Bogotá, 23 de febrero de 2021

Claudia Blum
Ministra
Ministerio de Relaciones Exteriores

Juan Felipe Espinosa
Director
Unidad Administrativa Especial Migración Colombia

Lucas Gómez
Gerente de Fronteras
Presidencia de la República

República de Colombia

REF: Comentarios al Estatuto Temporal de Protección para Migrantes Venezolanos

Respetados Ministra, Director y Gerente,

La Fundación Karisma es una organización de la sociedad civil colombiana que busca responder a las amenazas y oportunidades que plantea la "tecnología para el desarrollo" al ejercicio de los derechos humanos, desde perspectivas que promuevan la libertad de expresión y las equidades de género y social. Trabajamos desde el activismo, incorporando múltiples miradas —legales y tecnológicas—.

Por medio de la presente queremos poner en consideración los siguientes comentarios sobre el Estatuto Temporal de Protección para Migrantes Venezolanos (ETPMV). En primer lugar, consideramos necesario reevaluar la relación entre el proceso de identificación y el proceso de caracterización que propone el borrador de decreto. En segundo lugar, es necesario detener el uso de biometría y especialmente el reconocimiento facial y de iris que hace parte de la vigilancia de la frontera. Finalmente, subrayamos la necesidad de garantizar la seguridad digital de todos los datos personales recopilados en el contexto de control migratorio.

Quedamos atentos al desarrollo del proceso de comentarios del ETPMV, a las respuestas a estos comentarios y a cualquier duda o aclaración que podamos resolver sobre ellos.

Cordialmente,

Carolina Botero
Directora

Juan Diego Castañeda
Coordinador de investigación

1. Confusión entre los procesos de registro, identificación y caracterización

El artículo 6[1] determina dos objetos para el RUMV que son (1) la recolección de información para la formulación de políticas públicas e (2) identificar a los migrantes que cumplen con las condiciones del artículo 4.

El artículo 8[2] impone como requisito para la inclusión en el registro el autorizar la recolección datos biográficos, demográficos y biométricos.

1.1 Riesgos de discriminación por confundir identificación con caracterización

El registro, la identificación y la caracterización demográfica son procesos diferentes. Los procesos de construcción o establecimiento de la identidad son unos procedimientos que comienzan con un registro en el cual una persona, confía ciertos atributos suyos a una autoridad para que estos sean validados y se determine su unicidad frente a otras personas. Una vez estos datos han sido validados con otras bases de datos, la autoridad competente emite una credencial con la que otras autoridades y personas puedan identificar a una persona. Con los procedimientos de autenticación se establece si una persona es quien dice ser[3].

Finalmente, la caracterización de una población se refiere a un proceso a través del cual se busca determinar las condiciones particulares que la distinguen en términos económicos, sociales, culturales, entre otros, o generar un diagnóstico sobre sus condiciones en un momento específico[4]. Siguiendo a la iniciativa de Identificación para el Desarrollo del Banco Mundial, la caracterización no hace parte de un sistema de

[1] **Artículo 6. Objeto del Registro Único de Migrantes Venezolanos Bajo Régimen de Protección Temporal.** Este Registro tendrá como finalidad recaudar y actualizar información como insumo para la formulación y diseño de políticas públicas, e identificar a los migrantes de nacionalidad venezolana que cumplen alguna de las condiciones establecidas en el artículo 4, y deseen acceder a las medidas de protección temporal contenidas en el presente Estatuto.
Parágrafo 1. La información contenida en el Registro no tendrá fines sancionatorios, salvo las excepciones que establezca la Unidad Administrativa Especial Migración Colombia en el acto administrativo mediante el cual se lleve a cabo su implementación, sin perjuicio del cumplimiento de las medidas impuestas por las autoridades judiciales o administrativas competentes.

[2] **Artículo 8. Requisitos para ser incluido en el Registro.** Para ser incluido en el Registro, el migrante venezolano deberá cumplir los siguientes requisitos: (...) **5.** Autorizar la recolección de sus datos biográficos, demográficos y biométricos.

[3] World Bank Group, & Identification for Development. (2016). Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. World Bank Group.

[4] Gallo, N., Meneses, Y. Y Minotta, C. (2014). "Caracterización poblacional vista desde la perspectiva del desarrollo humano y el enfoque diferencial". Revista investigación y desarrollo vol 22 (2). http://dx.doi.org/10.14482/indes.22.2.5595

identidad, sino que la identidad es el medio para iniciar procesos de caracterización de la población que no implica formas de individualización[5].

En relación con estas definiciones, es posible establecer varios puntos. Primero, la caracterización demográfica funciona a nivel de poblaciones, no de individuos. El artículo 6 del ETPMVV la define como la recopilación de información sobre las personas migrantes de Venezuela para la formulación de políticas públicas. Segundo, la identificación es un proceso que opera a nivel individual mientras que la caracterización requiere solo información agregada y anonimizada para tomar decisiones de política pública. De ahí la necesidad de que el ETPMV aclare mejor los distintos elementos de registro, identificación y caracterización que lo componen.

El ETPMV no excluye la recolección de datos sensibles dentro de los datos demográficos. El numeral 5 del artículo 8 impone a las personas migrantes de Venezuela autorizar la recolección de datos biográficos, demográficos y biométricos, y se encarga a la UAE Migración Colombia determinar concretamente qué datos estarán obligados a entregar los migrantes. La falta de definiciones permite que en la implementación del RUMV se obligue a entregar datos sensibles como origen racial o étnico, orientación política, convicciones religiosas o filosóficas, afiliación política, pertenencia a sindicatos, organizaciones sociales, de derechos humanos o datos de salud y vida sexual. Como lo reconoce la Ley de Protección de datos (Ley 1581 de 2012) en su artículo 5, los datos sensibles requieren un nivel elevado de protección, y su tratamiento se prohíbe por regla general salvo excepciones específicas.

Por su naturaleza, la información para la caracterización puede generar discriminación. El tipo de datos que pueda solicitarse en el proceso de inclusión en el RUMV junto con el proceso de identificación puede permitir la discriminación de personas tal y como lo advierte el artículo 5 de la Ley de Protección de Datos. El resultado discriminatorio proviene del diseño del RUMV que permite unir la identidad de una persona con información sobre sus condiciones sociales, políticas, educativas o de salud, entre otras. Las autoridades entonces no deberían configurar la identidad legal de una persona a partir de información que puede usarse para fines discriminatorios.

Por ejemplo, usar números de identificación que por su construcción indican más información sobre la persona puede resultar en discriminación. En Sudáfrica hasta finales de los años ochenta, el número de identificación se construía para indicar el género, ciudadanía o residencia y la raza de la persona[6]. La Relatora Especial de las Naciones Unidas sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y

[5] World Bank Group & Identification for Development. (2019). ID4D Practitioner's Guide. World Bank Group.

[6] ID Enabling Environment Assessment : Guidance Note (English). Identification for Development Washington, D.C. : World Bank Group.
http://documents.worldbank.org/curated/en/881991559312326936/ID-Enabling-Environment-Assessment-Guidance-Note

formas conexas de intolerancia señaló que la recopilación y análisis de grandes cantidades de datos tuvo consecuencias discriminatorias e incluso letales durante el régimen de la Alemania Nazi, el genocidio en Rwanda o en la persecución de personas de estados árabes por autoridades de Estados Unidos luego de los ataques del 11 de septiembre de 2001[7].

En Ruanda, las tarjetas de identificación con información étnica fueron introducidas durante el gobierno colonial belga, además de recolectar sus datos biográficos, el sistema permitía conocer la etnia de esta persona. Con los estereotipos y violencias en el país, la existencia de una tarjeta de identificación étnica facilitó el asesinato masivo, pues era utilizada para identificar la etnia del portador y sus zonas de residencia[8].

En Estados Unidos, después del 11 de septiembre, el programa de Registro de Entrada y Salida de Seguridad Nacional (NSEER), desarrolló la primera base de datos biométrica para viajeros[9]. El proceso designó a personas de ciertas nacionalidades, como Irán, Irak, Libia, Sudán y Siria, que compartían ciertos criterios como un riesgo para la seguridad nacional. En el registro, se recogieron los datos biométricos del individuo (huella digital y patrones faciales), junto con información biográfica detallada. El programa fue reemplazado por U.S. - VISIT por funcionar con categorías en clave de nacionalidad y raza[10].

