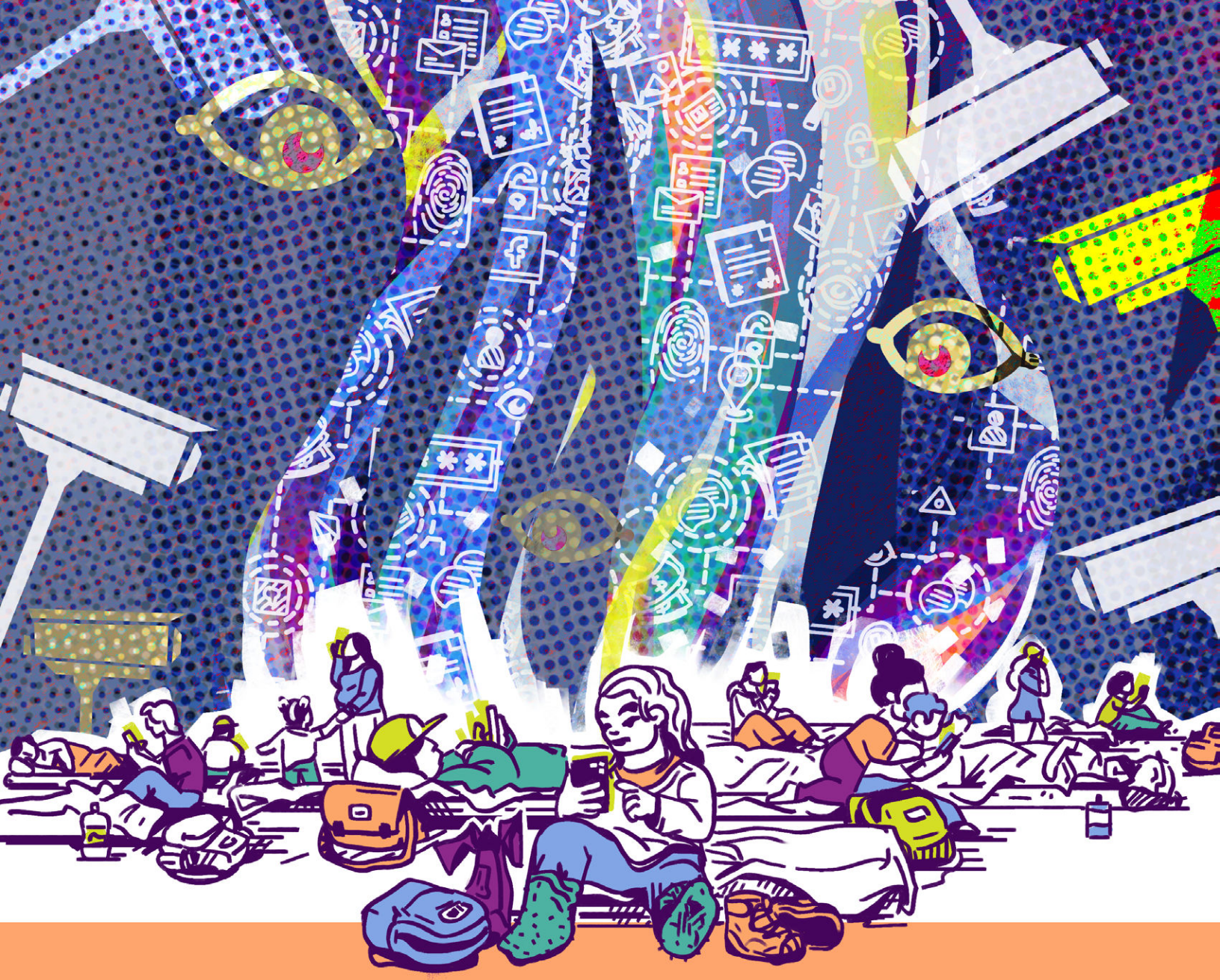


# PRIVACIDAD EN DESPLAZAMIENTO MIGRATORIO

Un diagnóstico sobre la vigilancia, protección de datos y seguridad digital en lugares de acogida de personas migrantes en México. Basado en testimonios.

#MIGRAR SIN VIGILANCIA
Coalición Latinoamericana

Este documento es una publicación de la **Coalición Latinoamericana #MigrarSinVigilancia**. La investigación fue coordinada, hecha, escrita y publicada por Adrián García (Centro LATAM Digital), Ángela Alarcón (Access Now), Haydeé Quijano (SocialTIC), Kathy Kruger (Al Otro Lado), Santiago Narváez (Red en Defensa de los Derechos Digitales), Veridiana Alimonti (Electronic Frontier Foundation), Victor Flores (International Refugee Assistance Project) y Ximena Mendieta (Centro LATAM Digital).

Agradecemos la colaboración de Alberto Écija, Franco Giandana, Giulio Coppi, Jesús Armando Juárez, Loren Giordano, Marcelo González, Milica Pandzic, Paolo Nigro, Rodolfo Zamaniego y Yamlek Mojica.

Y agradecemos particularmente el apoyo de cada albergue y casa de acogida que accedió a participar en las entrevistas que dan origen a este reporte: Border Line Crisis Center, Casa del Migrante Saltillo, Casa Frida, Casa Monarca, Casita Unión Trans y otros cinco albergues que prefirieron resguardar el anonimato.

Corrección de estilo: Ernesto Reséndiz

Ilustración y diseño: Andrés Artavia

Publicado en diciembre del 2024

Contacto:
Ángela Alarcón | Coordinadora de campañas para América Latina y el Caribe en Access Now
angela@accessnow.org

#MIGRAR SIN VIGILANCIA
Coalición Latinoamericana

# TABLA DE CONTENIDOS


**I. Introducción y metodología** **4**

**II. Tratamiento y protección de los datos personales en los albergues** **6**

a. Recolección de la información 6

b. Resguardo de los datos personales de las personas migrantes 10

c. Respuesta de los albergues a los incidentes de seguridad digital 12

**III. Acceso a la información de las personas migrantes** **13**

a. Vulneración de los dispositivos de las personas migrantes en la ruta 13

b. Robo de dispositivos pertenecientes a los albergues 15

c. Actores involucrados en los intentos y solicitudes de acceso a los datos de las personas migrantes 16

d. Decisiones migratorias a partir de los datos personales de las personas migrantes 24

**IV. Monitoreo y amenazas a los albergues y su personal** **26**

a. Servicios o dispositivos de los albergues que han sido brindados por terceros 26

b. Mecanismos de vigilancia dirigidos a los albergues 27

c. Amenazas digitales dirigidas al personal de los albergues 28

**V. Conclusiones y recomendaciones** **30**

# I. INTRODUCCIÓN Y METODOLOGÍA

Los datos personales de las personas migrantes son objeto de interés de múltiples agentes, tanto del orden público como fuera de él. Con el pretexto de mejorar la seguridad nacional, las autoridades habilitan mecanismos para hacerse de datos personales de este grupo de personas de manera intensiva y extractivista. Sumado a esto, la capacidad de cotejar dichos datos con otras bases de datos permite elaborar un perfil lo suficientemente descriptivo sobre quién es un individuo. Incluso cuando los datos hayan sido seudonimizados[1], la sumatoria de tanta información puede hacer a una persona identificable y perfilable. El procesamiento no consentido de estos datos es contrario a los derechos fundamentales y pone en riesgo la privacidad de la persona migrante, lo que puede llevar a la toma de medidas arbitrarias por parte de dichas autoridades.

Por otro lado, la delincuencia común y el crimen organizado sacan provecho de los datos personales de quienes migran para sus propios fines. A partir de robos, estafas y extorsiones, estos grupos criminales les despojan de su dinero y les captan para tráfico o trata de personas. Los actores relacionados con la causa por la que una persona emigró (por ejemplo, amenazas en la ciudad de origen) también muestran interés en cotejar la ruta de la persona migrante.

En medio de la vulnerabilidad física y digital que atraviesa gran parte de esta población, los albergues y las casas de acogida intentan cubrir sus necesidades y brindarles acompañamiento en una serie de procesos. Para hacer esto posible, los albergues recolectan datos personales de las personas en tránsito, lo cual traslada los riesgos antes mencionados a estos espacios.

El presente informe es una evaluación de los riesgos generados, por un lado, por los sistemas de vigilancia dispuestos a controlar la población migrante y, por el otro, de los riesgos que surgen de la vulneración a los datos personales que enfrentan los albergues que trabajan en el contexto migratorio en México, así como de las medidas de seguridad digital adoptadas para mitigarlos. El objetivo del informe es ser el punto de partida para el desarrollo de materiales, recomendaciones y prácticas que puedan servir para hacer frente a las amenazas identificadas.

