, y las responsabilidades que tiene conmigo el Estado colombiano?

2. El uso real que se está haciendo de los datos recolectados: ¿Qué tipo de políticas públicas se formularán con los datos recolectados? ¿Para qué fechas se está pensando su formulación? Si no se están utilizando los datos para plantear política pública ¿para qué se utilizan y quién tiene acceso a los mismos?

3. La capacidad real de desarrollo de las políticas que justifican la recolección de datos: ¿las políticas formuladas tienen presupuestos aprobados? ¿Cuánto se aprobó? ¿Cuáles son los programas y mecanismos a través de los cuáles se hará efectiva la política en el territorio nacional? ¿Cuáles son las entidades encargadas de ejecutar estos programas y mecanismos y en qué partes del territorio nacional?

4. Rol de la población migrante en el diseño y la implementación de programas y políticas: ¿cómo se está pensando el rol de la población migrante en estas políticas públicas y sus programas? Aquí es fundamental cuestionarse si sólo se piensan como receptores de las políticas, o si participan de manera activa en su diseño, construcción y evaluación.

5. Abordaje de fallas identificadas: ¿qué mecanismos se están implementando para subsanar o eliminar las fallas que se han presentado en el proceso del Estatuto Temporal de Protección al Migrante Venezolano? ¿cómo se están subsanando los vacíos?

En pocas palabras, es necesario que las personas que participan en el ecosistema de la migración, y especialmente la población migrante venezolana, ejerzan un rol de veeduría

ciudadana de los procesos que las involucran o que les afectan. Así mismo, que observen con ojo crítico las políticas, proyectos y mecanismos que exigen la recolección de sus datos personales para participar, pues la recolección y utilización de estos datos bajo unos fines específicos, les permiten exigir y verificar cumplimiento de los mismos.

Por último es necesario resaltar tiembién la posibilidad de que estos datos se estén recolectando con la intención de hacer más rígidas y estrtictas las políticas securitarias, es decir, que se consoliden en mecanismos de vigilancia sobre la población migrante. Esto es especialmente preocupante en la medida en que revelaría que el estado concibe a los foráneos como una población que ha de ser controlada de manera más rígida que la población nacional, lo que sin duda constituye la materialización de un prejuicio negativo infundado, que el Estado colombiano es el primero llamado a desmontar.

3. CONCLUSIONES

3.1 ¿Qué principios debería seguir cualquier proceso y sistema ligado a la regularización migratoria de las personas venezolanas?

Este análisis del sistema de datos biográficos y biométricos de la población migrante nos revela las muchas oportunidade de mejora que existen en este entorno. Para trazar un camino cierto hacia sistemas más justos de recolección de datos de identidad, tanto de población migrante como de otras minorías vulnerables y también de nacionales colombianos, desde Karisma hemos construido una serie de principios generales que consideramos todos los sistemas de identidad deberían respetar.

Estos principios se construyeron a través del análisis de múltiples documentos de guías y estándares de organizaciones internacionales. Además, los principios se complementaron con el análisis de experiencias internacionales que mostraron los riesgos de derechos humanos relacionados con los sistemas de identidad.

A pesar de la importancia de un sistema de identidad para la protección de derechos fundamentales, la Fundación Karisma reconoce que la identidad legal por sí misma no puede solucionar serios problemas de acceso a servicios de comunidades migrantes. Para que el acceso a beneficios y oportunidades mejore, estos servicios deben existir para toda la población, sin depender de su capacidad de identificarse o, peor aún, de demostrar su situación regular. Sin embargo, en muchos casos esta condición no se cumple en muchos casos en Colombia.

Aunque los sistemas de identidad legal pueden lograr poco por sí solos, pueden ser un primer paso para proteger los derechos humanos. Por esto, imaginamos los principios como parte de una agenda a largo plazo de los Estados para proteger a las personas garantizando que la inclusión de la tecnología en la garantía al derecho a la identidad legal no ponga en riesgo otros derechos.

Los principios que proponemos son:

1. Inclusión
2. No discriminación
3. Seguridad digital
4. Privacidad
5. Sostenibilidad
6. Estado de derecho

A continuación ofrecemos un breve resumen de cada uno, pero en nuestra página web pueden consultarse en profundidad.