Cuando hay información sobre la pertenencia a un grupo identitario o religioso esto puede alterar el juicio del observador de la credencial. Como mínimo, la presencia de categorías de clasificación crea y refuerza una mayor conciencia de las diferencias grupales[11]. Además, cuando estos grupos son socialmente marginalizados, se están perpetrando diferentes violencias, ya que puede darse un proceso de “marcación”.

---

[7] Achiume, T., & Relatoría Especial sobre las formas contemporáneas de racismo, discriminación racial, xenophobia y formas conexas de intolerancia de las Naciones Unidas. (2020). A/75/590 Reporte de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenophobia y formas conexas de intolerancia (párrafo 11) Este informe continúa el análisis iniciado por la Relatora Especial en su informe más reciente al Consejo de Derechos Humanos: Discriminación racial y tecnologías digitales emergentes: un análisis de derechos humanos, en que introdujo un enfoque basado en la igualdad para la gobernanza de los derechos humanos de las tecnologías digitales emergentes, con un enfoque en la discriminación racial resultante del diseño y uso de estas tecnologías. En la presentación de es estos informes la relatora instó a los actores estatales y no estatales a ir más allá de las estrategias "daltónicas" o "raciales" que ignoran el impacto racial y étnico de las tecnologías digitales emergentes haciendo un llamado claro a confrontar directamente las formas interseccionales de discriminación que resultan y se agravan por la adopción generalizada de estas tecnologías.(párrafo 1).

[8] Fussell, J. (2001). Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing. Prevent genocide international. http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/

[9] Epstein, C. (2007). Guilty bodies, productive bodies, destructive bodies: Crossing the biometric borders. International Political Sociology, 149–164.

[10] Íbid.

[11] Fussell, J. (2001). Op. Cit.

1.2 Riesgos al principio de finalidad en el tratamiento de datos

Los datos personales recolectados deben ser los estrictamente necesarios y proporcionales para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate. La Ley de Protección de Datos establece que el tratamiento de datos debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley (Art. 4 lit. b). La Corte Constitucional aclaró además que debe limitarse el tratamiento de datos personales al mínimo necesario respecto al objetivo de la base de datos donde se quieren incluir. Los datos solicitados deben ser adecuados, pertinentes y acordes con los fines de la base de datos[12]. Estos deberes están enmarcados en el respeto y garantía que están obligados a observar y promover los Estados en la recopilación, procesamiento y almacenamiento, entre otras formas de tratamiento de datos biométricos tal y como lo destaca la Asamblea General de las Naciones Unidas[13].

En su redacción actual, el parágrafo 1 del artículo 6 y el numeral 5 del artículo 8 exigen datos personales en su mayoría sensibles para propósitos diversos. Además de que no cumplen con el principio de finalidad de la Ley de Protección de datos, esta confusión puede implicar riesgos graves para la dignidad, intimidad e igualdad de las personas migrantes venezolanas.

Incluso para la producción de credenciales de identificación, la solicitud de datos biográficos puede tener resultados discriminatorios y no es útil para los fines de identificación.[14] Como establece la Ley de Protección de Datos, cuando el tratamiento tenga una finalidad estadística, como lo es por naturaleza el levantar información para el diseño de políticas públicas, es necesario adoptar las medidas para suprimir la identidad de los titulares de los datos (Art. 6 literal e). El ETPMV no establece ninguna medida para cumplir con este mandato legal en la construcción del RUMV.

Los datos biográficos y biométricos no son adecuados, pertinentes ni acordes para la recolección de información para el diseño de políticas públicas. El artículo 6 establece que uno de los fines del RUMV es generar insumos para formular políticas públicas. Sin embargo, no es necesario tener información sobre la identidad de un individuo en particular en relación con sus características demográficas o biográficas para diseñar políticas públicas. Dado que las acciones de gobierno no pueden dirigirse a personas concretas, la información de identificación no debe hacer parte del instrumento de caracterización de la población migrante que en el ETPMV está confundidas en el RUMV.

[12] Corte Constitucional. Sentencia C-748 de 2011. Sección 2.6.5.2.2.

[13] Asamblea General de las Naciones Unidas. Resolución aprobada por la Asamblea General el 17 de diciembre de 2018. “El derecho a la privacidad en la era digital”. A/RES/73/179. https://undocs.org/es/A/RES/73/179

[14] World Bank Group & Identification for Development. (2019). *ID4D Practitioner’s Guide*. World Bank Group.

Distinguir claramente la finalidad de las bases de datos y separarlas cuando haya finalidades diversas mejora la garantía que ofrece el principio de finalidad[15]. Unir o interoperar bases de datos con fines diferentes es un riesgo para el derecho a la protección de datos y la privacidad. En 2010, la Comisión Europea explicó que la idea de un sistema de intercambio de información comprensivo y que sirviera múltiples propósitos va en contra de la compartimentalización de la información con la que se han desarrollado los sistemas migratorios a esa fecha. Esos silos de información son más adecuados para la protección de los derechos a la privacidad y la protección de datos de las personas. Estas protecciones han sido erosionadas por los Reglamentos (UE) 2019/817 y 2019/818 que permiten el uso de los sistemas de información de migrantes que ya existían como "módulos" para alimentar otros sistemas nuevos.[16]

1.3 Riesgos al derecho a la igualdad entre nacionales de Venezuela y todas las demás nacionalidades

La unificación de procesos de caracterización e identificación legal no se hace con personas nacionales colombianos o de otras nacionalidades, sino solo se haría con migrantes de nacionalidad venezolana en condición de vulnerabilidad. Así, la constitucionalidad de este artículo debe ser examinada, pues implica un tratamiento discriminatorio de las personas migrantes.

La discrecionalidad del Estado para decidir el ingreso y permanencia de personas no colombianas no es ilimitada. El artículo 100 de la Constitución establece que los extranjeros gozarán de las mismas garantías que tienen las personas de nacionalidad colombiana. Si bien se reconoce la posibilidad de que haya diferencias en el ejercicio de sus derechos, esto no puede significar el desconocimiento de sus derechos fundamentales[17].

El RUMV impone límites injustificados al derecho a la intimidad y protección de datos de personas migrantes de Venezuela. El diseño del RUMV obliga a los migrantes de Venezuela a entregar los datos biográficos, demográficos y biométricos que defina la UAE Migración Colombia como requisito para producir su identidad legal. Para los nacionales colombianos, en cambio, la función de producción de identidad la lleva la Registraduría Nacional del Estado Civil mientras que la información para la caracterización demográfica está sectorizada o está a cargo del Departamento Administrativo de Estadística. Además, esta intromisión injustificada en la intimidad de los migrantes venezolanos sólo aplica para este grupo en función de su nacionalidad. A ninguna otra nacionalidad en Colombia

[15] Corte Constitucional. Sentencia C-748 de 2011. Sección 2.6.5.2.2.
[16] Jones, C. (2019). Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status. Platform for International Cooperation on Undocumented Migrants and Statewatch. https://picum.org/publications/
[17] Corte Constitucional. Sentencia C-1259 de 2001.

se le exige la entrega de los datos mencionados en el numeral 5 del artículo 8 para la producción de su identidad legal.

1.4 Riesgos al principio de libertad en el tratamiento de datos

La recolección de datos demográficos para obtener el Permiso por Protección Temporal (Artículo 8 numeral 5) puede ir en contra del principio de libertad establecido en la Ley Protección de Datos (Ley 1581 de 2012) pues las personas migrantes de Venezuela están sujetas a las condiciones que imponga el gobierno colombiano ya que migran en razón de una "crisis política, social y económica (...) agudizada y prolongada en el tiempo" (considerandos del ETPMV).

Las personas migrantes de Venezuela están en condiciones de extrema vulnerabilidad. En la presentación del ETPMV el Presidente Iván Duque califica la migración de muchas personas de Venezuela como una "huída" de las condiciones de pobreza de ese país[18]. El documento CONPES 3950 de 2018 parte de que la crisis migratoria tiene que ver con la salida de nacionales de Venezuela debido a "la difícil coyuntura económica, política y social"[19]. El mismo ETPMV en sus considerandos señala que la crisis política, social y económica por la que atraviesa Venezuela se ha prolongado en el tiempo. Esta calificación sistemática de la migración venezolana, incluso por diversos actores internacionales[20], como una huída resalta la condición de especial vulnerabilidad en la que se encuentran las personas migrantes afectadas por el ETPMV.