Para lograr dicho diagnóstico, la metodología de investigación se centró en la obtención de información cualitativa mediante la realización de entrevistas a personal de diez albergues

[1] El proceso de seudonimización de datos pretende que un grupo de datos no pueda ser atribuidos directamente a una persona en tanto no se cruce con otro grupo de datos, es decir, el proceso se puede revertir.

distribuídos en el norte, centro y sur del país. Debido a la información compartida en los testimonios, algunos de los espacios de acogida prefirieron resguardar el anonimato.

El informe funciona además como un ejercicio para conocer sobre las problemáticas mencionadas a partir de las voces y experiencias de las personas que diariamente brindan apoyo en terreno a las personas en tránsito, y para sugerir rutas de trabajo sobre cómo atenderlas.

Este informe fue realizado por la Coalición Latinoamericana #MigrarSinVigilancia[2], una agrupación conformada por más de treinta organizaciones de la sociedad civil para servir como frente común para resguardar los derechos humanos de las personas migrantes a partir de la protección de sus datos personales. Las entrevistas fueron realizadas entre los meses de mayo a julio del año 2024.

[2] Coalición Latinoamericana #MigrarSinVigilancia. (2023). Recuperado el 10 de septiembre de 2024 de https://migrarsinvigilancia.org/

# II. TRATAMIENTO Y PROTECCIÓN DE LOS DATOS PERSONALES EN LOS ALBERGUES

## A. Recolección de la información

El acompañamiento, servicios y atenciones de los espacios humanitarios conllevan la recolección de datos sensibles. Dicho proceso se torna más complejo con el uso de tecnologías y las facilidades y riesgos que éstas conllevan. Las necesidades en materia de protección de datos personales compiten con la constante demanda para atender urgencias de primera necesidad de la población migrante, así como con las limitaciones financieras y de recursos humanos. Esto obliga a los espacios de acogida a priorizar la asignación de recursos para solventar necesidades de primer orden por encima de los desafíos digitales, lo que implica varias áreas de oportunidad y mejora para los procesos de procesamiento y resguardo de la información personal.

Según los testimonios del personal de albergues recopilados en este reporte, todos los espacios obtienen información biográfica y demográfica de sus personas usuarias en mayor o menor medida. Si bien muchas de las categorías de los datos recolectados son similares entre los espacios de acogida, no hay un estándar absoluto. En general, al momento de su recepción, éstos solicitan información personal como nombres, fechas de nacimiento, nacionalidades, países de origen y números de identificación. Algunos espacios también recolectan el número de personas que viajan en un grupo y los vínculos entre las mismas.

Bajo la lógica de la minimización en la recolección de datos personales y de priorizar la asistencia a las personas en tránsito, algunos albergues señalaron brindar acompañamiento incluso si quien requiere los servicios no proporciona sus datos personales, o no hay manera de verificar su veracidad. El principio de minimización de datos implica que sólo se deben recolectar los datos personales que sean estrictamente necesarios para brindar un producto o servicio.[3] En ese sentido, el accionar de estos albergues ilustra que es posible reducir, en ciertos casos, la cantidad de información recolectada, sin afectar el funcionamiento del espacio de acogida.

[3] Más información sobre minimización de datos disponible en: Access Now. (2021) *Minimización de datos, fundamental para la protección de la privacidad y la reducción de daños*. Recuperado el 18 de octubre de 2024 de https://www.accessnow.org/wp-content/uploads/2021/07/Data-Minimization-Minimizacion-Datos-Spanish. pdf

> *Tampoco estamos ciento por ciento seguros que nos den información real, pero sí es un requisito para estar en nuestro albergue poder contar con los datos necesarios para tenerlos en nuestra base de datos".*
>
> **– Albergue anónimo.**

> *Si la persona no está de acuerdo en proporcionar sus datos personales, no es un impedimento para poder proporcionarle nosotros los servicios. Tampoco es un impedimento el que no nos muestre una identificación oficial. Nosotros partimos de la buena fe de la información que nos proporciona la persona y hasta ahí".*
>
> **– Albergue anónimo.**

Dos albergues manifestaron también tomar fotografías como parte del proceso de ingreso, y algunos espacios realizan dos o hasta tres entrevistas adicionales a través de las cuales recopilan datos de las personas en tránsito, incluyendo datos sensibles como su condición de salud o si han sufrido delitos o crímenes durante su camino, los motivos de salida de su país de origen y sus planes de viaje.

Según los hallazgos, la petición de datos por parte de los albergues persigue principalmente tres propósitos:

**1.** Entender las necesidades de la población atendida con el objetivo de brindar acompañamiento y atención personalizada para el acceso a derechos y/o servicios.

**2.** Rendir cuentas a donantes, financiadores y organizaciones socias de los albergues.

**3.** Responder a solicitudes judiciales. Algunas de las personas entrevistadas mencionaron haber recibido solicitudes mediante oficio por parte de fiscalías estatales para corroborar la estancia de personas usuarias.

El procesamiento de datos personales sólo es legítimo cuando se basa en una de las causas reconocidas en las leyes e instrumentos sobre privacidad. En el contexto de las actividades que llevan a cabo los albergues, la habilitación del tratamiento de datos que mejor se ajusta es la permitida a partir del consentimiento del titular de los datos, es decir, la manifestación libre e informada por la cual es la propia persona quien acepta que se procesen sus datos personales. La solicitud de consentimiento debe ser transparente y accesible por parte de quien la pide.

El consentimiento, además, es un mecanismo adecuado para respetar el derecho a la privacidad y observar los principios de legalidad y de transparencia. El consentimiento libre e informado para el procesamiento de datos personales es recogido en al menos cuatro documentos internacionales sobre estándares y principios de protección de datos personales que competen a México[4].

El procesamiento de datos personales que no cuenta con una causa de legitimación para ser llevado adelante carece de base legal para ser realizado. Existen algunas excepciones legítimas para procesar datos personales cuando no existe el consentimiento del titular. De acuerdo con la Organización de los Estados Americanos (OEA)[5], esto es posible "cuando el responsable cuente con fundamentos legales alternativos, establecidos en el derecho interno o en el derecho internacional". Además señalan que en contextos humanitarios donde puede ser difícil contar con el consentimiento, el interés público y los intereses vitales del titular de los datos podrían funcionar como fundamento jurídico. Sin embargo, estas excepciones no aplican cuando el tratamiento de los datos pueda resultar en efectos perjudiciales para el titular.[6]

En esa línea, entre las áreas de oportunidad identificadas se encuentra la estandarización del procedimiento de obtención de consentimiento. De acuerdo con las entrevistas realizadas para este informe, algunos de los albergues se apegan al Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[7] al momento de solicitar el consentimiento de sus personas usuarias de forma verbal. Según el artículo 18 de este Reglamento, las personas pueden autorizar el tratamiento de sus datos de dicha forma. Sin embargo, contar con una versión escrita podría facilitar el posterior acceso, rectificación, cancelación y oposición al procesamiento de los datos personales por parte del titular de los mismos, en este caso, la persona migrante. La normativa también establece que la creación de bases de datos sensibles, como son los biométricos[8], debe siempre responder a un mandato legal, al ámbito territorial de aplicación, o bien que el responsable "lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga".[9]

[4] Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas; Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos; Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE; Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA.

[5] Organización de los Estados Americanos (OEA), Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos. (2022). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.* Recuperado el 25 de septiembre de 2024 de https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_ 2021.pdf

[6] Íbid.

[7] Cámara de Diputadas y Diputados del Congreso de la Unión. (2011). *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Artículo 18. Recuperado el 10 de septiembre de 2024 de https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

[8] Los datos biométricos son "datos personales obtenidos a partir de un tratamiento técnico específico. Están relacionados con las características físicas, fisiológicas o conductuales de una persona natural y permiten o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Access Now. *Radiografía normativa: ¿dónde, qué y cómo se está regulando la inteligencia artificial en América Latina?* (2024). Recuperado el 10 de octubre de 2024 de https://www.accessnow.org/wp-content/uploads/2024/02/LAC-Reporte-regional-de-politicas-de-regulacion -a-la-IA.pdf

[9] Íbid referencia número 7.

