PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO MIGRATORIO LATINOAMERICANO

accessnow

accessnow.org

Access Now defiende y amplifica los derechos digitales de las personas y comunidades en situación de riesgo. Como una organización que aporta desde lo local a la escala mundial, nos asociamos con actores locales para llevar una agenda de derechos humanos al uso, desarrollo y gobernanza de las tecnologías digitales, y para intervenir allí donde las tecnologías afectan negativamente a nuestros derechos humanos. Combinando el apoyo técnico directo, la defensa estratégica, la concesión de fondos comunitarios y encuentros como RightsCon, luchamos por los derechos humanos en la era digital.

Protección de datos personales en el contexto migratorio en algunos países de Latinoamérica

Tabla de contenidos

I.INTRODUCCIÓN

La vigilancia sobre las personas migrantes, refugiadas y solicitantes de asilo en Latinoamérica es cada vez más compleja. El uso de tecnologías con capacidad de vigilancia en contextos migratorios supone una potencial injerencia desproporcionada en la vida privada de estas personas que colisiona con estándares internacionales de derechos humanos.

Muchos países de la región recolectan, procesan e intercambian con otros datos personales de migrantes, como nombre, apellido, edad, fecha de nacimiento, domicilio, incluyendo datos sensibles, como condiciones especiales de salud, **datos biométricos** como sus huellas dactilares, escaneo de iris, entre otros. Estos datos son recolectados por el gobierno de sus propios países, y de aquellos territorios que atraviesan en su trayecto hacia su destino, utilizando una gran variedad de técnicas, por ejemplo, dispositivos con capacidad de vigilancia basadas en datos biométricos.

Luego, esos mismos datos pueden ser utilizados para servir en los procesos de toma de decisiones sobre su destino migratorio, sin que tengan acceso a instancias donde poder defenderse adecuadamente y sin que existan necesariamente remedios para que puedan ejercer derechos vinculados a sus datos (por ejemplo, de acceso, rectificación, cancelación u oposición).

El siguiente reporte tiene como objetivo describir el marco legal y regulatorio aplicable a la recolección y tratamiento de datos personales de personas migrantes, refugiados y solicitantes de asilo en **Argentina, Chile, Ecuador, El Salvador, Guatemala, Honduras y México**, como casos testigo de lo que sucede en gran parte de América Latina y el Caribe, a los fines de que sirva como insumo para llevar adelante esfuerzos de incidencia por parte de organizaciones de la sociedad civil y otros actores en defensa del derecho fundamental a migrar. **A su vez, presentamos recomendaciones para robustecer la protección de los datos personales de personas migrantes, ya sea en específico en alguna jurisdicción de las ya mencionadas, o en general en la región.**

El documento brindará un glosario de términos que servirán para mejorar la comprensión del contexto general de los derechos humanos y de la protección de datos personales de personas migrantes, refugiados y solicitantes de asilo. Luego, abordaremos tres aspectos que reflejan la situación regulatoria de protección de datos y del despliegue de tecnologías con capacidades de vigilancia en contextos fronterizos, estos son:

I. La existencia o no de leyes de protección de datos, y en caso de que existan, su necesidad de actualización o su correcta adecuación a las más modernas técnicas legislativas en este sentido.
II. La regulación sobre el despliegue de tecnologías con capacidad de vigilancia en los contextos fronterizos.
III. La existencia de acuerdos de transferencia de datos entre países, o entre estos y organizaciones internacionales enfocadas en la situación fronteriza y migratoria a nivel global.

Agradecemos a las firmas legales que colaboraron de manera pro bono en los procesos de investigación en cada uno de los territorios abordados a partir de la conexión facilitada por **TrustLaw, el programa global de pro bono legal de la Thomson Reuters Foundation**. Las firmas participantes son: **Estudio O'Farrell en Argentina, Morales & Besa en Chile, Central Law en El Salvador, Honduras y Guatemala, Robalino Abogados en Ecuador, y Baker McKenzie en México.**

II. GLOSARIO

Biometría	Medios de identificación de un individuo a través de la medición de rasgos fisiológicos distinguibles o de comportamiento, tales como huellas digitales, cara, iris, retinas, características auriculares, voz, modo de andar, y otros.
Control fronterizo	Controles y actividades de monitoreo y/o vigilancia fronteriza realizadas en las fronteras físicas – aéreas (aeropuertos), marítimas (puertos marítimos, lacustres, fluviales) y terrestres (tierra, ferrocarril) – del Estado destinadas a regular la entrada (o la intención de entrar) y la salida de personas hacia y desde el territorio del Estado, en ejercicio de su soberanía.
Datos personales	Toda información sobre una persona física identificada o identificable, entendiéndose por tal toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
Datos sensibles	Datos personales que revelan rasgos íntimos de un individuo. Estos datos incluyen, de forma no exclusiva, los datos genéticos, biométricos y de salud, así como datos personales que revelen el origen racial y étnico, las opiniones políticas, las convicciones religiosas o ideológicas o la afiliación sindical, o cualquier otra característica que pueda derivar en discriminación o toma de decisiones arbitrarias.
Responsable	La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por su cuenta.
Encargado	La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable.
Migrante	Persona que abandona su país de residencia habitual, de forma temporal o definitiva.