Las personas migrantes no están en posición de consentir libremente a la recolección de datos. La Relatora Especial de las Naciones Unidas sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia ha señalado que Los gobiernos experimentan con personas migrantes tecnologías de control de fronteras. las personas migrantes no están en condiciones para negarse al tratamiento de sus datos personales y pocos recursos para impugnar. Esto significa que terminan siendo objeto de las políticas experimentales de identificación porque aceptan cualquier obligación que imponga un gobierno para recibirlos y todo esto ocurre en función de su origen nacional y su situación migratoria[21]. Por ello, la recolección de datos de personas migrantes, especialmente en contextos caracterizados por grandes diferencias de poder,

[18] El Espectador. (8 de febrero de 2021). *Estatuto Temporal de Protección: El plan para regularizar migrantes venezolanos en Colombia*. https://www.youtube.com/watch?v=0UwZN-i5Koc

[19] Documento CONPES 3950 de 2018.

[20] World Report 2021: Rights Trends in Venezuela. (15 de diciembre de 2020). Human Rights Watch. https://www.hrw.org/world-report/2021/country-chapters/venezuela

[21] Achiume, T., & Relatoría Especial sobre las formas contemporáneas de racismo, discriminación racial, xenophobia y formas conexas de intolerancia de las Naciones Unidas. (2020). A/75/590 Reporte de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenophobia y formas conexas de intolerancia. (Párrafos 34 y 38)

"plantea problemas relacionados con el consentimiento informado y la posibilidad de optar por no aportar datos"[22].

Algunas situaciones en los que los migrantes no se encuentran en la posibilidad de negar o consentir libremente el tratamiento de sus datos personales se pueden observar en los contextos humanitarios de varios países africanos, en donde el derecho al tratamiento de datos personales se ve opacado por la necesidad inminente de comida, refugio o atención médica[23]. En Zimbabue, por ejemplo, a pesar de una desconfianza ampliamente marcada hacia el gobierno y una falta de socialización sobre los objetivos de la recolección de datos, las poblaciones precarizadas y rurales, en especial granjeros alejados de los centros urbanos, entregaban sus datos para "sobrevivir y no morir de hambre"[24].

En consecuencia, la manera en la que se otorga el consentimiento para la recolección y tratamiento de datos personales en estos contextos puede no ser considerada del todo como libre y puede estar condicionada por las necesidades de una población en condición de vulnerabilidad que migra o que se encuentra en condiciones precarizadas. El consentimiento brindado por la necesidad no garantiza un conocimiento de aquello a lo que se está consintiendo, los derechos que se tienen frente a esa información o las implicaciones o usos posteriores que puede tener la información suministrada. Por eso, se deben pensar alternativas que consideren las dinámicas de poder que existen entre el Estado y poblaciones con alta vulnerabilidad, y que procuren instancias más colaborativas y cercanas con los migrantes.

Además de desafiar el principio de libertad estipulado por la Ley de Protección de datos, el consentimiento otorgado por personas migrantes en un contexto de necesidad y vulnerabilidad extrema, puede afectar la validez de cualquier autorización al tratamiento de datos personales. El artículo 3 de la Ley de Protección de datos requiere un consentimiento previo, expreso e informado por parte del titular para el tratamiento de sus datos personales. Toda noción de consentimiento implica elección y control reales por parte de los titulares. El Grupo de Trabajo del Artículo 29 en Europa[25] ha subrayado en opiniones sucesivas que el consentimiento por parte de un titular no puede ser considerado libre – y por ende, legítimo – si el titular no puede negar o retirar su consentimiento sin perjuicio[26].

---

[22] Ibíd.

[23] Baker, S. y Rahman, Z. (2019). "Digital ID in Ethiopian refugee camps: A case study". The engine room. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Ethiopia%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf

[24] Baker, S. (2019). "Digital ID in Zimbabwe: A case study".The engine room. https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf

[25] Grupo de Trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales previa la entrada en aplicación del Reglamento General de Protección de Datos (UE).

[26] Grupo de Trabajo del Artículo 29. (2018). WP259 Directrices sobre el consentimiento en el sentido del reglamento (UE) 2016/679.

1.5 Riesgos de discriminación al permitir sanciones por información en el RUMV

El RUMV propuesto en el ETPMV quedaría administrado por la entidad encargada de la vigilancia y control migratorio. El uso de información demográfica para fines sancionatorios queda al arbitrio de la misma entidad y sin salvaguardias para impedir usos discriminatorios.

La UAE Migración Colombia no es la entidad encargada de la construcción de políticas públicas que beneficien a las personas migrantes y en cambio ejerce funciones de seguridad nacional, control y verificación migratoria. Entre sus funciones se encuentran la inadmisión de personas que ingresan al país, la verificación del estatus migratorio de las personas extranjeras y la expulsión de personas que "a juicio de la autoridad migratoria realicen actividades que atenten contra la seguridad nacional, el orden público, la salud pública, la tranquilidad social la seguridad pública"[27].

Así mismo, la entidad cuenta con convenios interadministrativos con la Policía Nacional para el intercambio seguro y confidencial de información y en los que se sostiene que la Policía Nacional -en aras de salvaguardar el orden público y la soberanía nacional- "brindará apoyo y acompañamiento operativo permanente a migración Colombia en el desarrollo de sus labores en los puestos de control migratorio, ubicados a los largo del territorio nacional cuando Migración Colombia lo requiera"[28].

Estas funciones de seguridad y los convenios que tienen las entidades migratorias con entidades policiales y legales ha creado cierta preocupación. En el caso de Europa, el acceso de las entidades policiales y legales a las bases de EURODAC, han extendido la preocupación entre organizaciones de derechos humanos de que este acceso pueda estigmatizar a los solicitantes de asilo haciéndolos blanco de más investigaciones criminales y averiguaciones, debido a que sus datos biométricos se encuentran disponibles para investigaciones criminales[29].

1.6. Conclusiones y solicitudes

Los artículos 6 y 8 definen los dos objetivos del Registro Único de Migrantes Venezolanos (RUMV) que incluye la recolección de información para la construcción de política pública y la identificación de migrantes venezolanos. De esta forma, el RUMV unifica la caracterización demográfica con la identificación legal de las personas migrantes de nacionalidad venezolana en un solo sistema y que tiene por administradora a una sola

[27] Ministerio de Relaciones Exteriores. Decreto 1067 de 2015.

[28] Unidad Administrativa Especial de Migración Colombia, Resolución 2821 de 2014

[29] Roots, L. (2015). "The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination". Baltic Journal of European Studies Tallinn University of Technology 5, 2(19).

entidad con poderes de policía migratoria. Igualmente, el parágrafo del artículo 6 deja abierta la posibilidad de que Migración Colombia como encargada de la vigilancia y control migratorio utilice los datos de caracterización para fines sancionatorios. Con esto, se generan los siguientes problemas:

1. El decreto confunde tres procesos diferentes y los unifica: el registro, la identificación y la caracterización demográfica. Es decir, la identificación es un proceso individual y la caracterización es poblacional que utiliza información agregada y anonimizada. El Registro recogería datos sensibles y los ligaría a la identidad de una persona. Este tipo de sistemas pueden generar discriminación y graves violaciones de derechos humanos. Como se ha visto en múltiples casos internacionales y en las advertencias de relatorías de derechos humanos ante las Naciones Unidas.
2. El decreto no cumple con el principio de finalidad de la Ley de Protección de Datos y esta confusión puede implicar riesgos graves para la dignidad, intimidad e igualdad de las personas migrantes venezolanas. Los datos personales que se podrían recolectar para hacer la caracterización son sensibles y tienen finalidades diferentes. Es decir, los datos biográficos y biométricos no son adecuados, pertinentes ni acordes para el diseño de políticas públicas y los datos de caracterización no lo son para la identificación. Precisamente, la separación de la información en silos es una forma de protección.
3. El RUMV impone límites injustificados al derecho a la intimidad y protección de datos de personas migrantes de Venezuela que no se aplican para personas de otras nacionalidades cuando se unifica la caracterización con la identificación en una sola institución y en un solo sistema.
4. El decreto limita el derecho a la intimidad y la protección de datos de las personas migrantes de Venezuela que están en condiciones de extrema vulnerabilidad, pues no están en posición de consentir libremente a la recolección de datos. Además de desafiar el principio de libertad estipulado por la Ley de Protección de datos, el consentimiento otorgado por personas migrantes en un contexto de necesidad y vulnerabilidad extrema, puede afectar la validez de cualquier autorización al tratamiento de datos personales.
5. El decreto crea un solo sistema que recolecta datos personales de todo tipo de migrantes en condición de vulnerabilidad y quedaría administrado por la entidad encargada de la vigilancia y control migratorio con facultades policivas. El uso de información demográfica para fines sancionatorios queda al arbitrio de la misma entidad y sin salvaguardias para impedir usos discriminatorios.