3.1.1 Inclusión

> **Los Estados tienen la obligación de promover condiciones para el acceso igualitario e inclusivo a la identidad legal para todas las personas.**

Esto implica generar acciones que permitan el reconocimiento efectivo de los derechos de todas las personas. Así mismo, implica no sólo abstenerse de acciones discriminatorias, sino tomar medidas a favor de grupos particulares.

Un sistema de identidad que proteja los derechos humanos impone obligaciones a los Estados para garantizar la posibilidad de que todas las personas accedan a una identidad legal. El objetivo de cobertura universal también le impone nuevos requerimientos a los sistemas para asegurarse que la identidad legal creada no se convierta en una forma de discriminación, ni se preste para prácticas abusivas como la vigilancia indiscriminada o masiva. Esto implica por un lado, buscar la cobertura universal y establecer unas garantías mínimas de seguridad y, por el otro, eliminar las barreras de acceso a la identidad.

3.1.2 No discriminación

> **Los sistemas deben tratar a todas las personas en condiciones de igualdad y sin discriminación por razón de su origen o nacionalidad.**

Las razones para un trato diferencial deben ser excepcionales y estar fundamentadas en criterios de legalidad, necesidad y proporcionalidad propios de un Estado de Derecho. Desde esta perspectiva, es inadmisible el tratamiento de las personas desde enfoques punitivos así como la construcción de una política al servicio de funciones de vigilancia. Para el caso de las personas migrantes, deben descartarse prácticas como exigir más información que la exigida a los nacionales, o información que no contribuye a la formulación de política pública que las beneficie.

3.1.3 Seguridad Digital

Los sistemas de identidad deben proteger los datos de las personas de injerencias ilegítimas.

Un sistema de identidad robusto debe estar acompañado por un marco fuerte de seguridad digital. La recolección de grandes cantidades de información personal relacionada con la identidad, incluyendo datos biométricos y biográficos, son objetivos de atacantes interesados en explotar estos datos para su beneficio. Por esto, un marco de seguridad digital en un sistema de identidad implica la preservación de la disponibilidad, la confidencialidad y la integridad de la información de las personas y su infraestructura. Esto es aún más importante si la información, como en el caso de la población migrante, incluye información biométrica y biográfica especialmente sensible.

3.1.4 Privacidad

Los sistemas de identidad deben estar diseñados con un enfoque de privacidad por diseño.

Este principio recoge el enfoque de privacidad por diseño con el objetivo de diseñar los sistemas de tal forma que no se requieran acciones de parte de un individuo para proteger su derecho a la privacidad. Los principales requerimientos que surgen desde esta perspectiva son:

- **Proactividad:** El diseño debe anticipar y prevenir los daños a la privacidad antes de que pasen.
- **Estandarización:** Un uso sistemático de estándares aceptados internacionalmente y hacer análisis de riesgos.
- **Funcionalidad completa:** El sistema debe ser funcional para el beneficio de todas las partes interesadas.
- **Visibilidad y transparencia:** El sistema debe mantenerse visible y transparente para las personas usuarias y sujeto a verificación independiente.
- **Empoderamiento las personas:** El sistema debe empoderar a las personas usuarias sobre sus datos por medio del consentimiento informado, la exactitud de los datos y el acceso a los mismos.

3.1.5 Sostenibilidad

Los sistemas de identidad deben ser sostenibles financiera y operacionalmente.

Los sistemas de identidad deben ser sostenibles, mientras que mantienen la accesibilidad para las personas y las demás partes interesadas. Los sistemas de identidad deben buscar la neutralidad tecnológica para incrementar la flexibilidad del sistema y no impedir que se cumpla con los objetivos de inclusión social.

3.1.6 Estado de derecho

Los sistemas de identidad deben estar estructurados integralmente en los marcos regulatorios con responsabilidades y procedimientos claramente definidos.

Este principio señala la necesidad de que los sistemas de identidad estén estructurados a partir del reconocimiento amplio e integral de las políticas y marcos regulatorios de protección de los derechos humanos y estos sean aplicados, reconocidos y defendidos con integridad con una articulación clara y continua entre todos los actores.