A pesar de que los procesos de recolección y consentimiento de datos personales no están estandarizados y son perfectibles, el razonamiento para el tratamiento de estos no es un tema que pase desapercibido para los albergues. Por ejemplo, al explicar sobre la implementación de los instrumentos de entrevistas y recolección de datos de personas en tránsito que utilizan, Sebastián Rodríguez, de Casa Frida, indicó que "*parte de lo que buscamos es fomentar la autodeterminación en las personas y sobre todo cuidamos mucho la expectativa en términos de que se busca la reintegración económica, social y cultural cuando una persona decide integrarse a los programas*".

Más allá de los resguardos actuales y de las necesarias mejoras que se pueden implementar en el proceso de solicitud de consentimiento, es indispensable considerar el contexto de vulnerabilidad en el que se encuentran muchas personas migrantes. La realidad material y el plan migratorio de las personas en tránsito dificultan o imposibilitan que cuenten con la opción real de decir que no consienten brindar sus datos personales, cuando de ello puede depender, aunque sea momentáneamente, su seguridad o el éxito de su viaje.

Por ejemplo, un albergue se refirió a una situación en la que, para que las personas migrantes pudieran acceder a una cobija durante el invierno, el gobierno del estado solicitó los datos personales de dichas personas. Esta situación ilustra una vez más la falta de opciones reales para que una persona migrante, refugiada o solicitante de asilo se niegue a la recolección de datos personales. Las personas migrantes se ven obligadas a tomar decisiones basadas en la necesidad de resguardar su bienestar y el de las personas con las que viajan, lo que significa un desbalance en la solicitud, que termina siendo desproporcionada. "*Vaya usted a saber qué tenían que llenar ahí. No sé si se llevaban todos los datos de la INE [documento de identificación] o nada más la enseñaban, pero esa vez sí requirieron que todas las personas tuvieran una INE para poderles dar una cobija*", indicó Judith Cabrera, del Border Line Crisis Center.

## B. Resguardo de los datos personales de las personas migrantes

El grado de sensibilidad de la información recabada, el perfil de los entes que podrían estar interesados en obtenerla y la asignación de recursos plantean un reto a la hora de pensar en soluciones para el resguardo seguro de los datos personales de quienes pasan por un albergue o casa de acogida. Las personas entrevistadas señalaron una serie de plataformas y mecanismos que utilizan para almacenar y/o resguardar dicha información. Si bien no necesariamente toda la información recopilada en un albergue sigue el mismo flujo de procesos, entre las herramientas destacables mencionadas se encuentran:

**KoBo Toolbox y proGres:** ambas son herramientas implementadas por la Agencia de la ONU para los Refugiados (ACNUR). En el caso de KoBo Toolbox, y de acuerdo con la propia agencia, se trata de una herramienta "con el fin de solventar posibles deficiencias en materia de recolección y análisis de datos", además de permitir que "una amplia gama de partes interesadas consulte o cuente con datos en tiempo real en el terreno".[10]

Por otra parte, el Sistema Global de Registro de Perfiles (proGres, por sus siglas en inglés) es el principal lugar de almacenamiento de datos del ACNUR, y cuenta con distintas versiones. Si bien los albergues no cargan directamente los datos en proGres, existen funcionalidades para integrar los datos recolectados en KoBo en proGres[11].

Anteriormente proGres funcionaba de manera descentralizada por locación, pero de acuerdo con la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja, desde 2018 la arquitectura mudó hacia una única base de datos global de personas que acceden a sus servicios[12]. ProGres es una de las piezas que forma parte del Ecosistema de Registro y Manejo de Identidad de la Población (PRIMES, por sus siglas en inglés). La agencia indica que PRIMES "abarca todas las herramientas y aplicaciones interoperables de registro, manejo de identidad y manejo de casos del ACNUR (tanto las existentes, como proGres y BIMS, como las que se desarrollen en el futuro)".[13]

[10] Agencia de la ONU para los Refugiados. (2023). *KoBoToolbox mejorará con iniciativa conjunta para recabar y analizar datos en contextos de desplazamiento.* Recuperado el 25 de septiembre de 2024 de https://www.acnur.org/noticias/announcements/kobo-toolbox-mejorara-con-iniciativa-conjunta-para-recaba r-y-analizar-datos

[11] Agencia de la ONU para los Refugiados. (2021). *Almacenamiento y transferencia electrónica de datos personales de personas de interés fuera de Primes.* Recuperado el 22 de octubre de 2024 de https://emergency.unhcr.org/sites/default/files/2023-12/SP%20ELECTRONIC%20STORAGE%20AND%2 0TRANSFER%20%20OF%20PERSONAL%20DATA%20OF%20PERSONS%20OF%20%20CONCERN%20OUTSIDE%20PRIMES%2C%202021.pdf

[12] International Federation of Red Cross and Red Crescent Societies. (2023). *Investigating safe data sharing and systems interoperability in humanitarian cash assistance.* Recuperado el 25 de septiembre de 2024 de https://interoperability.ifrc.org/wp-content/uploads/2023/11/DIGIDInteroperability-InvestigatingSafeDataSh aringandSystemsInteroperability.pdf

[13] Agencia de la ONU para los Refugiados. (s.f.). De *ProGres a PRIMES: preguntas frecuentes.* Recuperado el 25 de septiembre de 2024 de https://www.acnur.org/media/de-progres-primes-preguntas-frecuentes

**Uwazi:** Sistemas de Información y Documentación sobre los Derechos Humanos (HURIDOCS, por sus siglas en inglés) es una organización no gubernamental que, según señala su sitio web, provee apoyo a organizaciones de derechos humanos que recopilan, organizan y utilizan información. La organización cuenta con una aplicación para bases de datos que ellos mismos desarrollaron (Uwazi) y que está a disposición de sus socios, pero HURIDOCS también ofrece estrategias relacionadas con los objetivos y usos de la información, y con cómo procesar ésta de manera segura y ética.[14]

Al menos dos albergues mencionaron también ser parte de la Red de Documentación de las Organizaciones Defensoras de Migrantes (REDODEM). Según señalan en su sitio web, los datos que registran, sean sociodemográficos o de documentación de violaciones de derechos humanos, son útiles para concretar "acciones de incidencia política, social y jurídica".[15]

También existen esfuerzos mancomunados para el desarrollo de herramientas propias para llevar a cabo el almacenamiento de la información. Luis Zavala, de Casa Monarca, refirió que actualmente están desarrollando su propio sistema de gestión de información a través de una colaboración con profesionales en ingeniería en sistemas. Por otro lado, un albergue que optó por preservar el anonimato indicó que el software para almacenar datos lo desarrollaron desde el propio albergue, lo que ha sido útil para suplir necesidades específicas:

> *En esta base incluimos la información relacionada a la atención integral de acompañamiento de casos, a la atención humanitaria. Realmente este* software *nos ha permitido incluir cualquier tipo de pregunta en este primer registro. También facilita tareas administrativas y gestión de nuestros procesos de compras y permite obtener fácilmente indicadores para nuestros donantes. La base la almacenamos en un servidor local".*
>
> **– Albergue anónimo.**

En cuanto a buenas prácticas, a lo largo de las entrevistas se conoció la posición de varios albergues ante peticiones de autoridades del gobierno y organizaciones internacionales para tener acceso a información de la población migrante. En su mayoría, los albergues entrevistados fueron explícitos en reconocer la importancia de salvaguardar la privacidad de las personas en tránsito y afirmaron que no comparten información personal con ninguna entidad -inclusive cuando han sido presionados- a menos que cuenten con una orden judicial o con un acuerdo de compartición de datos. Esta particularidad se aborda con mayor detalle en la sección III.c.

[14] HURIDOCS. (s.f.). Recuperado el 25 de septiembre de 2024 de https://huridocs.org/

[15] REDODEM. (s.f.). Recuperado el 25 de septiembre de 2024 de https://redodem.org/

## C. Respuesta de los albergues a los incidentes de seguridad digital

Los protocolos de respuesta a incidentes de seguridad digital suelen contemplar actividades para minimizar el impacto que puede llegar a tener la materialización de riesgos que amenazan la confidencialidad y la integridad de la información personal, así como procesos de análisis y mejora con el fin de prevenir futuros incidentes. Aunque este tipo de protocolos son una parte esencial en los procesos de seguridad digital, es común que las organizaciones no cuenten con ellos, o por lo menos no de manera sistematizada. Esta situación plantea un área de oportunidad para el desarrollo e implementación de este tipo de estrategias.