Norma	Cualquier reglamento, legislación o estatuto jurídico.

III. REGULACIÓN DE PROTECCIÓN DE DATOS PERSONALES EN LA REGIÓN

La adecuada regulación de la protección de datos personales se erige como garantía ante el potencial tratamiento dañino y discriminatorio, o desproporcionado, de los datos que son titularidad de las personas. Por ello, contar con leyes que incorporen los más altos estándares de protección de datos personales y las últimas tendencias en esta materia supone una gran ventaja para la región, y en particular, para las poblaciones vulnerables, como suelen ser la de las personas migrantes y solicitantes de asilo.

En Latinoamérica, existen proyectos de ley que buscan incorporar regulación de protección de datos personales, o actualizar las ya sancionadas para incorporar las últimas tendencias regulatorias. De cualquier manera, estos esfuerzos todavía no reciben tratamiento o sanción de parte de los poderes legislativos en la mayoría de los casos. Para los fines de este reporte, analizaremos específicamente la situación de los países que han sido objetivo de investigación.

Entre ellos existe un escenario diversificado en esta materia, con naciones con legislaciones vigentes sancionadas recientemente, como el caso de Ecuador y países con leyes que ya cuentan con varios años desde su sanción como Argentina, Chile o México. Así también, existen muchos países donde todavía no se han sancionados leyes adecuadas de protección de datos personales tal como El Salvador, Honduras o Guatemala.

A los fines de brindar un análisis de los países estudiados que incorpore la dimensión de la protección de datos personales de las personas migrantes, este reporte presenta a continuación los hallazgos encontrados por las firmas legales participantes, mencionadas en la introducción:

Argentina

Argentina cuenta con una legislación especial para la protección de datos personales desde el año 2000 (Ley 25.326), que se complementa con múltiples normas reglamentarias. Además, aprobó el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, de la Unión Europea (más conocido como Convenio 108), y su Protocolo Modificatorio (Convenio 108+).

No hay formalmente una diferencia normativa en cuanto a la protección de datos personales de nacionales y de personas migrantes, solicitantes de asilo o refugiadas. De cualquier manera, el marco normativo no se encuentra actualizado a las tendencias en protección de datos.

Además, mediante la Ley N° 15.869 Argentina adhirió a la Convención sobre el Estatuto de los Refugiados de 1951, en el marco de Naciones Unidas, y posteriormente también a su protocolo de 1961. Esta Convención establece la cooperación entre las autoridades nacionales con las Naciones Unidas, el compromiso de los estados contratantes para suministrar información y datos estadísticos que soliciten acerca de la condición de los refugiados y las leyes, reglamentos y decretos, que estén o entren en vigor, concernientes a los refugiados, entre otros. En la guía de interpretación de esta Convención se establece como principio la confidencialidad de la información personal sobre los solicitantes de asilo y los refugiados y a que la eventual divulgación de información personal a terceros deberá hacerse siempre con el consentimiento del solicitante de asilo o del refugiado, es decir, del titular del dato personal.

Por su parte, la Ley General de Reconocimiento y Protección al Refugiado, número 26.165, establece que toda la información relacionada con la solicitud de la condición de refugiado tendrá carácter estrictamente confidencial.

Finalmente, a la fecha de publicación de este reporte, existe un proceso de actualización mediante un proyecto de ley presentado ante el Congreso de la Nación que busca lograr este objetivo, aún sin tratamiento.

Chile

El derecho a la protección de datos personales se encuentra consagrado en el artículo 19 N°4 de la Constitución Política de la República. Este derecho constitucional es desarrollado principalmente a través de la Ley N° 19.628 sobre Protección de la Vida Privada (la “LPVP”). Quedará sujeto a la LPVP todo procesamiento de Datos Personales que sea llevado a cabo en Chile, sin importar si dicho tratamiento es llevado a cabo por particulares o por organismos públicos. La LPVP se aplica a todos los habitantes de la República de Chile, sean estos nacionales o extranjeros. De esta manera, no existe una diferencia entre la Protección de Datos Personales de nacionales y de personas migrantes, solicitantes de asilo o refugiadas.

A su vez, y al igual que en el caso de Argentina, Chile cuenta con un proyecto de ley de actualización del régimen de protección de datos personales pendiente de tratamiento.