Por todo lo anterior, solicitamos:

1. Diferenciar con claridad los procesos de registro, identificación y caracterización de personas migrantes venezolanas. Esto implica también lo siguiente:
2. Determinar con claridad qué datos se requieren recolectar para la inclusión de estas personas en el registro, para la producción del Permiso de Protección

Temporal como credencial de identificación y para hacer la caracterización a nivel de población de estas personas.

3. La información para la caracterización de la población migrante venezolana no puede estar atada a los datos biográficos y biométricos de cada migrante que hace el registro con miras a la obtención del PPT.
4. La información de caracterización demográfica de las personas migrantes debe ser recolectada y administrada por una autoridad diferente a la que está a cargo de la identificación y verificación migratoria como Migración Colombia. Esta separación de la información de caracterización ya se hizo en el Registro Administrativo de Migrantes Venezolanos que administró la Unidad Nacional para la Gestión del Riesgo (Decreto 542 de 2018). Otra opción es que la administración siga los lineamientos para nacionales cuyos datos de caracterización son administrados por Departamento Administrativo Nacional de Estadística.
5. Realizar una evaluación de la necesidad y proporcionalidad de (1) la recolección, (2) el análisis y (3) el almacenamiento de cada dato en relación con los fines diferenciados de registro, identificación o caracterización. Además se debe determinar si no hay formas alternativas y menos invasivas para conseguir los mismos resultados. Esta evaluación debe ser hecha antes del procesamiento de datos personales y debe informar el diseño y la aplicación del RUMV con relación a los riesgos y estrategias de mitigación. Esta evaluación debe ser pública.
6. Una vez se haya determinado la necesidad y proporcionalidad de tratamiento de cada dato para cada una de las tres finalidades, es fundamental desarrollar una estrategia de compartimentalización para garantizar que los datos tratados para una finalidad específica no sean tratados para otra finalidad de forma innecesaria o encubierta.
7. Hacer una evaluación de impacto en derechos humanos de la implementación de requisitos para la identificación, registro y caracterización diferenciados entre nacionales colombianos, venezolanos y otras nacionalidades. Esta evaluación debe ser hecha antes de procesar con el procesamiento de datos personales y debe informar el diseño y la aplicación del RUMV con relación a los riesgos y estrategias de mitigación. Se debe hacer pública esta evaluación.
8. Las distinciones entre nacionales y extranjeros deben obedecer a criterios estrictos de legalidad, necesidad y proporcionalidad. El ETPMV debe eliminar los requisitos que no se puedan justificar luego de un análisis a partir de estos criterios.
9. Teniendo en cuenta la imposibilidad en la que se encuentran las personas migrantes venezolanas para negarse a la entrega de datos personales a autoridades colombianas para los trámites de registro e identificación (art. 8 num 5), se debe evaluar qué datos biográficos y biométricos son estrictamente necesarios para cumplir los fines de dichos trámites y sean utilizados solamente por la(s) finalidad(es) incluidas en el Decreto. Esta evaluación debe ser hecha antes de iniciar con el procesamiento de datos personales y debe informar el diseño y la aplicación del RUMV con relación a los riesgos y estrategias de mitigación. Esta evaluación debe ser pública.

10. Para fines de caracterización de la población migrante venezolana, en tanto tiene fines estadísticos propios del diseño e implementación de políticas públicas se debe respetar y asegurar el cumplimiento del requisito de anonimización del artículo 6 literal e) de la Ley de Protección de Datos.
11. Para fines de registro e identificación de personas migrantes venezolanas, se debe prohibir la recolección de datos sensibles de acuerdo con la definición del artículo 5 de la Ley de Protección de Datos.
12. Se debe reconocer expresamente las asimetrías de poder que existen entre las personas migrantes de Venezuela y las autoridades colombianas como la base para determinar los datos personales que se obligue a entregar para realizar los procesos de registro e identificación.
13. Los datos de caracterización de la población migrante venezolana para fines de diseño e implementación de políticas públicas no puede tener fines sancionatorios como lo permite la redacción actual del parágrafo 1 del artículo 6.

2. Falta de necesidad y proporcionalidad al permitir sanciones por no actualizar datos en el RUMV

El artículo 9[30] obliga a las personas migrantes inscritas en el RUMV a actualizar sus datos so pena de sanción administrativa.

En el marco de los comentarios anteriores respecto a la necesidad de separar la identificación de la caracterización de personas migrantes de Venezuela, notamos que el artículo 9 del ETPMV hace responsables a estas personas de mantener la actualización de sus datos personales. Teniendo en cuenta que el ETPMV no trae una definición calra de datos "biográficos, demográficos y biométricos", no es clara la razón de ser del deber de actualizar constantemente estos datos. Es necesario entonces especificar los datos que se exigirán como "biográficos, demográficos y biométricos" para evaluar la necesidad de actualizar constantemente estos datos.

En segundo lugar, el objetivo del RUMV es obtener información para el desarrollo de políticas públicas. Debido a que estas políticas no cambian cada vez que una persona actualiza sus datos biográficos, demográficos y biométricos, el artículo 9 impone una carga desproporcionada sobre las personas migrantes en dos sentidos: (1) en su condición de vulnerabilidad deben dedicar tiempo a trámites burocráticos de actualización

[30] **Artículo 9. Actualización de la información del Registro.** Toda persona incluida en el Registro Único de Migrantes Venezolanos Bajo Régimen de Protección Temporal, tendrá la obligación de actualizar sus datos tan pronto se presente un cambio en la situación o información registrada inicialmente, a través de los mecanismos que defina la Unidad Administrativa Especial Migración Colombia, so pena de las sanciones administrativas a que haya lugar.
Parágrafo. La Unidad Administrativa Especial Migración Colombia, podrá efectuar jornadas periódicas de actualización de datos cuando lo requiera, para lo cual definirá los parámetros e instrucciones para llevar a cabo dicha actualización.

innecesaria de datos que no cambian y (2) se castiga a las personas migrantes por las fallas que pueda presentar los sistemas de la UAE Migración Colombia para la actualización de los datos. Adicionalmente, esta obligación invierte el deber del administrador de la base de datos de mantener actualizada la información, tal y como establece el principio de veracidad y los artículos 17 y 18 de la Ley de Protección de Datos.

Por todo lo anterior, solicitamos:

1. El artículo 9 debe ser eliminado teniendo en cuenta la falta de definición de los términos "datos biográficos, demográficos y biométricos" y la confusión entre los procesos de registro, identificación y caracterización.
2. Conservar la carga burocrática de la actualización de datos que impone el artículo 9 debe ir acompañada de una evaluación de la necesidad de dicha actualización de acuerdo con una definición clara de los datos que harán parte del RUMV.
3. Cualquier deber de actualización de datos que se imponga en las personas migrantes venezolanas debe ser el resultado de una evaluación de la necesidad y proporcionalidad de esta obligación respecto a cada dato que las autoridades colombianas requieran y para cada forma de tratamiento y finalidad.

3. Recolección forzada de datos biométricos

El numeral 5 del artículo 8 del ETPMV exige a las personas migrantes venezolanas autorizar la recolección de sus datos "biográficos, demográficos y biométricos"[31] para inscribirse en el RUMV y en consecuencia, para recibir el Permiso por Protección Temporal.

En esta parte describimos los riesgos para los derechos humanos de las personas migrantes venezolanas derivados de la recolección de datos biométricos en particular.