Si bien un gran número de los albergues entrevistados declara contar con protocolos de respuesta a incidentes de seguridad, la gran mayoría de estos no incluyen respuestas a incidentes de tipo digital. Entre los testimonios recabados en este tema, las prácticas actualmente adoptadas están relacionadas principalmente al cambio de contraseñas ante accesos no autorizados a cuentas de correo electrónico o redes locales, o al cambio de números de teléfono ante llamadas de origen incierto o mal intencionadas, así como el bloqueo de dichos números. Como se verá más adelante, el tipo de amenazas digitales que enfrentan los lugares de acogida va mucho más allá de las descritas anteriormente, por lo que existe una importante necesidad de establecer protocolos que las aborden.

Además de las acciones de prevención y respuesta, otra parte esencial de los protocolos de seguridad digital es la documentación de incidentes. La falta de documentación puede provocar que las amenazas pasen desapercibidas y por lo tanto sean ignoradas o desestimadas. Asimismo, esta práctica es útil para respaldar denuncias en las que es necesario contar con evidencia sistematizada. Mediante la documentación es posible detectar patrones de amenazas y asociar los incidentes a coyunturas pertinentes, lo que puede facilitar la identificación del perpetrador en caso de que no se le conozca.

Un ejemplo relacionado a la documentación de incidentes en materia de seguridad digital es el llevado a cabo por la Casa del Migrante Saltillo, la cual declaró que, como parte del proceso para reportar al Mecanismo de Protección para Personas Defensoras de Derechos Humanos y Periodistas[16], documentan las estafas y extorsiones telefónicas que el albergue recibe: "*Se hace allí el reporte del incidente, se cambia la línea del teléfono y en la medida de lo posible se renueva el equipo*".

[16] El Mecanismo de Protección para Personas Defensoras de Derechos Humanos y Periodistas es una instancia federal que, con mayor o menor éxito, tiene como objetivo salvaguardar a las personas que sufren amenazas debido a su labor. Se puede consultar más información en https://www.gob.mx/defensorasyperiodistas y https://hchr.org.mx/puntal/prevencion-y-proteccion/proteccion-a-periodistas-en-riesgo/mecanismos-guber namentales/mecanismo-de-proteccion-federal/#:~:text=El%20Mecanismo%20tiene%20como%20objetivo ,tambi%C3%A9n%20a%20organizaciones%20y%20colectivos.

# III. ACCESO A LA INFORMACIÓN DE LAS PERSONAS MIGRANTES

## A. Vulneración de los dispositivos de las personas migrantes en la ruta

Al consultarle al personal de los albergues si conocían situaciones en las que se han vulnerado los dispositivos de las personas migrantes en la ruta, identificaron dos tipos de perpetradores: por un lado, actores de la delincuencia común y el crimen organizado, y, por el otro, las autoridades.

Respecto al primer grupo, el robo de teléfonos celulares es bastante frecuente[17]. Este tipo de delito puede estar matizado por un accionar violento de gravedad variada. "*Se dan mucho los secuestros y las extorsiones, por lo que les exigen las contraseñas para desbloquear los teléfonos*", indicó el personal de un albergue que prefirió preservar el anonimato.

Otro albergue señaló que en los últimos meses se han conocido historias en las que, tras el robo de los dispositivos de las personas migrantes, se detectó el uso de sus datos personales: "*Hemos sabido de personas que experimentaron el robo de datos personales de sus celulares durante el camino. Expresaron que les habían ingresado a sus cuentas y que, parece ser, extrajeron su información*", indicó César Barranco, de Casa del Migrante Saltillo.

Respecto a la vulneración de dispositivos por parte de autoridades, algunos albergues relataron historias en las que agentes sustrajeron los teléfonos celulares de las personas migrantes, tanto de forma temporal como de manera permanente:

[17] Además, la investigación *Acceso y uso de datos móviles en poblaciones migrantes* (2023) del Centro LATAM Digital señala que este tipo de hechos exacerba la vulnerabilidad preexistente en los migrantes en tránsito al limitar su acceso a servicios y trámites. Recuperado el 7 de octubre de 2024 de https://centrolatam.digital/wp-content/uploads/2023/04/Acceso-y-uso-de-datos-moviles-en-poblaciones-migrantes-1.pdf

*Yo creo que la amplia mayoría de las personas que viajan en autobús de Tapachula para Tijuana ha sufrido de ese tipo de violencia. No sabemos con certeza quién es el perpetrador. Las personas migrantes nos han indicado que fue la policía o la Guardia Nacional, pero realmente no sabemos si sean más bien los carteles".*

**– Susana Barrales, Casita Unión Trans.**

*Al albergue llegan muchas familias que las trae el Instituto Nacional de Migración (INM). Ellos detienen a las personas migrantes y como ven que van con niños pequeños, en vez de trasladarlos a la estación migratoria, les quitan sus pertenencias (básicamente su documentación y sus teléfonos), y les traen al albergue. Cuando nos dejan a nosotros este grupo de personas, también nos dejan una bolsa con teléfonos y otra bolsa con sus identificaciones".*

**– Albergue anónimo.**

El albergue añadió que muchos celulares vienen apagados, y que se desconoce si son las personas migrantes quienes los apagan antes de dárselos a los agentes del INM. Por otra parte, según refiere, el INM no le explica a las personas migrantes por qué les están quitando sus pertenencias ni les brindan algún tipo de documentación que lo acredite. Múltiple evidencia[18] apunta a que el INM contaría con dispositivos de análisis forense que permiten acceder a información en dispositivos móviles -inclusive si se encuentran bloqueados mediante clave- lo cual plantea preocupaciones de posibles violaciones a la privacidad cuando se confiscan o retienen los dispositivos.

[18] Red en Defensa de los Derechos Digitales (R3D). (2023). *Uso de las Tecnologías Digitales en los Contextos Migratorios: Necesidades, Oportunidades y Riesgos para el Ejercicio de los Derechos Humanos de las Personas Migrantes, Defensoras y Periodistas.* Recuperado el 8 de octubre de 2024 de https://r3d.mx/wp-content/uploads/Informe-_-Uso-de-las-tecnologias-digitales-en-los-contextos-migratorios-_-Necesidades-oportunidades-y-riesgos-para-el-ejercicio-de-los-derechos-humanos-de-las-personas-migrantes-defensoras-y-periodistas-R3D.pdf

## B. Robo de dispositivos pertenecientes a los albergues

Algunos de los albergues entrevistados declararon haber experimentado incidentes de robo de dispositivos. Si bien los motivos son desconocidos, se sospecha que podría tratarse de actos llevados a cabo por el crimen organizado en posible colusión con la autoridad, por personas que habrían estado trabajando en el albergue o que se hospedaron allí, o inclusive por parte de la comunidad que podría estar en contra de la presencia del albergue en esa zona. Personal de uno de los albergues narró que hace unos años sus oficinas administrativas sufrieron un incendio intencional. Tras las investigaciones pudieron corroborar que los perpetradores primero sacaron equipos de cómputo y otros dispositivos, y que posteriormente prendieron fuego al establecimiento. Al consultarle por coyunturas que pudieran ser relevantes, relató:

> *Tenemos una hipótesis relacionada a coyunturas más locales, no sabemos si está relacionada con otras coyunturas más regionales. Este hecho se dio en un momento crítico de un conflicto que el albergue ha mantenido con la colonia [barrio] circundante, en donde además ha participado constantemente la autoridad municipal en contra del albergue. Ya sabemos: los vecinos acusando que los albergues somos 'protectores de delincuentes' y etc. Entonces la autoridad municipal, a favor de la comunidad local, empezó a participar en una confrontación pública entre nosotros y ellos en los medios de comunicación.*
>
> *La autoridad municipal decía que la mayoría de migrantes eran 'criminales' o cometían 'prácticas criminales'. Pero a través de medios formales de acceso a la información les demostramos que no era correcto: que ni la autoridad municipal, estatal y federal habían detenido, procesado o encarcelado a personas migrantes en la magnitud que ellos decían. Luego el conflicto empezó a crecer y también se sumó el crimen organizado. Al final creemos que quien perpetró directamente el incendio fue el crimen organizado, no sabemos si en colusión con otro actor".*
>
> **– Albergue anónimo.**

Las estrategias adoptadas para recuperar información en caso de robo de dispositivos también varían entre los albergues. Uno de los espacios entrevistados que enfrentó un robo de este tipo declara que sólo fue necesario cambiar contraseñas, pues contaban con mecanismos de respaldo y protección de información a través de almacenamiento en la nube. Este formato de almacenamiento puede minimizar el riesgo de pérdida de información, al tiempo que plantea requerimientos robustos de seguridad digital para la protección de tales datos.