Sin perjuicio de lo anterior, el artículo 144 de la Ley N°21.325 sobre Extranjería y Migración estipula una obligación especial al Servicio Nacional de Migraciones, la Policía de Investigaciones de Chile, Carabineros de Chile y al Servicio de Registro

	Civil e Identificación en relación al cuidado, confidencialidad y reserva de los Datos Personales de extranjeros, cualquiera sea su calidad migratoria.
Ecuador	La Constitución de la República del Ecuador indica en su Art. 9 que las personas extranjeras que se encuentren en el territorio ecuatoriano tendrán los mismos derechos y deberes que las ecuatorianas. A su vez, Ecuador cuenta con normas que regulan la Protección de Datos Personales, entre la que destaca la recientemente sancionada Ley Orgánica de Protección de Datos Personales (la "LOPD"), enfocada en regular los derechos y libertades que se desarrollan en el entorno de Internet. Esta ley ha sido recientemente reglamentada el 6 de noviembre del 2023 por el poder ejecutivo nacional. Aún resta conocer quién será designado como autoridad competente en la aplicación de la misma.
El Salvador, Guatemala, y Honduras:	No cuentan con normativa específica en materia de protección de datos personales.
México	La protección de datos personales se regula principalmente por la Constitución Mexicana, y las leyes especiales. Existe una ley para regular el tratamiento de los datos personales por entidades privadas y una distinta para regular su tratamiento por entidades públicas. La primera es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (la "LFPDPPP"), y su Reglamento, y la segunda es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (la "LFPDPPSO"). Sin embargo, existen también distintas recomendaciones emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ("INAI"), la autoridad en materia de protección de datos personales en México. La protección de datos personales en México no la detona la nacionalidad, residencia o la ciudadanía, ya que este marco regula el tratamiento de todos los datos personales de personas en México, incluidos los datos personales de personas migrantes, refugiados y solicitantes de asilo en México, aun cuando estos no cuenten con nacionalidad Mexicana, residencia o ciudadanía. Incluso, cabe señalar que el INAI ha publicado recursos específicos para extranjeros[1].

[1] https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/guiapdpextranjeros_esp.pdf

El anterior desglose revela la ausencia de normativas suficientes en la región para proteger los datos personales de las personas migrantes, solicitantes de asilo o refugiadas. Al mismo tiempo, sin haber sido incorporado directamente a los resultados transcritos, es necesario apuntar a la falta de independencia que existe en varias autoridades de protección de datos personales en Latinoamérica. La independencia de las autoridades responsables de la aplicación de las leyes de protección de datos es un requisito imprescindible para garantizar su observación y aplicación. Por ejemplo, en Argentina depende del poder ejecutivo nacional, o en el caso de Ecuador, la ausencia de designación de la autoridad impone desafíos para la protección de datos personales.

Finalmente, hay que destacar que estos resultados describen un mapa regulatorio claramente diverso, pero que de cualquier manera evidencian la necesidad de avanzar o actualizar leyes que protejan los datos personales atendiendo a los más altos estándares internacionales.

VI. REGULACIÓN DE PROTECCIÓN DE DATOS PERSONALES EN LA REGIÓN

El despliegue de tecnologías con capacidades de vigilancia en Latinoamérica implica un desafío para garantizar el derecho a la privacidad y a la protección de datos personales, entre otros. En nuestra región, las políticas públicas que promueven a estos mecanismos como herramientas para prevenir y perseguir el crimen (incluyendo en esta categoría a la migración irregular), están en crecimiento.

Estas políticas muchas veces plantean una limitación desproporcionada al ejercicio del derecho a la privacidad, por su capacidad de injerencia invasiva en el ámbito íntimo y en la expectativa de privacidad de las personas. Más allá de los supuestos resultados positivos que el despliegue de este tipo de tecnología podría tener en la reducción del nivel del delito (y que no ha sido demostrada[2]), existe documentación que revela como su eficiencia cae cuando se analizan datos biométricos de ciertas poblaciones, como son aquellas que poseen tez morena u oscura o personas adultas mayores[3].

Distintas autoridades judiciales de países de la región sostienen que la finalidad de prevención del delito no constituye una base de legitimación para autorizar este tipo de tecnologías (por ejemplo, la sentencia de la Corte Constitucional de Colombia[4], la sentencia del Tribunal de Justicia de San Pablo[5], o la sentencia en Argentina que suspende las cámaras de reconocimiento facial[6]).

Estas políticas de aumentar las capacidades de vigilancia y, sobre todo, aquella basada en datos biométricos se expande también a los contextos fronterizos, con el afán de servir a las autoridades en la gestión de los flujos migratorios. Más allá de los desafíos al derecho a la privacidad y a la

[2] https://www.accessnow.org/press-release/pronunciamiento-terminar-acuerdos-biometricos-migrantes/
[3] https://www.accessnow.org/wp-content/uploads/2021/06/BanBS-Spanish.pdf
[4] https://www.corteconstitucional.gov.co/relatoria/2020/C-094-20.htm
[5] https://accessnow.org/sentenca-maio-7-2021-sao-paulo-metro
[6] https://drive.google.com/file/d/1eoR6Ilwdon_JcT9356nE6yJ1E_uxsyXB/view

autodeterminación informativa que supone el uso de estas tecnologías, estas políticas públicas podrían fomentar la decisión de las personas migrantes a optar por rutas más peligrosas, ya sea por las propias condiciones naturales que presentan o por la existencia de grupos de crimen organizado[7].