3.1 Riesgos de discriminación y la dignidad al considerar los sistemas de reconocimiento facial contratados

En noviembre de 2020, la Unidad Administrativa Especial Migración Colombia suscribió el contrato 106 de 2020 con la empresa Bytte S.A.S por más de 14 mil millones de pesos para implementar un sistema que permita el registro, consulta, cotejamiento y gestión de la identidad biográfica, demográfica y multibiométrica (facial, dactilar e iris) de los migrantes venezolanos que se encuentran en territorio colombiano. De acuerdo con la documentación del contrato, el objetivo del contrato es el diseño de un sistema para la recolección de datos biométricos como el rostro para poder identificar a las personas que

[31] Artículo 8. Requisitos para ser incluido en el Registro. Para ser incluido en el Registro, el migrante venezolano deberá cumplir los siguientes requisitos: (...) 5. Autorizar la recolección de sus datos biográficos, demográficos y biométricos.

pasan la frontera de forma automática con cámaras ubicadas en la zona de frontera[32]. Igualmente, el sistema que se contrató debe ser capaz de buscar la imagen del rostro alojada en la base de datos con imágenes extraídas de un video o de una fotografía [33]. Así mismo, el sistema debe ser capaz de utilizarse en entornos con múltiples personas para identificar de forma simultánea hasta 30 personas y generar alertas por personas no registradas o no reconocidas por el sistema[34]. Además, el sistema debe funcionar con una aplicación móvil de verificación migratoria que los oficiales de Migración Colombia puedan identificar y consultar los antecedentes administrativos y judiciales de una persona usando la cámara de sus dispositivos[35].

El requisito de recolección de datos biométricos en el contexto del contrato firmado implica la creación de un sistema de vigilancia masiva y discriminación centrado en las personas migrantes provenientes de Venezuela y que, por su estatus migratorio, se encuentran en condición de vulnerabilidad. Como lo ha explicitado el gobierno colombiano, las personas que llegan provenientes de Venezuela huyen de una crisis social, económica y política. Así mismo, como han resaltado el Banco Internacional de Reconstrucción y Fomento, los movimientos actuales de migrantes comparten características con las crisis de refugiados que se han presentado en otros países, principalmente por la llegada acelerada de personas en condiciones de vulnerabilidad socioeconómica altas[36].

Por esto, las personas que serían inscritas al estatuto son las personas en claras condiciones de vulnerabilidad que pueden presentar diversas complicaciones para acceder a otras formas de regularización migratoria y que son clasificadas como sujetos de especial protección constitucional. En ese sentido, el decreto debe estar en línea con la idea de protección al migrante y no ser una herramienta para ejercer violencia sobre estas personas. EL RUMV no puede ser utilizado como un sistema de vigilancia que trate de identificar a las personas en múltiples espacios como una forma de determinar si una persona es o no “confiable” para el Estado. Es decir, la identificación de migrantes no puede exigirse con fines o por razones discriminatorias ni para fines de hostigamiento. Un sistema de identidad debe proteger el derecho a la defensa, el debido proceso, la presunción de inocencia y la libertad, entre otros derechos y garantías fundamentales.

En varios contextos, los datos de identificación o acceso a derechos terminan en sistemas de vigilancia masiva que discrimina ciertas poblaciones. Los Estados recogen datos para identificación en casos específicos que terminan en vigilancia, argumentando usos o

[32] Migración Colombia. Contrato No. 106 de 2020, p. 17

[33] Migración Colombia. Estudios Previos del Proceso de Licitación Pública No. 03 de 2020, p. 19

[34] Ibíd., p. 19

[35] Ibíd., p.p. 14-15

[36] Banco Internacional de Reconstrucción y Fomento/Banco Mundial (2018). Migración desde Venezuela a Colombia: impactos y estrategia de respuesta en el corto y mediano plazo, p.13.

necesidades de seguridad nacional[37]. Por ejemplo, en la provincia de Xinjiang en China, las bases de datos biométricas creadas para otorgar identidad legal se utilizan para vigilar y ejercer violencia contra la minoría Uyghur. Esta base de datos contiene fotos, ADN, iris, patrones de voz y las diez huellas dactilares. El sistema de identidad es utilizado por la Policía para identificar automáticamente personas en las cámaras de reconocimiento facial colocadas en las ciudades principales tanto privadas como públicas[38]. Los Uyghur solo pueden circular por algunas zonas y, cuando se alejan más de 300 metros, el sistema informa a las autoridades[39]. Igualmente, sitios públicos como las estaciones de servicio, los centros comerciales, los edificios públicos, los mercados y las estaciones de tren tienen puntos de control que autentican a las personas y recogen datos de su comportamiento diario incluyendo localización, hora, frecuencia y razones de visita [40].

En India, los datos biométricos de extranjeros y minorías se utilizan para la detención y deportación de minorías "no deseadas" incluyendo refugiados víctimas de violencia étnica como los Rohingya[41]. En Europa, las personas que buscan refugio mencionan la degradación que implica la recolección de datos biométricos y la violencia que reciben por parte de la policía migratoria que trata de identificarlos sin su consentimiento y sin justificación[42]. En Nueva Zelanda, experimentan con tecnologías de reconocimiento facial para identificar "futuras personas problemáticas" lo que ha llevado a organizaciones civiles a demandar el sistema [43].

---

[37] UNHCR. (2018). UNHCR Strategy on Digital Identity and Inclusion. https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf.

[38] Ver: The Economic Times. (27 August 2018). Aadhaar verdict: Legal, but limit use to government benefits, says Supreme Court. The Economic Times. https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-legal-butlimit-use-to-government-benefits-says-supreme-court/articleshow/65973337.cms? from=mdr
y Zand, B. (26 June 2018). A Surveillance State Unlike Any the World Has Ever Seen. Der Spiegel. http://www.spiegel.de/international/world/china-s-xinjiangprovince- a-surveillance-state-unlike-any-the-world-has-ever-seen-a-1220174.html

[39] Ver: Bloomberg (17 January 2018). "China Uses Facial Recognition to Fence In Villagers in Far West." *Bloomberg News*. https://www.bloomberg.com/news/articles/2018-01-17/china-said-to-test-facial-recognition-fence-in-muslim-heavy-area. y Chin, J, and C Bürge (19 December 2017). "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life." *The Wall Street Journal*, December 19, 2017. https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355.

[40]Ver: The Economist (31 May 2018). "China Has Turned Xinjiang into a Police State like No Other." *The Economist*. https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other
y Millward, J. (2 March 2018) "What It's Like to Live in a Surveillance State." *The New York Times*. https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html.

[41] Achiume, T., & Relatoría Especial sobre las formas contemporáneas de racismo, discriminación racial, xenophobia y formas conexas de intolerancia de las Naciones Unidas. (2020). A/75/590 Reporte de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenophobia y formas conexas de intolerancia (párrafo 23)

[42] Molnar, P. and et al. Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up (2020), p. 16.

[43] Ibíd., p. 14.

Recientemente en Kenia, las Cortes han puesto freno a la plena adopción de un nuevo sistema de identificación biométrico, en respuesta de la acción judicial por parte de la sociedad civil, que ha alertado del impacto discriminatorio del sistema en los grupos marginados, así como sobre su diseño invasivo, incluida la centralización de almacenes masivos de datos personales sin salvaguardias y control para evitar extralimitaciones, el acceso no autorizado y otras formas de abuso[44].

En el sector humanitario hay algunas organizaciones que en reconocimiento de los riesgos asociados con el procesamiento de datos biométricos por las personas que están asistiendo han tomado una posición muy cuidadosa en su utilización. Por ejemplo, el Comité Internacional de la Cruz Roja (CICR) ha desarrollado una política por el uso de datos biométricos en casos de uso limitados y dentro de un marco muy bien definido[45] y Oxfam sigue explorando los riesgos y beneficios del uso de datos biométricas en sus propios programas[46].

3.2 Riesgos al derecho a la igualdad y no discriminación entre nacionales de Venezuela y todas las demás nacionalidades al recolectar biometría facial

En el contrato firmado por Migración Colombia se incluye la recolección de datos biométricos como los faciales que, como se mencionó, tienen serias implicaciones de derechos humanos. Sin embargo, los datos para reconocimiento facial no se recolectan para personas de otras nacionalidades. En este caso, la persona portadora de una Cédula de Extranjería, definida como el documento oficial de identificación de los migrantes residentes en Colombia, no requiere la recolección de datos biométricos faciales, sino que utiliza biometría decadactilar[47]. Así mismo, el establecimiento de cámaras de reconocimiento biométrico en puestos de control fronterizo que se encuentran en la frontera con Venezuela[48] y que reciben mayor afluencia de migrantes venezolanos, no es una tendencia que se repita en otros puestos de control fronterizo alrededor del país.