La diversidad de amenazas a las que se enfrentan los albergues relacionadas al robo de dispositivos y sustracción de información plantea la necesidad del desarrollo y adopción de estrategias y mecanismos de seguridad física y digital que se adapten al panorama de riesgos y capacidades de los mismos.

## C. Actores involucrados en los intentos y solicitudes de acceso a los datos de las personas migrantes

A lo largo de las entrevistas, el personal de los albergues narró distintas situaciones en las que actores ajenos al quehacer del albergue les han solicitado datos personales de las personas en tránsito que atienden. La mayoría de los albergues entrevistados indicó que únicamente comparten estadísticas o números totales de personas que han apoyado, y no los datos desagregados. Sin embargo, existen algunas instancias en las que se dan transferencias de los datos personales, las cuales pueden ser agrupadas en las siguientes categorías de acuerdo a los actores con quienes se comparten los datos:

**- Autoridades e instituciones públicas:**

Algunos albergues reconocieron casos en los que es necesario compartir los datos personales de las personas migrantes con autoridades o instituciones públicas, concretamente cuando: 1) la vida de la persona migrante está en riesgo, por ejemplo, en la búsqueda de personas desaparecidas o cuando existe una emergencia de salud; y 2) cuando hay un trámite administrativo-legal que lo requiera, como puede ser la regularización del estatus migratorio de una persona o el retorno voluntario asistido, así como el respectivo acompañamiento jurídico. Por ejemplo, personal de Casita Unión Trans ha cooperado y compartido información con autoridades para obtener atención especializada en casos específicos de violencia, buscando métodos alternos a la aplicación CBP One[19].

> *Solamente lo hacemos cuando el caso es complejo y nos urge aplicar por un medio que no sea CBP One. Hacemos una aplicación por violencia de género o si la persona viene huyendo de un problema muy fuerte o de persecución social. En ese caso, llevo a la persona a otras instancias donde compartimos información para que puedan darle acceso más rápido".*
>
> **– Susana Barrales, Casita Unión Trans.**

[19] CBP One es una aplicación para que personas migrantes que se encuentran en ciertos lugares de México programen citas para presentarse en un "puerto de ingreso" en la frontera suroeste de Estados Unidos. CBP One es problemática por varios motivos, incluyendo la asignación errónea de citas, la baja disponibilidad de citas en relación a la demanda, largos tiempos de espera, bloqueos frecuentes de la aplicación y el rechazo de las fotografías -por ejemplo, por su ineficiencia para registrar personas con tonos oscuros de piel-. Las personas solicitantes de asilo también enfrentan trabas debido a la falta de teléfonos inteligentes para acceder a la aplicación, la falta de conocimiento sobre cómo utilizarla, la dificultad para acceder a electricidad e internet y las limitaciones en el idioma, pues actualmente solo está disponible en español, inglés y creole haitiano. Más información disponible en https://www.accessnow.org/glosario-migrarsinvigilancia/

Resulta destacable que la mayoría de las personas entrevistadas narraron situaciones en las que se opusieron a solicitudes informales de entrega de datos personales por parte de autoridades o instituciones públicas, y les indicaron que recurrieran a los procedimientos judiciales establecidos si deseaban obtener dicha información. Por ejemplo, frente a un altercado entre personas migrantes y autoridades ocurrido en las afueras de uno de los albergues, el cual fue parcialmente registrado por las cámaras externas de las instalaciones, agentes del orden público exigieron la entrega del video o de las personas involucradas. Al respecto el albergue indicó:

> *¿En calidad de qué se las entrego [a las personas]? Yo no soy autoridad, yo no soy nadie para determinar si tal o cual persona fue. Si ellos la reconocen, pues que hagan lo que toque hacer en términos legales pero yo no puedo entregarles así nada más las personas o el video. Ellos decían que tenía que entregárselas porque estaban escondidas en el albergue, y que si no lo hacía iban a promover los recursos necesarios para que entrara la fuerza pública y demás. Yo le dije 'pues haz lo que te toque hacer'".*
>
> **– Albergue anónimo.**

Resulta alarmante que al menos uno de los albergues que prefirió preservar el anonimato relató que una autoridad no especificada le exige frecuentemente los datos desagregados. "*Sí hay que proveer mensualmente una lista del alcance que tenemos, por así decirlo. Entonces en esa lista no solamente puedes decir 'hoy atendí a 50 personas', sino que a fuerzas tienes que dar nombre, apellido o número de identidad y nacionalidad*", indicó personal de dicho albergue.

Además de las solicitudes expresas de entrega de datos, la vigilancia de la población migrante también constituye una forma de obtener información de las personas en tránsito. Por ejemplo, personal de un albergue de Tlaxcala señaló que el gobierno estatal decidió instalar cámaras en una avenida aledaña a sus instalaciones, como una respuesta del gobierno estatal para prevenir y atender situaciones de inseguridad y determinar si éstas son o no provocadas por personas migrantes. Al preguntarle sobre quién tiene acceso a los videos captados por estas, el albergue indicó:

> *La medida conlleva un riesgo y es que no sabemos para qué utiliza la información la autoridad, en este caso la Secretaría de Seguridad Ciudadana, y quién tiene acceso a esa información, y qué uso se le da a esa información.*
>
> *Entendemos que las cámaras son manejadas y están conectadas con el C5, que es el centro de control de todo el sistema de videovigilancia de la policía estatal, pero no sabemos sus características tecnológicas".*
>
> **– Albergue anónimo.**

El Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano (C5) fue inaugurado en Tlaxcala en el año 2023. Medios locales han reportado que el Centro cuenta con tecnología de reconocimiento facial en más 1700 puntos de monitoreo[20]. Los sistemas de vigilancia masiva con capacidades remotas de reconocimiento facial e identificación con otros datos biométricos han sido ampliamente cuestionadas por la sociedad civil debido, entre otras razones, a la falta de consentimiento por parte de las personas captadas en las imágenes y la vulneración al principio de inocencia de dichas personas, lo que en definitiva los convierte en tecnología que atenta contra la privacidad desde su diseño[21].

### - Actores humanitarios y de cooperación internacional:

El personal de los albergues entrevistados identificó circunstancias en las que organizaciones dedicadas a la asistencia humanitaria, así como organismos de cooperación internacional que financian los albergues, recolectaron o solicitaron los datos personales de la población en tránsito atendida.

ACNUR fue mencionada por dos albergues como una de las organizaciones con la que, a partir de convenios firmados[22], se comparte información de personas en tránsito para casos concretos, como es el programa de integración local, que incluye a personas refugiadas. Esta transferencia de información, dependiendo del albergue, puede ocurrir a través de correos electrónicos o aplicaciones de mensajería, o bien a través de KoBo, una herramienta de ACNUR para recopilar, gestionar y analizar datos, la cual abordamos en la sección II.b. de este reporte.

[20] El Diario de Tlaxcala. (2023). *Inauguran el Centro de Monitoreo C5 en Tlaxcala: Un paso hacia la seguridad integral.* Recuperado el 26 de septiembre de 2024 de https://www.eldiariodetlaxcala.com/134744-2/

[21] Access Now. *Ban Biometric Surveillance.* (s.f.). Recuperado el 26 de septiembre de 2024 de https://www.accessnow.org/campaign/ban-biometric-surveillance/

[22] Un albergue señaló que a través del "Acuerdo de Protección de Datos" (nombre del convenio firmado con ACNUR) transmiten primordialmente información estadística por medio de KoBo como parte de la rendición de cuentas y seguimiento a indicadores del proyecto. Cuando se requiere se comparten datos personales. Un ejemplo de esto podría ser cuando el albergue desea canalizar a una persona refugiada para atención de ACNUR por algún aspecto de protección (salud, legal o de integración). En esos casos se comparte lo mínimo necesario para la canalización; es decir, nombre, edad y nacionalidad.