"Por diseño, estas tecnologías representan una amenaza para los derechos de las personas y ya han causado daños significativos. Ninguna salvaguarda legal o técnica podría ser suficiente para eliminar completamente el peligro que implican, y, por eso, creemos que no se deben utilizar en ningún caso en espacios públicos o de acceso público, ya sea por gobiernos o el sector privado. El potencial de abuso es demasiado grande, y las consecuencias, demasiado graves".

La cita anterior pertenece a la "*Carta abierta para solicitar una prohibición global sobre el uso de las tecnologías de reconocimiento facial y reconocimiento biométrico remoto que facilitan la vigilancia orientada, masiva y discriminatoria*[8]", cuya lectura recomendamos tanto para comprender los desafíos que presentan estas tecnologías para los derechos humanos, como para conocer las recomendaciones o solicitudes que los hacedores de políticas públicas, miembros del poder judicial, y organizaciones internacionales deberían incorporar.

Ante el interrogante sobre la regulación existente en materia de tecnologías con capacidades de vigilancia en los países consultados, obtuvimos los siguientes resultados:

Argentina

Las siguientes Normas en Argentina mencionan el uso de tecnologías con capacidades de vigilancia:

1. **Disposición de la Dirección Nacional de Protección de Datos Personales N° 10/15:** Introduce condiciones de licitud para las actividades de recolección y posterior tratamiento de imágenes digitales de personas con fines de seguridad. Allí se indica que, para poder tratar esas imágenes, se deben colocar carteles informativos.
2. **Resolución de la Agencia de Acceso a la Información Pública N° 4/19:** Aprueba criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley N° 25.326 (de protección de datos personales). Para el ejercicio del derecho de acceso a los datos personales recolectados mediante sistemas de video vigilancia, el responsable de la base de datos deberá aplicar alguna técnica de disociación, de forma que solo pueda ser identificado el titular de los datos que haya requerido acceso a esa información. Esta resolución también define a los datos biométricos como *"aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o*

[7] https://www.context.news/surveillance/surveillance-tech-makes-us-mexico-border-even-deadlier
[8] https://www.accessnow.org/wp-content/uploads/2021/06/BanBS-Spanish.pdf

conductuales de una persona humana, que permitan o confirmen su identificación única".

Luego, como parte de la investigación, las firmas legales fueron consultadas sobre la existencia de obligatoriedad de conducir estudios de impacto a la protección de datos personales, a la privacidad, o a los derechos humanos, como requisito para el despliegue de este tipo de sistemas.

Como resultado, se informó que en Argentina no existen normas que obliguen a las autoridades a hacer este tipo de exámenes ya sea antes, durante o después de implementar o seleccionar estas tecnologías con capacidades de vigilancia.

Chile

En Chile existen normas que regulan la obtención de información a través de tecnologías con capacidades de vigilancia. Sin embargo, se trata de una regulación disgregada y de aplicación específica para ciertos casos. No existe un único cuerpo legal de aplicación general que trate esta materia. Algunas de las más relevantes en este aspecto son:

1. **Código Procesal Penal:** El Código Procesal Penal (el "CPC") es la norma que regula los procedimientos para la investigación y persecución de delitos cometidos en Chile. Los artículos 181 y 226 del CPC refieren a las actuaciones de investigación dentro de un proceso judicial, situación que no forma parte del objeto de este reporte, por lo que no se ampliará (siempre que la injerencia a la privacidad de las personas sea realizada dentro de una investigación judicial, podría estar legitimada por las excepciones existentes).
2. **Ley sobre el Sistema de Inteligencia del Estado y que crea la Agencia Nacional de Inteligencia:** La ley N°19.974, sobre el Sistema de Inteligencia del Estado, crea la Agencia Nacional de Inteligencia (la "Ley de Inteligencia") y establece la posibilidad que los organismos que componen el sistema de inteligencia del Estado utilicen procedimientos especiales para la obtención de información, a saber:
    a. La intervención de las comunicaciones telefónicas, informáticas radiales y de la correspondencia en cualquiera de sus formas;
    b. La intervención de sistemas y redes informáticas;
    c. La escucha y grabación electrónica incluyendo la audiovisual; y
    d. La intervención de cualquier otro sistema tecnológico destinado a la transmisión, almacenamiento o procesamiento de comunicaciones o informaciones.