4. ANEXO: ALGUNAS HERRAMIENTAS PARA ORGANIZACIONES Y PERSONAS MIGRANTES

4.1 El ecosistema de información: ¿quién recoge los datos? ¿quién los usa? ¿para qué?

El desarrollo de talleres participativos con la población migrante venezolana deja un aspecto bastante claro y es que hay un constante flujo de información desde las organizaciones sociales que acompañan a la población migrante, y las personas migrantes, hacia instituciones públicas y privadas de diversa índole. Estos flujos de información -desde la experiencia de los migrantes- son fundamentales para acceder a bienes y servicios del Estado, ayuda por parte de las ONG, entidades internacionales, o grupos territoriales. Sin embargo, en estos procesos no siempre se respeta el derecho a la protección de datos, el consentimiento libre o el establecimiento claro y directo de los usos de la información.

Por solo mencionar un caso general, aún subsiste la recopilación de información de las personas migrantes que desean acceder a programas alimenticios o paquetes de ayuda de algunas organizaciones territoriales de orden privado. En estos procesos, el migrante en situación de vulnerabilidad y con pocas oportunidades económicas no cuenta realmente con las condiciones para negarse a brindar sus datos personales, pues esta negación implica no tener acceso a comida, a un refugio o inclusive a algunos bonos que permiten subsanar necesidades a corto plazo. En estas condiciones, pensar en un consentimiento brindado de manera libre e informado resulta completamente difícil.

Este ecosistema, en el que participan múltiples actores sociales de orden público y privado que se relacionan de manera cotidiana para atender a la población migrante es complejo. No obstante, la piedra angular para su funcionamiento es la comunidad migrante venezolana y la información que esta -en su búsqueda de mejores condiciones socio-económicas y de integración- brinda a las diversas entidades territoriales o del orden nacional. Así mismo, este papel también es suplido en algunos casos por las organizaciones sociales que apoyan a las personas migrantes.

4.2 Precauciones a seguir por parte de las organizaciones sociales y personas migrantes en este ecosistema

En este ecosistema complejo las organizaciones que apoyan a la población migrante o las personas migrantes se encuentran compartiendo de manera constante información privada y sensible como su orientación sexual, su pertenencia racial o étnica, o -como hemos hablado en esta cartilla- sus datos biométricos. Como personas individuales que entregamos datos, o como organizaciones sociales que manejamos datos de otras personas debemos siempre tener presentes dos documentos que son fundamentales para el manejo de datos personales: la política de privacidad y el formato de consentimiento informado.

Como personas debemos asegurarnos de conocer la política de privacidad y de que se nos brinde un formato de consentimiento informado para garantizar que conocemos qué se hará con nuestros datos, quién tendrá acceso a ellos, y cómo se guardarán y si estamos o no de acuerdo con esta información. Como organizaciones que manejan datos personales de varias personas debemos asegurarnos siempre de tener una política de privacidad clara para que estas personas que nos confían sus datos entiendan qué se hará con ellos, y un formato de consentimiento informado para que nieguen o acepten el uso de su información personal.

Estos dos formatos deben siempre estar acorde con el artículo 15 de la Constitución Política de Colombia que sostiene en relación con los datos personales:

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

Así mismo, deben respetar la Ley estatutaria 1581 de 2012 a través de la cuál se brindan y establecen disposiciones generales para la protección de datos personales. A continuación, presentamos dos formatos de cada uno de estos documentos -que pueden ser modificados- y exponemos las secciones que deben contener.

4.2.1 Consentimiento informado

El consentimiento informado es un documento en el cuál se le informa a una persona en específico en qué consiste la recolección de sus datos personales, la participación en un taller o actividad específica desarrollada por una entidad, institución, ONG u organización. En este documento también se le brinda a la persona información sobre los objetivos, alcances y usos que se hará de la información recolectada directamente o en las actividades relacionadas. Esto se hace para que en este mismo documento la persona pueda manifestar de manera libre e informada si está de acuerdo o no con participar de las actividades o del proceso de recolección de la información.

Aunque el consentimiento informado es un requisito legal para la recolección de datos, es mucho más importante que cumplir con el requisito, el garantizar que las personas comprendan cuáles pueden ser las consecuencias de entregar los datos, en ese sentido, estos formatos deben ser sólo una guía para explicar a las personas las implicaciones de la recolección de sus datos.