Además del intercambio de datos bajo convenio con ACNUR, al menos una de las casas de acogida señaló que dicha agencia está interesada en registrar los datos de las personas en tránsito en situaciones que, desde su perspectiva, no necesariamente lo ameritan, como mediante el proceso de acompañamiento que dicha organización ofrece a personas en tránsito que buscan solicitar asilo en un país. Es pertinente subrayar que, por un lado, el principio de minimización de datos establece que solo se deben recolectar aquellos datos que sean estrictamente necesarios para el fin que se persiga, y que, además, no es obligatorio contar con el acompañamiento de ningún ente para presentar una solicitud de asilo en un país. Al respecto el albergue indicó:

> *Muchas organizaciones estamos muy preocupadas porque la dinámica es que un poco se incita a que se tenga que pasar por el sistema de registro ante el ACNUR y que ahí se concentre la mayoría de la información. Se invita y se insiste mucho en que pasen por sus sistemas de registro como una práctica común. En ese sentido nos parece que no siempre terminaría siendo una buena práctica".*
>
> **– Albergue anónimo.**

Aparte de la recolección y compartición de datos con ACNUR, al menos uno de los albergues con quien tiene convenio refirió que esta agencia es también su principal financiador. Esto puede generar efectos disuasorios para objetar las solicitudes de acceso a datos personales por parte de dicha agencia -en este caso datos personales de solicitantes de asilo o refugiadas, categorías que cuentan con protecciones especiales bajo la Convención sobre el Estatuto de los Refugiados[23] y el Protocolo sobre el Estatuto de los Refugiados[24]- mientras que al mismo tiempo deben cumplir con las exigencias propias de un ente que subvenciona la capacidad de funcionamiento de un albergue.

El almacenamiento de datos personales de la población en tránsito por parte de ACNUR reviste preocupaciones, toda vez que la agencia tiene acuerdos con autoridades estadounidenses, como el Departamento de Seguridad Nacional[25] (DHS por sus siglas en inglés), para el intercambio de información biográfica y de datos biométricos. La evaluación del impacto a la privacidad del acuerdo, realizada por el DHS[26], reconoce riesgos que no han sido totalmente mitigados, como el hecho de que el titular de los datos personales (la persona

[23] *Convención sobre el Estatuto de los Refugiados.* (1951). Recuperado el 26 de septiembre de 2024 de https://www.acnur.org/sites/default/files/2023-05/Convencion_1951.pdf

[24] *Protocolo sobre el Estatuto de los Refugiados.* (1967). Recuperado el 26 de septiembre de 2024 de https://www.acnur.org/sites/default/files/legacy-pdf/5b076dcd4.pdf

[25] El memorando no está disponible públicamente. La evaluación a la privacidad de dicho acuerdo, realizada por el DHS, hace mención al mismo: https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf

[26] Department of Homeland Security. (2019). *Privacy Assessment for the United Nations High Commissioner for Refugees (UNHCR) Information Data Share*. Recuperado el 26 de septiembre de 2024 de https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf

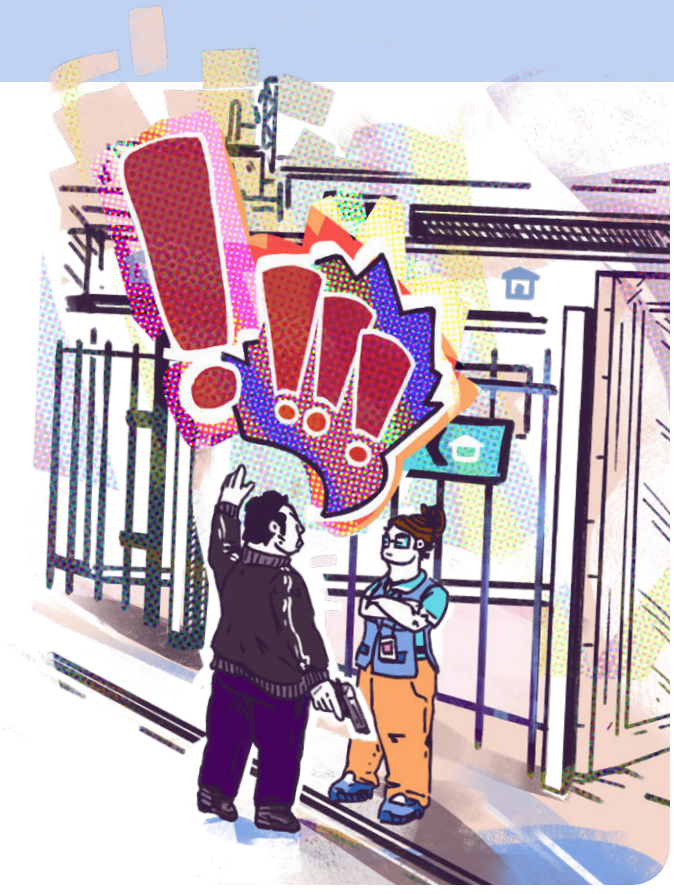
en tránsito) puede desconocer en dónde o con quién más se compartirán sus datos, o que estos sean utilizados para propósitos fuera de lo especificado en el acuerdo, por lo que existe el riesgo de que los mismos puedan ser usados en prácticas de vigilancia y de perfilamiento. Esta situación plantea un nuevo nivel de complejidad, pues la instancia que recopila y comparte los datos personales es un actor humanitario.

La colisión entre derechos e intereses puede ocurrir con otros entes financiadores. Uno de los albergues anotó que una de las agencias de cooperación que les financia les ha solicitado listas de asistencia, de registro y de beneficiarios, entre otros. Este requerimiento es percibido como ilegítimo, cuestionable y arbitrario, pues no existe una correlación entre conocer la identidad de las personas que pasan por un albergue y el quehacer de una agencia financiadora. El personal del albergue reflexionó al respecto:

> *Hemos discutido mucho sobre la obligación de que las agencias de cooperación tengan información que, para el fin que corresponde y está en el proyecto, pues no les tocaría. Pero eso es un problema que luego no logra solucionarse fácilmente en la práctica con las agencias de cooperación. Porque en ese caso tendrían que firmarme ellos también un documento que acredite que ellos también van a tener responsabilidad sobre el uso de la información".*
>
> **– Albergue anónimo.**

### - Crimen organizado y terceros no verificados:

Una problemática que refirieron varios albergues es la falta de claridad sobre qué actor está solicitando los datos personales de una persona migrante. Son muchos los actores que desean acceder a este tipo de información para sus propios intereses: traficantes de personas (también conocidos como "coyotes"); tratantes de personas; familiares mal intencionados; delincuentes comunes; narcotraficantes y crimen organizado. Estos grupos también pueden operar en conjunción entre ellos o con autoridades corruptas. Los albergues son en gran medida conscientes de lo codiciada que es la información de las personas migrantes y del papel que las casas



de acogida juegan para resguardar su privacidad y con ello, su seguridad. "*Hay una lógica detrás, y es que cada persona que pasa por nuestras organizaciones o que son orientados por nuestros servicios puede ser una persona menos que caiga víctima o cliente de las dinámicas del crimen organizado*", resumió Sebastián Rodríguez, de Casa Frida.

La experiencia y el contexto han ayudado a los albergues a identificar cuando una solicitud es sospechosa y no necesariamente proviene de quien dice venir. Cuando se carece de certeza sobre quién les contacta, en general los albergues optan por ignorar el pedido o negar la entrega de la información. Un albergue lo ejemplificó de la siguiente manera:

> *Una vez llegó un sujeto diciendo que era de la Guardia Nacional pidiendo información de una persona. En teoría la persona que vino de la Guardia Nacional no venía uniformada, no venía identificada, no sabemos si pertenecía al crimen organizado.*
>
> *También una vez llegó un grupo armado pidiendo información sobre una persona en movilidad. Nadie puede dar información de alguien que se encuentre albergado aquí dentro, únicamente en casos de personas que la autoridad anda buscando y sólo si vienen con una orden judicial, de otra forma no es posible".*
>
> **– Albergue anónimo.**

Otro recurso utilizado para intentar acceder a información de personas migrantes a través de los albergues es por medio de llamadas telefónicas y redes sociales, lo que dificulta que se pueda confirmar quién es el solicitante:

> *Con frecuencia recibimos llamadas: 'es que le hablo de la zona militar tal y pedimos información de cuántas personas tienen, cuántos datos, etc'. Pensamos: o ciertamente es el ejército, o es el crimen organizado. Ambas cosas son de riesgo para nosotros.*
>
> *También nos han hecho llamadas telefónicas con cierta frecuencia para pedirnos saber si tal o cual persona se encuentra o se encontró en el albergue en determinado periodo. Es muy difícil para nosotros saber si en efecto estamos hablando con el familiar de la persona que está siendo buscada, o más bien intuimos que es un traficante u otro elemento del crimen organizado. A veces por la forma de preguntar y la orientación de las preguntas ya podemos diferenciar quién es quién, eso lo adquirimos con la práctica".*
>
> **– Albergue anónimo.**