De cualquier manera, mencionamos esta ley porque en su propio articulado se afirma que estos procedimientos deben estar limitados a actividades de inteligencia y contrainteligencia, que tengan por objetivo resguardar la seguridad nacional y a la protección de las amenazas de terrorismo, crimen organizado y narcotráfico. Estos objetivos, si bien nobles y atendibles, son demasiados abstractos y pueden dar lugar a situaciones donde la vigilancia se ejerza de manera desproporcionada.

La norma continúa detallando que para que la Agencia pueda hacer uso de estos mecanismos, los directores o jefes de los organismos de inteligencia deben solicitar una autorización judicial. Estos mecanismos sólo pueden ser utilizados por los organismos de inteligencia cuando sea estrictamente indispensable para el cumplimiento de sus objetivos y la información no pueda ser obtenida de fuentes abiertas.

De igual manera que en Argentina, en Chile tampoco se identifican normas que contengan una obligatoriedad de llevar adelante estudios de impacto de protección de datos personales o a los derechos humanos.

Ecuador

Según el artículo 13 de la Ley de Seguridad Pública y del Estado (la "LSPYDE"), Ecuador cuenta con una Entidad rectora del Sistema Nacional de Inteligencia (de derecho público) la cual tiene independencia administrativa y financiera y personalidad jurídica. Entre las definiciones más relevantes provistas en la referida norma se encuentran la de Inteligencia y la de contrainteligencia (descrita como "la actividad de inteligencia que se realiza con el propósito de evitar o contrarrestar la efectividad de las operaciones de inteligencia que representan amenazas o riesgos para la seguridad").

Por su parte, el artículo 20 contempla las circunstancias en la cuáles los organismos de inteligencia podrán requerir, retener, abrir, interceptar o examinar documentos o comunicaciones. Esta norma no es del todo relevante para los fines de este reporte, ya que las investigaciones que se desarrollen en el marco de una investigación judicial difieren de aquellas que regulan la vigilancia masiva en espacios públicos o en contextos migratorios.

Sí es de interés desde la óptica de protección de derechos de personas migrantes que el artículo 22 de la "LSPYDE" prohíbe expresamente a cualquier organismo de inteligencia obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de "su etnia, orientación sexual, credo religioso, acciones privadas, posición política o de adhesión o

	pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción".
El Salvador	La investigación en este país arroja como principales hallazgos la ley de Acceso a la Información Pública y la Ley Especial Contra los Delitos Informáticos y Conexos (la "Ley de Delitos Informáticos"). Estas normas son las que se consideran más relevantes; sin embargo, dichas leyes no regulan de manera específica el uso de las tecnologías mencionadas, sino de manera general y bajo ciertos supuestos, como la penalización por el uso indebido de ellas (y no la protección de los ciudadanos cuyos datos son recolectados por medio de dichas tecnologías). De igual manera, no existen normas que obliguen a las autoridades a realizar un examen de diligencia debida en materia de derechos humanos o una evaluación de impactos en materia de protección de datos personales.
Guatemala	No hay leyes especiales que regulen el uso de tecnologías con capacidades de vigilancia, ni normas que obliguen a las autoridades a realizar un examen de diligencia debida en materia de derechos humanos o una evaluación de impactos en materia de protección de datos personales.
Honduras	No hay leyes especiales que regulen el uso de tecnologías con capacidades de vigilancia, ni normas que obliguen a las autoridades a realizar un examen de diligencia debida en materia de derechos humanos.
México	A pesar de que en México no existe una legislación especial para regular el uso de tecnologías con capacidades de vigilancia, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos personales ("INAI") ha publicado guías respecto del tratamiento de datos biométricos, así como, modelos de los avisos de privacidad que deben ser utilizados cuando se utiliza tecnología de video vigilancia. Asimismo, cabe señalar que tanto la LFPDPPP para entidades privadas, como la LGPDPPSO, para entidades públicas consideran obligatorio llevar a cabo exámenes de impacto a la protección de datos, privacidad, o a los derechos humanos frente al uso de estos sistemas.

En base a los hallazgos compartidos en esta sección, debemos señalar que la ausencia de regulación específica en el uso de este tipo de tecnologías y mecanismos de vigilancia se percibe como un déficit

que presentan la mayoría de los países analizados con relación al respeto de los derechos humanos de la población migrante. Se recomienda a los países, y sobre todo a aquellos que perciben un alto flujo migratorio, avanzar en esta deuda legislativa.

De igual manera, la falta de obligatoriedad en el análisis de los impactos de los países estudiados puede habilitar graves infracciones a los derechos fundamentales y a la protección de los datos personales de los migrantes. Esto es también un vacío normativo en detrimento de estas comunidades, que en gran medida se encuentran compuestas por personas que presentan demandas urgentes de atención y custodia sobre su seguridad física y psicológica.