FORMATO GUIA DE CONSENTIMIENTO INFORMADO

1. Presentación de los objetivos de la recolección de datos para los y las participantes

La siguiente recolección de datos se desarrolla en el marco de las actividades desarrolladas por ___ **(nombre de la organización/entidad/ong/etc)** ____ en el marco de ____ **(actividad que está realizando o realizará)** _____. El objetivo principal de este encuentro es ____ **(explicación clara del objetivo de la actividad)** _____.

La recolección de estos datos a través de esta actividad se realiza en respeto de y en conformidad con la Ley 1581 de 2012, el artículo 15 de la Constitución Política de Colombia y el Decreto 1377 de 2013.

¿Cuál es el objetivo de la actividad o de la recolección de datos?

El objetivo de esta actividad es _____ **(explicación mucho más clara y extensa del objetivo de la recolección de datos para la actividad que se busca realizar)**_____

2. ¿Qué espera de la actividad o de la recolección de datos? ¿Cómo será mi participación?

Aquí debe explicarse cuál es la actividad que se va a realizar, cuál es el papel de las personas cuyos datos se recolectan, y como organización/entidad/ong qué se va a hacer. Aquí también debe estar claro qué información se va a recolectar, de qué manera y en qué momento.

3. ¿Qué sucederá con la información recolectada durante de la actividad o del proceso de recolección de datos?

En este punto debe estar explicado de manera clara y detallada para qué se va a utilizar la información que se recolecta de las personas, quiénes van a tener acceso a ella y con qué motivo, quién va a almacenarla.

4. ¿Cómo se garantizará mi privacidad?

Aquí debe explicitar cómo se va a garantizar que se cumpla con el uso, almacenamiento y privacidad que se les dijo a las personas que iba a tener la información que se entregó. Aquí, van herramientas como: la anonimización de la información, el almacenamiento en bases de datos privadas, el acceso solo a determinados usuarios, entre otras medidas.

5. Consentimiento informado

Al continuar con la actividad usted confirma que entiende de manera clara la razón por la que este se realiza, cuáles son las actividades en las que participa y los usos que se le dará a la información que usted brinde en ellas.

También confirma que acepta de manera libre, informada y voluntaria lo consignado en este documento y que se encuentra de acuerdo con ello y con el posterior uso de la información recolectada por parte de _____ **(nombre de la institución, entidad, ong, etc)** _____, para ____**(el objetivo arriba mencionado)**____.

En caso de querer participar de manera libre, voluntaria e informada de este proceso y sus actividades, le invitamos a manifestar con un sí su aceptación a participar y a que su información sea recolectada y tratada como se manifiesta en este documento.

Nombre de la persona que participa _____
Tipo de identificación ___
Número de identificación _____
Firma _____

Acepto participar y que mi información se recolecte y se trate según lo consignado en este documento:
SI _____ **NO** _____.

4.2.2 Política de protección y tratamiento de datos personales

Las políticas de tratamiento de datos personales tienen como objetivo cumplir con el artículo 15 de la Constitución Política, lo reglamentado en la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, a través de la difusión de los principios que rigen la recolección, uso, manejo, tratamiento y almacenamiento de la información personal hecha por una entidad, organización o institución determinada.

También, en cumplimiento de la normativa mencionada, las políticas de tratamiento de datos deben explicitar los medios por los que las personas pueden solicitar la eliminación, corrección, rectificación o actualización de los datos que de ellos poseen estas entidades o revocar la autorización la persona brindó a estas para su uso.

Al igual que con el consentimiento informado, las políticas de protección y tratamiento de datos, aunque son un requisito legal para quienes recogen y tratan datos, lo verdaderamente importante son las buenas prácticas detrás de la política. De nada sirve un documento bien elaborado si no está acompañado por una conciencia de la importancia de los datos, una buena disposición para cumplir lo estipulado y las prácticas acordes a ello.

FORMATO GUIA DE POLÍTICA DE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

¿Quiénes somos? ¿Por qué tenemos una política de tratamiento de datos personales?

Aquí se debería presentar una descripción sobre la empresa/entidad/fundación, cuál es su misión, visión y objetivos.

En cumplimiento del artículo 15 de la Constitución Política, lo reglamentado en la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, y todas sus normativas y directrices asociadas, desde (nombre de la entidad, institución u organización) reconocemos el derecho a la privacidad, la intimidad, la dignidad de las personas, al igual que su derecho a rectificar, actualizar o revocar permisos de uso de su información personal. Por esta razón, adoptamos la siguiente política de tratamiento y protección de datos personales.