En el caso de Casa Frida y Casita Unión Trans, al tratarse de lugares de acogida que específicamente brindan apoyo a personas en tránsito que han sido víctimas de violencia y que se identifican como parte de la población LGBTIQ+, quienes pretenden atacarles pueden estar motivados por las intersecciones de dicha población, y trasladan las amenazas también al personal de los albergues:

> *Hemos recibido ciertos ataques o ciertos intentos de comunicarse a nuestras redes sociales diciendo 'oigan sabemos que fulanito, fulanita está ahí con ustedes, queremos contactarle'. Nuestros protocolos son muy estrictos y nunca compartimos información con nadie exterior. Primero vamos con la persona, si es que la persona está con nosotras, y le explicamos la situación para que ella decida. Y entonces ahí ya sale muchas veces que no quieren estar en contacto porque pueden ser sus agresores o alguien cercano a sus agresores".*
>
> **– Sebastián Rodríguez, Casa Frida.**

> *Me han amenazado, pero nunca han obtenido la información de nadie. Es peligroso cuando vienen personas huyendo del crimen organizado, que pasa mucho. Pero a veces las personas migrantes también huyen de sus parejas porque han sido violentadas. Más de una vez las parejas han llegado hasta nuestro albergue buscando a la persona, y entonces me toca decirles que se tienen que retirar o le voy a hablar a la policía, que ya lo he hecho. De las parejas también he recibido amenazas".*
>
> **– Susana Barrales, Casita Unión Trans.**

Existe también preocupación por sospechas de filtración de datos personales de personas en tránsito por parte de terceros no identificados, que podrían implicar la colusión de más de un tipo de agente perpetrador. Casa Frida indicó que las personas migrantes reportan haber recibido llamadas de supuestos funcionarios públicos que les ofrecen acceso a procedimientos alternos para facilitar su proceso migratorio. Se desconoce la veracidad de la autoría de las llamadas e incluso existen sospechas de que hayan sido realizadas por agentes delincuenciales, pero el contenido de las mismas reviste riesgos independientemente de quién las realiza:

*Beneficiarias de nuestros programas han sido contactadas por supuestos funcionarios públicos para ofrecerles rutas alternas más rápidas para sus procesos. Esto es muy alarmante porque podría haber extracción de datos desde las mismas autoridades si de verdad son ellos. Aunque también sospechamos que sea resultado de la compra de chips [tarjetas SIM] en la calle. Creemos que pueden haber redes delincuenciales que se dedican a identificar cuando una persona en contexto de movilidad compra un número de teléfono mexicano.*

*Hay varias dinámicas complejas, porque, por ejemplo, en todos los puntos donde las personas migrantes se presentan ante las autoridades, las propias instituciones tratan de convencerles de comprar los chips desde ahí".*

**– Sebastián Rodríguez, Casa Frida.**

## D. Decisiones migratorias a partir de los datos personales de las personas migrantes

Los acuerdos y tecnologías que respaldan el extractivismo de datos personales de las personas migrantes, así como la cuestionable obtención del consentimiento de las personas en tránsito para que procesen sus datos personales, además de la arbitrariedad y opacidad que con frecuencia rodea la toma de decisiones migratorias, delinean un panorama de desprotección para esta población.

Al consultar a los albergues si conocían de situaciones donde las autoridades tomaran medidas migratorias sin explicación -lo que podría ser señal de un posible perfilamiento a partir de datos personales previamente recolectados-, uno de ellos se refirió a los procesos de solicitud de la condición de refugiado, o de regularización temporal o permanente:

> *"A muchas personas se les niega este proceso porque tienen lo que aquí llaman la "ficha roja" o "alerta roja" [también conocida como alerta migratoria]. Esto quiere decir que tienen algún impedimento en su país de origen o en México, pero ellos en general no lo saben. Con ese argumento la autoridad desecha o deniega este tipo de procesos.*
>
> *Muchas organizaciones, incluyéndonos, intentamos conocer más al respecto, porque ¿cómo puede una persona argumentar algo a su favor si no sabe de qué está siendo acusada? Pero es casi imposible saber por qué tienen la "alerta roja". Hay muchos casos de ese tipo donde se les niegan estos procesos tan sólo por estar "fichados" y a la persona no le indican por qué. Puede ser por todo y por nada; una determinación muy arbitraria de la autoridad".*
>
> **– Albergue anónimo.**

La información proporcionada por el albergue resuena con la denuncia administrativa presentada ante el DHS en 2023 por Access Now, el Centro Nacional de Justicia para los Inmigrantes y Cristosal a través de la Clínica de Derechos Humanos Internacionales y Resolución de Conflictos de la Facultad de Derecho de Stanford[27]. La denuncia pide que se investigue el uso que Estados Unidos hace de datos potencialmente erróneos provenientes

[27] Access Now. (2023). *Organizaciones de derechos humanos piden investigación sobre intercambio de información entre Estados Unidos y gobiernos autoritarios para procesos migratorios.* Recuperado el 26 de septiembre de 2024 de https://www.accessnow.org/press-release/denuncia-dhs-el-salvador/

específicamente de autoridades de El Salvador, país que lleva más de dos años bajo un cuestionable "estado de excepción" que ha justificado la detención arbitraria de personas[28], y cuyos datos personales se comparten luego con otros estados.[29]

Dicha denuncia señala que El Salvador emite notificaciones rojas ante INTERPOL[30] a un ritmo desproporcionadamente alto. Aunque 195 países son miembros de INTERPOL y El Salvador tiene una población muy pequeña en relación con otros países miembros, al momento del envío de la denuncia, el estado salvadoreño representaba alrededor del 16% de las notificaciones rojas activas[31]. La denuncia señala que en varios casos, el gobierno de El Salvador emitió notificaciones rojas persecutorias que, como luego los acusados y su defensa lograron demostrar en los tribunales, se basaban en órdenes de arresto falsas, acusaciones infundadas u otras pruebas no corroboradas.

La denuncia también señala que, en ocasiones, el DHS incluso expulsó a solicitantes de asilo proveniente de El Salvador sin darles la oportunidad de apelar la decisión y cuestionar la veracidad de las pruebas presentadas contra ellos. De vuelta en El Salvador, parte de estas personas han sido detenidas, encarceladas y sometidas a nuevas formas de persecución.

[28] Human Rights Watch (HRW). (2022). *El Salvador: Abusos generalizados durante el régimen de excepción.* Recuperado el 22 de octubre de 2024 de https://www.hrw.org/es/news/2022/12/07/el-salvador-abusos-generalizados-durante-el-regimen-de-excepcion

[29] Íbid referencia número 27.

[30] "Una Notificación Roja es una solicitud dirigida a las fuerzas de seguridad del mundo entero para localizar y detener provisionalmente a una persona en espera de su extradición, entrega o acción legal similar. Una Notificación Roja no es una orden de arresto internacional. Las personas son buscadas por el país miembro solicitante o un tribunal internacional. Los países miembros aplican sus propias leyes para decidir si arrestan o no a una persona. La mayoría de las Notificaciones Rojas están restringidas al uso exclusivo de las fuerzas de seguridad" [traducción propia]. INTERPOL. View Red Notices. (s.f.).
Recuperado el 22 de octubre de 2024 de https://www.interpol.int/en/How-we-work/Notices/Red-Notices/View-Red-Notices

[31] Íbid referencia número 27.

# IV. MONITOREO Y AMENAZAS A LOS ALBERGUES Y SU PERSONAL

## A. Servicios o dispositivos de los albergues que han sido brindados por terceros

Para aliviar la carga de algunas de las necesidades de los albergues, el apoyo en ocasiones puede venir en forma de donación de recursos. A diferencia de otros bienes, como la alimentación o la ropa, los dispositivos y servicios digitales representan una preocupación en tanto pueden ser configurados, monitoreados o vulnerados remotamente. Contar con socios de confianza y desarrollar capacidades sobre el uso de la tecnología brindada es vital para reducir los riesgos.