Estas medidas de verificación biométrica y de recolección de datos biométricos de una población en específico, establecen condiciones diferenciales para la migración y la permanencia en el país que contribuyen a la creación de regímenes fronterizos y

[44] Open Society Justice Initiative (marzo de 2020) Documento informativo sobre el Sistema de Manejo de Identidad Integral Nacional en Kenya, https://www.justiceinitiative.org/uploads/477c2588-00eb-4edd-b457-bf0d138fd197/briefing-kenya-niims-03232020.pdf
[45] International Committee of the Red Cross. (2019). The ICRC biometrics policy. https://www.icrc.org/en/document/icrc-biometrics-policy
[46] The Engine Room & Oxfam. (2018). Biometrics in the Humanitarian Sector. https://policy-practice.oxfam.org/resources/biometrics-in-the-humanitarian-sector-620454/
[47] Ministerio de Relaciones Exteriores, Decreto 1067 de 2015
[48] Migración Colombia. Contrato No. 106 de 2020, p.17.

regulatorios[49]. Es decir, sistemas que segregan la movilidad, la permanencia y el acceso a derechos de una población específica en función de su nacionalidad. Este elemento puede abrir las puertas para una discriminación sistemática de esta población.

3.3 No hay un examen de necesidad y proporcionalidad para la recolección de datos biométricos

El requerimiento de recolectar datos biométricos como los faciales debería responder a un examen de necesidad y proporcionalidad. Este examen debe garantiza que la recolección de datos biométricos no sea arbitraria y que no responde a una acción discriminatoria en contra de un grupo de migrantes que se caracteriza por sus altos niveles de vulnerabilidad. Por esto, no se explica la obligación de recolectar datos de biometría facial cuando los datos de biometría decadactilar son estándar en todos los procesos de identificación y autenticación de personas para el acceso a derechos en Colombia. Además, organizaciones como el Banco Mundial han mostrado que la biometría decadactilar tiene mejores desempeños y aceptación que la facial[50]. Igualmente, varias investigaciones han mostrado las serias limitaciones que tiene el reconocimiento facial para funcionar en grupos históricamente discriminados como las personas negras, las mujeres y las personas asiáticas[51].

3.4 Riesgos al principio de libertad en el tratamiento de datos biométricos

Los datos biométricos son caracterizados por la Ley de Protección de Datos (Ley 1581 de 2012) como datos sensibles, lo que impone la obligación de que las autoridades consideren las posibilidades de discriminación que implica la recolección, análisis, uso y almacenamiento de estos datos. La obligación de considerar los riesgos de discriminación es aún más relevante en el caso de poblaciones migrantes en condición de vulnerabilidad que no están en condiciones ni quieren negarse a las exigencias del Estado al que están forzadas a ingresar.

Como se mencionó, las personas migrantes no están en condiciones para negarse al tratamiento de sus datos personales y pocos recursos para impugnar. Así, los gobiernos utilizan estas limitaciones para imponerles políticas experimentales que no serían

[49] Achiume, T., & Relatoría Especial sobre las formas contemporáneas de racismo, discriminación racial, xenophobia y formas conexas de intolerancia de las Naciones Unidas. (2020). A/75/590 Reporte de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenophobia y formas conexas de intolerancia (párrafo 8).
[50] World Bank Group and Identification for Development. Technology landscape for digital identificacion, p. 16.
[51] Magnet, S. (2011). When Biometrics Fail: Gender, Race, and the Technology of Identity. Duke University Press.

aceptables con nacionales o con otras nacionalidades. De esta forma, las personas migrantes en condición de vulnerabilidad terminan siendo sujetos de experimentación de una tecnología como el reconocimiento facial.

3.5 Riesgos de igualdad y discriminación para las comunidades sobre las que la identificación biométrica falla

Para que la biometría funcione, el reconocimiento de patrones depende de la probabilidad de que el registro que capta la máquina de reconocimiento coincida con el dato guardado en una base de datos. Esto quiere decir que los sistemas no son infalibles, solo ofrecen una probabilidad [52]. Los datos biométricos no siempre son confiables. Existen múltiples ejemplos de falsos negativos (cuando el sistema no identifica una coincidencia erróneamente) y falsos positivos (cuando el sistema identifica una coincidencia erróneamente)[53]. El problema de confianza se ve exacerbado cuando los datos biométricos no siempre pueden ser recolectados. En una encuesta dirigida a estados miembros de la UE sobre la recopilación de datos biométricos de postulantes para un visado Schengen, 61% de los encuestados reportaron haber experimentado dificultades en la recopilación de datos biométricos[54]. Por otro lado, las tecnologías biométricas tienen problemas de funcionamiento con algunos cuerpos que han sido sistemáticamente discriminados [55].

En cuanto al reconocimiento facial, también se han encontrado numerosos obstáculos para la identificación de personas con pieles oscuras, especialmente en las mujeres [56]. Además, el reconocimiento de iris tiene fallas para reconocer personas con ojos oscuros [57]. Estos errores de lectura pueden llevar a falsos positivos y falsos negativos que comprometen el acceso de las personas a servicios básicos, cuando estos dependen de una autenticación plena. Inclusive, en India los fallos de reconocimiento del sistema biométrico Aadhaar están relacionados con el aumento de las muertes por inanición [58].

De igual forma, el reconocimiento facial depende de la calidad técnica de la foto, es decir, aspectos como la luz, el artefacto con el que se captura o si la foto es tomada en interior

[52] Asociación por los Derechos Civiles (2019). “La Identidad Que No Podemos Cambiar: Cómo La Biometría Afecta Nuestros Derechos Humanos.” Asociación por los Derechos Civiles, 2019. https://adc.org.ar/wp-content/uploads/2019/06/027-A-la-identidad-que-no-podemos-cambiar-04-2017.pdf.
[53] Gelb, A. y Clark, J. (2013). Identification for Development: the Biometrics Revolution. Working Paper 315, p. 9 -11.
[54] European Commission. (2016). SWD (2016) 328. Evaluation of the implementation of Regulation (EC) No. 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, p. 105.
[55] Browne, S. (2015). Black Matters: On the Surveillance of Blackness. Duke University Press.
[56] Kaurin, Dragana (2019). “Data Protection and Digital Agency for Refugees,” no. 12, p. 30.
[57] Magnet, S. (2011). When Biometrics Fail: Gender, Race, and the Technology of Identity. Duke University Press.
[58] Huffington Post India (26 September 2018). “Aadhaar Linked To Half The Reported Starvation Deaths Since 2015, Say Researchers.” Huffington Post India https://www.huffingtonpost.in/2018/09/25/aadhaar-linked-to-half-the-reported-starvation-deaths-since-2015-say-researchers_a_23539768/

o en exterior, afectan el registro biométrico[59]. Este tipo de fallas pueden reproducir inequidades sociales preexistentes y excluir de forma sistemática a cuerpos que no se adscriben a los patrones de reconocimiento blanco y masculino[60].

3.6 El uso de datos biométricos exige altos estándares de seguridad digital y grandes afectaciones ante una fuga de información

Los datos biométricos se presentan como la mejor forma de asegurar la identificación y la autenticación de una persona en cualquier proceso público. Sin embargo, a diferencia de una contraseña o un token que se pueden cambiar en caso de pérdida o robo, los datos biométricos tienen la característica de que son irremplazables[61]. Así, en el caso de una fuga de datos, la persona puede perder los factores que le permiten identificarse y autenticarse. Este riesgo es latente considerando que ya hay casos en los que han copiado huellas digitales en latex para tener acceso a sistemas[62] y que han creado el ADN de una persona a partir de su saliva[63].

Por esto, el mantenimiento de un sistema biométrico necesariamente implica un alto nivel de seguridad técnica y organizacional para evitar la pérdida o el robo de datos. Ahora bien, dos recientes casos han mostrado que las autoridades migratorias no tienen la capacidad para administrar este tipo de datos. Por un lado, a finales del 2020 el Laboratorio de Seguridad Digital de la Fundación Karisma (K-Lab) detectó una vulnerabilidad que exponía los datos personales de más de 800.000 personas que utilizaron el sistema de citas de Migración Colombia. Entre estos datos se incluían nombre, apellido, tipo y número de documento, año de nacimiento, sexo, teléfono y correo electrónico. Además, era posible obtener más de 4000 documentos de las personas concernientes a los trámites que realizaban en la autoridad migratoria[64].

Por otro lado, a principios de este año el medio La Silla Vacía reveló que los datos de las visas electrónicas de más de 550.000 personas estaban disponibles para descarga en la página del Ministerio de Relaciones Exteriores durante un tiempo indeterminado. Inclusive, el sistema tenía datos de menores de edad. A pesar de que la falla fue advertida

[59] World Bank Group and Identification for Development. Technology landscape for digital identificacion, p. 23

[60] Browne, S. (2015). Op. Cit.