1. ¿Qué datos personales recolectamos?

En esta sección es necesario describir de manera clara y detallada cuáles son los datos personales que recolecta la organización, fundación, institución, etc.. Así mismo, debe explicitar a través de qué medios, canales y espacios realiza este proceso.

2. ¿Cuál es la finalidad de la recolección, uso y tratamiento de los datos personales que se recogen?

En esta sección es necesario describir de manera clara y detallada cuáles son los usos que se le brinda a la información que fue recolectada a través de los medios que se mencionaron anteriormente.

3. ¿Cuáles son los derechos de las personas que nos entregan sus datos o cuyos datos recolectamos?

1. Tiene derecho a conocer cuáles son los datos que tiene la fundación/organización sobre usted, para qué se utilizan y cómo estos se almacenan.

2. Actualizar o rectificar los datos que tenemos sobre usted en nuestras bases de datos.

3. Tiene derecho a que se eliminen sus datos personales de nuestra base de datos y a revocar la autorización que nos ha brindado para hacer uso de ellos.

4. Tiene derecho a solicitar pruebas de que usted nos otorgó autorización para recolectar, utilizar y almacenar sus datos personales. Salvo en aquellos casos en donde por ley, no es necesaria la autorización expresa del titular de los datos para realizar este tratamiento.

5. Cuando considere que sus datos personales no se están tratando acorde a los principios de la ley o que no se están respetando las condiciones iniciales a las que accedió para hacer el tratamiento de sus datos personales, tiene derecho a presentar la queja ante la entidad competente. Para este caso, la Superintendencia de Industria y Comercio (SIC).

4. ¿Quién o quiénes son los responsables del tratamiento de datos personales?

(Nombre del área o la entidad, organización, fundación) será el responsable del tratamiento de los datos personales y las bases de datos, puede enviar sus peticiones, consultas y reclamos a través de: xxxxxx@xxxxxx.com o en la dirección_____

*Aquí debe manifestarse quién es la persona, departamento o área responsable del manejo de los datos personales y se deben brindar datos que permitan comunicarse con esta en caso de que se requiera actualizar, consultar, verificar, o revocar permisos alrededor de los datos personales.

5. ¿Con quiénes podrá la fundación, organización o institución compartir la información recolectada?

*En este punto se nombran las entidades con las que se compartirá la información, así como la pertinencia, necesidad y legalidad que justifican este intercambio.

6. ¿Cuánto tiempo se planea conservar la información por parte de la entidad, organización, institución o fundación?

*En este punto debe explicitar por cuánto tiempo se tendrán almacenados y se utilizarán los datos personales recolectados. Así mismo, se explicará en qué caso y tiempo se eliminarán los datos.

Con las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial, o según las condiciones establecidas en el artículo 13 de la Ley 1581 de 2012.

7. ¿Cuál es la vigencia de la política de privacidad de datos personales?

*En este punto debe explicarse cuando se realizó esta política de recolección de datos personales, con que frecuencia se revisa y se ajusta, y a través de qué medios se le avisa a los usuarios sobre estos cambios.

4.3 Indicaciones generales sobre la acción de tutela

Esta sección de la guía fue elaborada por DeJusticia

4.3.1 ¿Qué es la acción de tutela?

Es un derecho y un mecanismo de protección, el cual puede ser interpuesto por cualquier persona cuando sus derechos fundamentales resulten vulnerados o amenazados por la acción u omisión de cualquier autoridad pública o de los particulares en los casos que señale la ley.

Se caracteriza por ser un mecanismo:

- **Subsidiario y excepcional:** solamente procede cuando no se disponga de otro mecanismo de defensa judicial, o salvo que se pretenda evitar una vulneración inminente a los derechos fundamentales. (Art. 6, # 1 del Decreto 2591 de 1991).
- **Inmediato:** su propósito es otorgar sin dilaciones la protección a la que haya lugar (Art. 18 del Decreto 2591 de 1991).
- **Sencillo:** no exige conocimientos jurídicos para interponerse (Art. 1 del Decreto 2591 de 1991).
- **Específico:** se creó como mecanismo especial de protección de los derechos fundamentales (Art. 1 del Decreto 2591 de 1991).
- **Eficaz:** siempre exige del juez un pronunciamiento de fondo, bien sea para conceder o negar la protección solicitada (Art. 1 del Decreto 2591 de 1991).