V. ACUERDOS PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES DE MIGRANTES, REFUGIADOS O SOLICITANTES DE ASILO

La creciente facilidad técnica para el intercambio de datos e información entre diferentes Estados facilita el diseño de políticas de cooperación en materia judicial y de seguridad nacional. Con el objetivo de combatir el narcotráfico y la trata de personas, así como para reducir las actividades de grupos delictivos organizados, muchos países de la región mantienen acuerdos con otros u con organizaciones internacionales de asistencia humanitaria, a los fines de la transferencia de datos personales de migrantes, refugiados o solicitantes de asilo.

Estos acuerdos son particularmente amplios y no establecen límites ni garantías para el procesamiento de datos que impidan a los entes cometer abusos. A esta problemática se suma que la veracidad y fiabilidad de los datos recolectados dependen de autoridades arbitrarias, y con antecedentes de violación a las garantías procesales internacionalmente reconocidas (por ejemplo, como sucede con El Salvador y el intercambio de información que realiza con el Departamento de Seguridad Nacional de los Estados Unidos[9]).
En línea con esta posibilidad, se solicitó a las firmas encargadas de la investigación en cada uno de los países involucrados en este reporte que informasen sobre la existencia de estos acuerdos y de su contenido para el caso de que pudieran identificarse. A continuación, se comparten los resultados obtenidos:

Argentina	Entre los objetivos que establece la Ley de Política Migratoria Argentina, Ley N° 25.871, se encuentra el de “Promover promover el intercambio de información en el ámbito internacional, y la asistencia técnica y capacitación de los recursos humanos, para prevenir y combatir eficazmente a la delincuencia organizada transnacional”.

[9] https://www.accessnow.org/press-release/denuncia-dhs-el-salvador/

Al mismo tiempo, Argentina hace parte del Sistema de Intercambio de Información de Seguridad del MERCOSUR (el "SISME"), una herramienta de cooperación y asistencia mutua. A través de esta, las fuerzas de seguridad, policiales y demás organismos vinculados a políticas de seguridad de los estados de la unión aduanera colaboran con la lucha contra el crimen organizado. A partir de esta herramienta, podrán ser objeto de intercambio los datos relativos a personas, bienes y sucesos operacionales policiales y toda otra categoría que se estime pertinente incorporar a futuro[10].

Chile

La Ley N°21.016 tiene por finalidad facilitar el intercambio recíproco de información con otros países, para lo cual modificó el artículo 5 de la Ley de PDI y el artículo 3 de la Ley de Carabineros, obligando a las Fuerzas de Orden de la República de Chile, específicamente la PDI y Carabineros de Chile, a prestar la cooperación necesaria en cumplimiento de tratados internacionales ratificados y vigentes en Chile, incluyendo el intercambio de datos personales.

Chile ha suscrito diversos acuerdos con entidades no gubernamentales enfocados a la recolección y transferencia de datos personales de personas migrantes, refugiadas o solicitantes de asilo, entre los que podemos señalar:

I. Convención sobre el Estatuto de Los Refugiados (1951), (la "Convención") del Alto Comisionado de las Naciones Unidas para los Refugiados (la "ACNUR"), suscrito por Chile el 18 de enero de 1972.
II. Tratados sobre cooperación y colaboración en temas migratorios firmados entre Chile y la Organización Internacional para la Migración (la "OIM"): El Manual de la OIM sobre protección y asistencia para personas migrantes vulnerables señala en el apartado 6.3 expresamente la recopilación de datos de personas migrantes: "La recopilación de datos debe efectuarse de conformidad con la legislación nacional y regional sobre protección de datos. Puede haber casos en que, debido a la confidencialidad de los informes, sólo sea adecuada una divulgación limitada"[11].

A su vez, Chile ha suscrito los siguientes acuerdos con otros Estados:

I. Acuerdo sobre Residencia para nacionales de los Estados Parte del MERCOSUR, Chile y Bolivia: El referido acuerdo establece, en su artículo 7, el deber de los Estados de intercambiar información, por ejemplo,

[10] https://servicios.infoleg.gob.ar/infolegInternet/anexos/90000-94999/92016/texact.htm
[11] https://publications.iom.int/books/manual-de-la-oim-sobre-proteccion-y-asistencia-para-personas-migrantes-vulnerables-la

respecto de aquellos inmigrantes que hayan obtenido la residencia definitiva en el país receptor.

II. Convenio de Migración entre Chile y España (1961): El artículo 5 de este convenio establece el derecho de Chile para la revisión de los datos de aquellos candidatos que hayan sido preseleccionados por parte del Instituto Español de Emigración para emigrar de España y asentarse en Chile.

III. Declaración de la Organización para la Cooperación y el Desarrollo Económicos (la "OCDE") sobre el acceso de los gobiernos a los datos personales de entidades del sector privado: Esta declaración regula la forma en que los Estados deben solicitar los Datos Personales, así como el trato que se les debe otorgar al momento de su transferencia o intercambio con otros Estados con el objetivo de promover la confianza en el flujo de los datos transfronterizos.