[61] Privacy International (2013). Biometrics: Friend or Foe, p. 11

[62] Farivar, C. (22 September 2006), Digital fingerprint door lock defeated by photocopied 'print, Engadget. http://www.engadget.com/2006/09/22/digital-fingerprint-door-lock-defeated-byphotocopied- print/

[63] Harmon, K. (18 August 2009), Lab creates fake DNA evidence, Scientific American http://www.scientificamerican.com/blog/post.cfm?id=lab-creates-fake-dna-evidence-2009-08-18 Jain, A. K., and Pankanti, S. (September 2008), Beyond Fingerprinting, American Scientist, pp. 79-81. http://libserver.wlsh.tyc.edu.tw/sa/pdf.file/en/e080/e080p082.pdf

[64] Laboratorio de Seguridad Digital de la Fundación Karisma K-Lab (21 de enero de 2021). “Reporte de problema de seguridad en la página de Migración Colombia”. Disponible en: https://web.karisma.org.co/reporte-de-problema-de-seguridad-en-la-pagina-de-migracion-colombia-noviembre-de-2020/

a las autoridades por una persona anónima y por el medio de comunicación, no se solucionó el problema hasta que se publicó la historia[65].

Las personas que huyen de conflictos o situaciones de crisis, tal como los migrantes venezolanos, tienen un interés legítimo en proteger su identidad, ubicación y movimientos. La falta de compartimentalización de estos datos y altos estándares de seguridad podría exponer a los titulares a riesgos.

3.7 Riesgos para los derechos de los niños, niñas y adolescentes

Los niños, niñas y adolescentes (NNA en adelante) son sujetos de especial protección. La Constitución Política establece que los derechos de los niños prevalecerán sobre los derechos de los demás y resalta la obligación del Estado de asistir y proteger al niño para el ejercicio pleno de sus derechos (Art. 44).

La Relatora Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo ha señalado que los riesgos derivados del tratamiento de datos biométricos se amplifican cuando se trata de los derechos de ciertos grupos en condición marginal o vulnerable[66]. En particular, para el caso de los NNA, el tratamiento de datos biométricos de NNA debe cumplir con las salvaguardas establecidas en la Convención de los derechos de los niños, particularmente con la protección del interés superior de los NNA que está ampliamente reconocido en nuestra legislación[67].

En su artículo 16, la Convención sobre los Derechos del Niño establece la prohibición de injerencias arbitrarias o ilegales en su vida privada y la protección legal contra esas injerencias o ataques. En este marco, las consideraciones que hacemos sobre los riesgos de discriminación y al derecho a la intimidad, entre otros, son particularmente relevantes para el caso de los NNA pues pesa sobre el Estado la obligación especial de evitar la discrimininación en su por causa de las condiciones de sus padres, como lo señala el artículo 2.2 de la misma Convención[68].

---

[65] La Silla Vacía (15 de enero de 2021). “Un bache de seguridad amenazó los datos de extranjeros y Cancillería no sabía. Disponible en: https://lasillavacia.com/bache-seguridad-amenazo-los-datos-extranjeros-y-cancilleria-no-sabia-79749

[66] Huszti-Orbán, K., & Ní Aoláin, F. (2020). Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? Human Rights Center University of Minnesota. https://www.law.umn.edu/human-rights-center/research/use-biometric-data-identify-terrorists

[67] Ley 1098 de 2006. Artículo 8. Interés Superior de los Niños, las Niñas y Los Adolescentes. Se entiende por interés superior del niño, niña y adolescente, el imperativo que obliga a todas las personas a garantizar la satisfacción integral y simultánea de todos sus Derechos Humanos, que son universales, prevalentes e interdependientes.

[68] Convención sobre los Derechos del Niño. Artículo 2.2. Los Estados Partes tomarán todas las medidas apropiadas para garantizar que el niño se vea protegido contra toda forma de discriminación o castigo por causa de la condición, las actividades, las opiniones expresadas o las creencias de sus padres, o sus tutores o de sus familiares.

La Ley de Protección de Datos impone el deber de respetar los derechos prevalente de los NNA en el tratamiento de datos[69]. Este artículo además implica, primero, que la finalidad del tratamiento de datos no sólo debe perseguir un fin legítimo sino que éste persiga el interés superior de los NNA[70]. Segundo, los NNA tiene que ser escuchados y a que sus opiniones, en este caso sobre el tratamiento de datos biométricos, sean tenidas en cuenta[71].

Otras legislaciones han reconocido la necesidad de implementar protecciones particulares para el tratamiento de datos personales de NNA. Por ejemplo, el Reglamento General de Protección de Datos de la Unión Europea considera que los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales"[72]. Algunas de los riesgos particulares a los que se enfrentan los NNA en el tratamiento de sus datos biométricos son que las tecnologías están diseñadas para funcionar en adultos, que los NNA tienen menos autonomía y oportunidades para tomar decisiones sobre su participación en servicios y programas oficiales y que los NNA están sujetos a un tiempo mayor de recolección y acumulación de datos a lo largo de sus vidas debido a los constantes cambios tecnológicos[73].

Teniendo en cuenta las especiales protecciones necesarias para asegurar los derechos y el interés superior de los NNA, UNICEF recomienda que se realice una evaluación de impacto relativa a la protección de datos respecto al tratamiento de los datos biométricos de los NNA[74]. El Reino Unido cuenta con legislación especial sobre obligaciones para el tratamiento de datos personales de NNA dentro de las que se encuentran estas mismas obligaciones de respeto del interés superior de los NNA y la realización de evaluaciones de impacto, entre otras[75]

[69] Ley 1581 de 2012. Artículo 7. Inciso 1.

[70] Corte Constitucional. Sentencia C-748 de 2011. Sección 2.9.3.4. "los datos de los niños, las niñas y adolescentes pueden ser objeto de tratamiento siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales e inequívocamente responda a la realización del principio de su interés superior, cuya aplicación específica devendrá del análisis de cada caso en particular".

[71] Ley 1098 de 2006. Artículo 26. Derecho al debido proceso. (...) En toda actuación administrativa, judicial o de cualquier otra naturaleza en que estén involucrados, los niños, las niñas y los adolescentes, tendrán derecho a ser escuchados y sus opiniones deberán ser tenidas en cuenta.

[72] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, "Reglamento General de Protección de Datos". Considerandos número 38.

[73] UNICEF. (2019). Faces, Fingerprints & Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programs. https://data.unicef.org/wp-content/uploads/2019/10/Biometrics_guidance_document_faces_fingersprint_feet-July-2019.pdf

[74] UNICEF. (2018). Children's Online Privacy And Freedom Of Expression: Industry Toolkit. https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

[75] Information Commisioner's Office. (2021, enero 28). Children's Code hub. Children's Code Hub; ICO. https://ico.org.uk/for-organisations/childrens-code-hub/

3.8. Conclusiones y solicitudes

Considerando que el Estatuto Temporal de Protección para Migrantes Venezolanos se implementará en el marco del mencionado contrato, la obligación de entregar datos biométricos no definidos por el borrador de decreto es un requerimiento que representa un riesgo grave para los derechos fundamentales a la intimidad, la igualdad y no discriminación y la dignidad de las personas migrantes.

1. El contrato de Migración Colombia demuestra que se recolectarán datos biométricos como el rostro para identificar a las personas migrantes en espacios públicos incluyendo cámaras en la frontera, dispositivos móviles utilizados por oficiales de verificación migratoria y cualquier video o imagen. Esto es una franca violación de los derechos fundamentales de los migrantes que se acogen al estatuto buscando protección del Estado colombiano y que están en condiciones de vulnerabilidad y, por tanto, son sujetos de especial protección constitucional.
2. La recolección de datos biométricos que son clasificados como sensibles por la Ley de Protección de Datos y que podrían permitir la identificación de los migrantes que se acojan al estatuto representan una forma de discriminación considerando que este tipo de sistemas no son utilizados ni obligatorios para nacionales colombianos y de otras nacionalidades.
3. Este tipo de requerimiento es arbitrario y no responde a un examen de necesidad y proporcionalidad considerando que la biometría decadactilar ofrece suficientes garantías de confianza para el acceso a servicios fundamentales en Colombia.
4. La obligación para entregar datos sensibles como los biométricos debe estar sustentada en una evaluación de la necesidad y proporcionalidad de exigir la entrega de datos biométricos a personas en condición de vulnerabilidad. Las organizaciones de defensa de derechos de los migrantes han reconocido que una persona en condición de vulnerabilidad no tiene forma de entregar un consentimiento realmente libre y esto viola el principio de libertad de la Ley de Protección de Datos.
5. Múltiples estudios han establecido que la autenticación biométrica presenta fallas con personas vulnerables. Especialmente, sistemas experimentales como el reconocimiento facial. Sin embargo, el ETPMV no reconoce la necesidad de ofrecer alternativas para las personas que no pueden producir ciertos datos biométricos.
6. Los datos biométricos se usan cada vez más como medio de autenticación y tienen la particularidad de no poderse cambiar en caso de fuga de estos. Se puede cambiar una contraseña o un certificado criptográfico pero no puede cambiar su huella dactilar o su iris. Esto aumenta aún más la sensibilidad de estos datos y asigna una responsabilidad muy alta -en términos de deber de seguridad digital- a quien los almacena.