4.3.2 ¿Cuándo procede la acción de tutela?

- Cuando los derechos fundamentales de una persona o una comunidad han sido vulnerados o amenazados por la acción u omisión de una autoridad pública, o de un particular cuando presten servicios públicos. Cuando no existan otros mecanismos de defensa judicial de protección para garantizar la protección de los derechos fundamentales vulnerados o amenazados.
- O existiendo dicho medio ordinario, la acción se interponga como un mecanismo transitorio para evitar un perjuicio irreparable, entiéndase como perjuicio irremediable la amenaza grave e inminente de la violación del derecho fundamental.

4.3.3 ¿Quién puede presentar la acción de tutela?

Toda persona que considere vulnerado o amenazado uno de sus derechos fundamentales puede ejercer la acción de tutela en forma directa o a través de un tercero, quien actúe a su nombre, para reclamar ante cualquier juez de la república la protección inmediata de sus derechos.

4.3.4 ¿Cómo y ante quién se presenta una acción de tutela?

Esta acción se puede presentar de manera verbal o escrita, ante cualquier juez o tribunal donde ocurrió la vulneración o amenaza del derecho, y deberá incluir la siguiente información:

a. Los datos de identificación de quien presenta la tutela y del representante en caso de que la persona haya escogido tenerlo. Una narración de los hechos que lo llevaron a presentar la acción de tutela.
b. Señalar los posibles derechos vulnerados.
c. Identificar a la persona o entidad que ha cometido la amenaza o agravio contra los derechos fundamentales.
d. Plantear la solución que usted considere conveniente para proteger sus derechos.
e. Incluir la dirección física y/o electrónica para recibir la notificación judicial. Asegurar que no ha interpuesto una solicitud ante otra autoridad al mismo tiempo, para proteger los derechos vulnerados.

4.3.5 ¿Cuánto tiempo se demora el juez en resolver la acción de tutela?

Una vez presentada la acción de tutela, el juez analizará la situación y tomará una decisión dentro de los 10 días hábiles siguientes a la solicitud. De encontrar que realmente existe una amenaza o violación a los derechos fundamentales, dará órdenes expresas a los responsables para que se supere la situación y se protejan los derechos.

4.3.6 ¿Qué se puede hacer si la decisión del juez no le satisface?

Dentro de tres (3) días hábiles siguientes a la notificación de la decisión del fallo de tutela, se podrá presentar un escrito de impugnación, ante el mismo despacho que profirió la decisión, en la cual manifestará las razones de su inconformidad. Es suficiente con que la persona manifieste o escriba la palabra "impugno"

¡Ten en cuenta!

Para presentar una tutela:

- No se requiere de un abogado.
- El trámite es gratuito.
- No se pueden interponer dos acciones de tutela por los mismos hechos.

¡Importante!

- Si la decisión del juez no se cumple, o no se ejecuta en el tiempo indicado, el accionante puede acudir ante el mismo juez de primera instancia para presentar el incidente de desacato.
- En caso de requerir asesoría para presentar una tutela, existe la posibilidad de acudir a las Personerías Municipales, Defensoría del Pueblo, o Consultorios Jurídicos de las universidades que tengan programas de Derecho, quienes incluso pueden presentar la acción de tutela en nombre de cualquier persona que lo solicite o que esté en situación de desamparo o indefensión. Recuerde que este tipo de servicios prestados por estas instituciones son completamente gratuitos para todas persona que lo requiera, incluidas las personas migrantes en situación irregular.

4.3.7 ¿Dónde encontrar más información?

- Constitución Política de Colombia (artículo 86):
https://www.constitucioncolombia.com/titulo-2/capitulo-4/articulo-86
- Decreto 2591 de 1991 "Por el cual se reglamenta la acción de tutela consagrada en el artículo 86 de la Constitución Política"
https://www.suin-juriscol.gov.co/viewDocument.asp?id=1470723.
- Decreto 1983 del 30 de noviembre de 2017
https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30034333
- Defensoría del Pueblo: https://www.defensoria.gov.co/
- Personerías municipales

Fundación

Karisma