Ecuador

Ecuador ha suscrito los siguientes acuerdos en relación a esta materia:

I. Acuerdo suscrito entre ACNUR y Ecuador para uso de sistema informático ProGres v4. Este sistema es parte integrante del Ecosistema de Gestión de Identidad de Registro de Población del ACNUR (PRIMES) y tiene como finalidad el registro y gestión de casos, garantizando una plataforma común para la colaboración.

II. Acuerdo Grupo de Trabajo para Refugiados y Migrantes (el "GTRM") en Ecuador y el Ministerio de Relaciones Exteriores y Movilidad Humana. Siempre que en el marco de cumplir con la finalidad y misión del GTRM se comparta información de una persona específica entre instituciones, se seguirá un estándar mínimo para ello, el que implica contar con la autorización del titular de los datos.

A su vez, los acuerdos que Ecuador suscribe con otros Estados son los siguientes:

I. Acuerdo para la implementación de la Plataforma Bilateral de Consulta de Alertas Migratorias Colombia – Ecuador: Esta plataforma es un programa informático que tiene la finalidad de compartir información, en tiempo real, sobre ciudadanos que registren boletas de detención. Esta herramienta mejorará la eficacia en la generación de alertas migratorias entre ambas naciones, lo cual aportará al trabajo de las instituciones policiales.

II. Estatuto Migratorio Andino - Decisión 878. Norma que regula el derecho comunitario de circulación y establece la residencia temporal y

permanente para los ciudadanos andinos en Bolivia, Colombia, Ecuador y Perú. La norma establece además el intercambio de información migratoria que podrá incluir flujos migratorios, alertas e impedimentos que pesaren sobre residentes en la CAN, así como de aquellos que sean requeridos por la autoridad judicial competente.

Guatemala, Honduras

Ni Honduras ni Guatemala cuentan actualmente con una ley de protección de datos personales, por lo que cualquier tratamiento abusivo de estos sería evaluado según la discrecionalidad de autoridades sin un marco regulatorio.

Estos dos países[12][13] cuentan con acuerdos no vinculantes de transferencias de datos personales con los Estados Unidos. Su objetivo es mejorar el control del flujo migratorio, la reducción del delito transfronterizo y las amenazas a la seguridad nacional. Estos acuerdos han permitido un número indeterminado de transferencias de datos personales de personas migrantes, incluyendo sus datos biométricos, desde los países centroamericanos a su par del norte.

La vigilancia transfronteriza de las personas migrantes a partir de sus datos personales es posible gracias a sistemas interoperables que se nutren de múltiples fuentes y a los que pueden acceder autoridades de los países signatarios de los acuerdos. Estos datos en manos de las autoridades migratorias de los EE.UU. son utilizados para analizar las solicitudes de asilo y/o de migración de las personas nacionales de los países que los envían, pero muchas veces, debido a la inexactitud de la información que contienen, las personas migrantes son afectadas con decisiones que rechazan o demoran sus solicitudes.

Al mismo tiempo, usualmente no encuentran a disposición mecanismos de remediación de las decisiones migratorias que las autoridades estadounidenses toman en base a estos datos. Los datos biométricos son datos sensibles, por lo que su tratamiento no debe ser tomado a la ligera.

El Salvador

El caso de El Salvador es similar al de los dos países centroamericanos ya analizados. Sin contar con una ley especial de protección de datos personales, cuenta[14] con un acuerdo no vinculante de transferencia de datos personales con Estados Unidos con los mismos objetivos declarados que en los casos anteriores.

[12] https://immigrationlitigation.org/wp-content/uploads/2022/10/IARC-ICE.pdf#page=6
[13] https://immigrationlitigation.org/wp-content/uploads/2022/10/IARC-ICE.pdf#page=13
[14] https://www.transparencia.gob.sv/institutions/rree/documents/338533/download

La diferencia es que El Salvador se encuentra en un estado de excepción que ha perdurado por más de un año, habilitando detenciones arbitrarias y otras violaciones a los derechos fundamentales de sus nacionales[15]. Por este motivo, es que el flujo de datos personales sobre las personas migrantes que se transfieren hacia los EE.UU. debería analizarse desde una perspectiva diferente.

Todo estado que no respeta las garantías procesales mínimas podría estar violando derechos fundamentales y, por ende, los datos que genera y comparte no ser fiables[16]. Por otro lado, reportes existentes dentro de las autoridades de Estados Unidos dan cuenta de esta situación, por lo que el diagnóstico sobre la fiabilidad de la información que comparten no surge únicamente desde las organizaciones de derechos humanos, sino también desde instancias gubernamentales del país de destino de preferencia de gran cantidad de migrantes salvadoreños.