Por todo lo anterior, solicitamos que:

1. Se restrinja la recolección de datos biométricos a las huellas digitales cambiando la palabra "biométricos" por "huellas digitales" en línea con los registros biométricos de personas de otras nacionalidades.
2. Se establezcan en el ETPMV procedimientos para asegurar la inclusión de las personas migrantes venezolanas con alternativas no biométricas para los casos en los que no se puedan producir los datos biométricos para la identificación o fallen los equipos.
3. Se realice una evaluación del impacto en derechos humanos de la implementación de alternativas biométricas antes de empezar con el proceso de tratamiento de los datos personales de acuerdo con cada dato, cada finalidad y cada actividad de tratamiento.

4. Seguridad digital

En los anteriores comentarios hay varios elementos de seguridad digital. Sin embargo, sobre este tema subsisten múltiples vacíos. Por tanto, describimos una serie de elementos que es necesario incorporar en el ETPMV.

No existe software totalmente seguro, así que las personas que desarrollen el software deben activamente buscar vulnerabilidades y mantener actualizado el sistema por medio de parches para reducir el riesgo de seguridad digital[76]. Un sistema que usará y hospedará datos de alta sensibilidad, como lo son los datos biométricos, deberá garantizar el uso de altos estándares de seguridad en su diseño. El modelo de seguridad por diseño -que supone construir desde el inicio sistemas seguros- incluye asumir que habrá ataques y vulnerabilidades, y buscar mecanismos que puedan mitigar los efectos de este tipo de acciones. Por esto, el decreto debería incorporar obligaciones de continuo mantenimiento, auditorías y manejo de reportes de vulnerabilidades.

Otro reciente informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre políticas para productos inteligentes recuerda a los Estados sus obligaciones fuera de su papel como reguladores, los gobiernos son también agentes económicos[77]. De esta forma, pueden aprovechar su poder adquisitivo y predicar con el ejemplo para influir en el comportamiento de otras partes interesadas. Los gobiernos pueden utilizar las políticas de contratación pública para incentivar a los actores del lado de la oferta a certificar la seguridad digital de los productos inteligentes. Así mismo, los gobiernos deberían adherirse a los principios que promulgan, por ejemplo, en lo que respecta a la oportuna aplicación de parches a las vulnerabilidades. El rol de los Estados como consumidores y contratistas de sistemas les obliga a ser especialmente cuidadosos

[76] OECD (2020) . Encouraging vulnerability treatment Responsible management, handling and disclosure of vulnerabilities". https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf
[77] OECD (2021). Smart policies for smart products: A policy maker's guide to enhancing the digital security of products. https://www.oecd.org/digital/smart-policies-for-smart-products.pdf

con los estándares de seguridad digital. Especialmente, si el desarrollo involucra riesgos de discriminación e impone barreras al ejercicio de derechos. En este caso, el decreto no aborda esta dimensión con suficiente responsabilidad.

Adicionalmente, grupos como el Article 29 Working Party (hoy European Data Protection Board)[78] y la Autoridad Francesa CNIL[79] han desarrollado recomendaciones para el uso y administración de datos biométricos que pueden servir para, desde los aspectos técnicos, proteger esos datos como:

- no almacenar lo datos biométricos en sí mismo sino datos derivados (ej. puntos de la huella dactilar) sin posibilidad de volver a calcular las características biométricas de origen;
- Estos datos derivados se deben almacenar en la base de datos en una forma cifrada o el resultado de un algoritmo de hash usando una llave secreta;
- tener una separación (compartimentar) estos datos biométricos de los otros datos de la persona;
- asociar un código de integridad a los datos biométricos (ej. hash, o firma);
- en el control de identidad / autenticidad, el cliente no debe transmitir al servidor los datos biométricos en sí mismo sino datos derivados, cifrados o en los cuales se haya aplicado un hash.

Considerando el trabajo que Karisma ha realizado, a través del laboratorio K-Lab, analizando sistemas del Estado que usan intensivamente datos de las personas[80], podemos afirmar que este decreto debería prever una serie de acciones que protejan la privacidad y seguridad tales como:

1. El documento que crea y regula un sistema informático que usará datos personales sensibles debe incluir los mecanismos de evaluación de impacto, desempeño -antes y después de su puesta en marcha-, supervisión y control, tanto propios como indicando la forma en que facilita los externos.
    - Debe prever los recursos y cargos para que la entidad encargada del sistema cuente con las capacidades internas necesarias que le permitan por sí misma probar el sistema constantemente para verificar la existencia de vulnerabilidades y poder atender reportes de fallas de seguridad, cuando sea necesario. Esto no puede estar en manos del tercero contratista, es responsabilidad de la entidad.

[78] Article 29 Working Party (2012). “Opinion 3/2012 on developments in biometric technologies”. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[79] Autoridad Francesa CNIL (2019). “Deliberación 2019-001 del 10 de enero del 2019”. Disponible en https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf

[80] El último análisis de los ejercicios realizados por el K+Lab durante 2020 con algunas recomendaciones puede consultarse acá https://web.karisma.org.co/vulnerabilidades-reportadas-por-el-klab-de-karisma-a-entidades-publicas-en-2020/

- Debe establecer la obligación y dar los recursos para realizar auditorías especializadas regularmente y prever que versiones generales de estos informes deberán ser comunicadas a las autoridades de protección de datos y publicadas para conocimiento de todas las personas,
- Debe indicar las funciones que cumplen las autoridades públicas en relación con las garantías y ejercicios de derechos que pueden verse afectadas por el sistema,
- Debe manifestar que cualquiera, pero sobre todo las partes interesadas en este tema, debe poder hacer seguimiento al sistema contribuyendo así a la confianza. Reconocer y desarrollar el rol de la veeduría ciudadana es una forma de poner en práctica mecanismos de co-responsabilidad para mejorar la seguridad digital, la privacidad y la calidad del sistema, como lo sugiere el Conpes de seguridad digital y lo recomienda la OCDE en el documento sobre vulnerabilidades ya mencionado.

Estas son las previsiones que permitirán constantemente hacer los ajustes necesarios e informar sobre el despliegue y efectividad de la medida, garantizando que hay una conexión real entre la finalidad del sistema y el tratamiento de datos personales que éste hace.

2. Se debe indicar en el decreto los criterios y exigencias en materia de estándares de calidad del desarrollo, privacidad y seguridad por diseño que se exigen al contratista en el diseño y desarrollo del sistema. De modo que sea expresa la forma como el sistema garantiza la apropiada gestión de los datos personales, sobre todo de datos tan sensibles como los biométricos. Es obligación del Estado demostrar que su diseño está pensado para proteger la privacidad, que es el mayor riesgo, y la seguridad, que es una de las formas de preservarla.
3. El decreto debe establecer las fases de desarrollo que permitan esquemas de evaluación y prueba. Hemos determinado que los sistemas del Estado suelen desplegar el prototipo como producto y, por tanto, no se da espacio para revisar el código, su arquitectura y funcionamiento. Por esto, es necesario que las diferentes fases del desarrollo se conozcan de modo que existan espacios para que las partes interesadas verifiquen el respeto a las garantías y ejercicio de derechos de las personas en las características que quedarán embebidas en el código.
4. Debe quedar claro en este documento el tiempo en que el sistema hará tratamiento de los datos personales en las diferentes circunstancias. Cuando se cumple el tiempo de tratamiento de los datos en cada caso, éstos deberán ser borrados y por tanto el decreto debe establecer la forma en que harán efectiva dicha previsión.