México

Finalmente, México cuenta con acuerdos tanto vinculantes como no vinculantes[17] de transferencias de datos personales con Estados Unidos y con otros países limítrofes hacia el sur.

Los acuerdos no vinculantes con los EE.UU. son similares a los anteriormente descritos respecto de los países de Centroamérica pero también han celebrado un acuerdo vinculante, conocido como “Acuerdo del Bicentenario”, que reemplazará al Acuerdo de Mérida. Lamentablemente, diferentes solicitudes de acceso al contenido de este acuerdo no han sido fructíferas, por lo que aún se desconoce su composición. Luego, lo indicado ya en los apartados anteriores es trasladable al caso de México, que si bien cuenta con una regulación específica en materia de protección de datos personales (ver el apartado correspondiente en este reporte), podría no ser suficiente para resguardar los derechos de los mexicanos migrantes, al igual que de migrantes provenientes de otras nacionalidades que atraviesan el territorio mexicano en su trayecto hacia los EE.UU. También debemos mencionar que México es parte del Tratado entre México, Estados Unidos y Canadá, el cual dedica un capítulo respecto de la transferencia de información. Asimismo, México ha ratificado el Convenio 108, mismo que permite a México el intercambio efectivo y seguro de datos personales entre este país y la Unión Europea.

[15] https://www.accessnow.org/el-salvador-datos-poco-fiables-acorralan-personas-migrantes-en-ee-uu/
[16] https://www.accessnow.org/press-release/denuncia-dhs-el-salvador/
[17] https://r3d.mx/wp-content/uploads/SOC-2017.pdf

La existencia de los acuerdos mencionados en estos últimos apartados pone en riesgo la seguridad y la protección de los derechos de las personas migrantes. Por ello, deben ser abandonados por los países involucrados, acción que ha sido solicitada y sostenida[18] por una serie de organizaciones de la sociedad civil, entre las que se encuentra Access Now. Por ello, creemos necesario una vez más sostener la necesidad de respetar el derecho fundamental a migrar sin vigilancia[19] de toda persona, y de recibir asilo y otras formas de asistencia por parte de los países de tránsito y destino.

VI. PALABRAS FINALES

Este reporte presentó las situaciones específicas de un grupo de países de la región, que dan cuenta de los desafíos que enfrentan en materia de protección de datos personales. Latinoamérica tiene la oportunidad de posicionarse como una región que respeta los derechos fundamentales de las personas migrantes, su privacidad, y los datos personales de los millones de personas que habitan sus territorios, especialmente de las personas migrantes, refugiadas y solicitantes de asilo.

En la región, quienes deciden migrar de manera irregular deben afrontar grandes retos durante todo el trayecto hasta llegar a su destino. Además de los desafíos naturales que encuentran en el recorrido, como impenetrables junglas y desiertos, insuficiente acceso al agua potable y a alimento adecuado, existen otros peligros como los grupos criminales que intentan aprovecharse de su vulnerabilidad a través de robos, abusos e incluso homicidios.

Sumado a todos estos obstáculos, cuando la población migrante logra alcanzar la frontera del país de destino, se encuentran con una infraestructura de vigilancia que vulnera la protección de sus datos personales y otros derechos fundamentales, tornándose en una clara dificultad de ejercer el derecho fundamental a migrar.

Desde la necesidad de avanzar con la sanción y/o actualización de sus leyes de protección de datos personales, pasando por la falta de regulación en el despliegue de tecnologías con capacidad de vigilancia, más el sostenimiento de acuerdos de transferencia de datos personales en perjuicio de las personas migrantes, la región claramente debe avanzar en políticas coherentes y abandonar aquellas que se identifiquen en detrimento de sus propios nacionales.

Esperamos que los hacedores de políticas públicas y aquellas personas responsables de la toma de decisiones en cada uno de los países estudiados, y de los otros territorios que por razones de brevedad no se han incluido en esta investigación, reconozcan la importancia de respetar y velar por la protección de los datos personales y de la dimensión del desafío que supone la custodia de la privacidad.

[18] https://www.accessnow.org/press-release/pronunciamiento-terminar-acuerdos-biometricos-migrantes/
[19] https://www.accessnow.org/exigimos-que-las-personas-puedan-migrar-sin-vigilancia/

Para más información:

Franco Giandana Gigena
(franco@accessnow.org)
Ángela Alarcón
(angela@accessnow.org)
Gaspar Pisanu
(Gaspar@accessnow.org)

Access Now (https://www.accessnow.org) defiende y amplifica los derechos digitales de las personas usuarias en situación de riesgo en todo el mundo. Mediante la combinación de apoyo técnico directo, participación en políticas públicas integrales, incidencia internacional, subvenciones a organizaciones comunitarias y eventos como RightsCon, luchamos por los derechos humanos en la era digital.