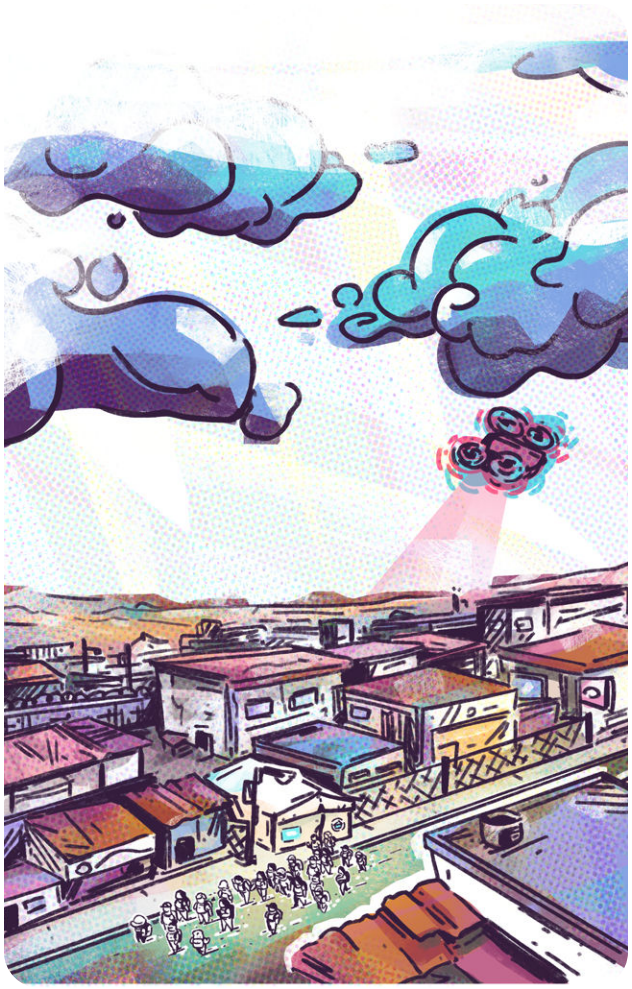
Para efectos del alcance de este reporte, indagamos si los albergues habían recibido elementos de esta índole y por parte de qué actor. Las personas entrevistadas señalaron una variedad de servicios, dispositivos y donantes. La donación del servicio de redes de internet y de computadoras fueron los aspectos señalados con mayor frecuencia (cuatro y tres albergues, respectivamente). Además de esto se mencionaron sistemas de videovigilancia, pantallas y programas de procesamiento de texto, y en un caso, el servicio de correo electrónico a través de May First Movement Technology[32].

Respecto a quiénes donaron la tecnología, los albergues mencionaron organizaciones nacionales de sociedad civil, organizaciones humanitarias internacionales, agencias u organizaciones de la ONU (ACNUR y la Organización Internacional para las Migraciones), sector privado y gobierno.

Respecto al sector gubernamental, uno de los albergues indicó que el gobierno les brindó el *router* tras la implementación de la aplicación CBP One para programar citas antes de presentarse en un puerto de entrada en la frontera suroeste de Estados Unidos, de manera que las personas migrantes se puedan conectar a esa red, mientras el albergue utiliza otra.

[32] May First Movement Technology es una cooperativa sin fines de lucro de organizaciones y activistas en Estados Unidos y México. De acuerdo con su sitio web, alojan más de 10.000 direcciones de correo electrónico y más de 2000 sitios web en su hardware de propiedad colectiva que se ejecuta exclusivamente en discos cifrados. Además de alojar esos datos, la organización participa en redes, coaliciones y campañas relacionadas con la tecnología. Más información disponible en: https://mayfirst.coop/es/

## B. Mecanismos de vigilancia dirigidos a los albergues



Durante las entrevistas, algunas personas expresaron preocupación tanto por medidas de monitoreo focalizado -por ejemplo, al sospechar que sus comunicaciones pueden estar intervenidas- como por el avistamiento de tecnología que habilita la vigilancia masiva, por ejemplo, vehículos aéreos no tripulados (drones). Uno de los albergues señaló que desde el 2021 empezaron a ver drones sobrevolando sus instalaciones y zonas aledañas. Si bien no tienen certeza de quién envía los dispositivos, señalan que en ese mismo periodo ocurrió uno de los tránsitos masivos más relevantes en los últimos años en México y que el Instituto Nacional de Migración (INM) con frecuencia consultaba a los albergues, tanto formal como informalmente, cuántas personas migrantes pasaban por allí. El albergue detalló:

> *Creemos que una forma de tener acceso a cuántos migrantes había en el albergue es volando los drones. Todavía en el último medio año por lo menos en dos ocasiones confirmamos que siguen volando drones. No sabemos si es de la misma autoridad municipal, estatal, o las instituciones de seguridad pública, pero constantemente vemos este tipo de medidas.*
>
> *Además, tras el diálogo que hemos tenido con las autoridades migratorias sabemos que hay cámaras instaladas a lo largo de las vías del tren, por lo que para ellos es relativamente fácil ir monitoreando cuántas personas migrantes vienen a bordo del tren, en qué puntos van pasando, etc. O sea, ya los están esperando con prácticas de contención y de detención migratoria. Pero también justo como llegaban a nuestro albergue grupos grandes de migrantes, entonces el Instituto quería ir monitoreando cuántos migrantes había".*
>
> **– Albergue anónimo.**

La narrativa predominante para justificar la adopción de este tipo de medidas de vigilancia es otorgar mayor seguridad. Si bien existen fines legítimos y proporcionales para ciertos tipos de monitoreo, la vigilancia biométrica remota masiva es inevitablemente invasiva de la privacidad de las personas. Específicamente se socava su derecho al consentimiento para el procesamiento de sus datos personales, se mina el principio de presunción de inocencia -pues se vigila a toda una población sin que haya una base legal que lo justifique- y puede generar un efecto inhibitorio entre la población observada. La falta de claridad acerca de la recolección y uso de la información, así como la criminalización y militarización de la política migratoria en México[33] y la posible colusión entre el crimen organizado y autoridades del gobierno[34] también son factores de riesgo para la protección de los datos personales de las personas en tránsito.

## C. Amenazas digitales dirigidas al personal de los albergues

Quienes se acercan a los albergues con la intención de conocer datos personales no se interesan únicamente en las personas en tránsito, sino también en la información y hábitos del personal del albergue. Esto representa un riesgo para su seguridad, pues al ser defensores y defensoras de una población vulnerable se convierten también en blanco de actores amenazantes. "*Cada vez es más frecuente que a alguien del personal le estén intentando hackear el celular o algún tipo de cuenta, incluso ha habido extorsión o fraude por medio de líneas telefónicas propias del albergue*", indicó César Barranco, de Casa del Migrante Saltillo.

[33] Más información disponible en el reporte del Programa de Asuntos Migratorios y el Programa de Seguridad Ciudadana de la Universidad Iberoamericana. (2024). *La militarización del Instituto Nacional de Migración y sus implicaciones en las violaciones a derechos humanos de las personas migrantes*. https://readymag.website/u3038421399/informeINM/

[34] Red en Defensa de los Derechos Digitales (R3D). (2023). *Uso de las Tecnologías Digitales en los Contextos Migratorios: Necesidades, Oportunidades y Riesgos para el Ejercicio de los Derechos Humanos de las Personas Migrantes, Defensoras y Periodistas.* Recuperado el 8 de octubre de 2024 de https://r3d.mx/wp-content/uploads/Informe-_-Uso-de-las-tecnologias-digitales-en-los-contextos-migratorio s-_-Necesidades-oportunidades-y-riesgos-para-el-ejercicio-de-los-derechos-humanos-de-las-personas-migrantes-defensoras-y-periodistas-R3D.pdf

*Con mucha frecuencia piden datos míos como director. Yo intuyo que es para corroborar datos, porque a veces ni siquiera piden dinero. Pero luego, analizándolo con el equipo, creemos que lo único que hacen es ir avanzando en el conocimiento de la información personal que tienen para corroborar quién soy, de dónde soy, dónde me muevo, qué hago, quién está a cargo de qué, cuáles son los horarios. Y si uno se engancha con la llamada, pues estaríamos proporcionando información que en suma es delicada".*

**– Albergue anónimo.**

Las sospechas de vigilancia y monitoreo alarman al personal de los albergues. Algunas casas de acogida mencionaron específicamente el temor de que las líneas telefónicas estuvieran intervenidas. El peligro que revierte este tipo de prácticas pasa por la extracción de datos personales y de cómo estos pueden ser instrumentalizados por parte del agente ejecutor. Conocer la locación de una persona defensora de derechos humanos, por ejemplo, puede trasladar los riesgos del plano digital al plano físico. Saberse bajo vigilancia también conlleva un efecto inhibitorio que mantiene a la persona en alerta sobre qué acciones tomar y qué medios de comunicación utilizar, todo esto en el marco de la atención crítica brindada a la población vulnerable.

*No sé si sea paranoia, pero me parece que las personas que defendemos los derechos humanos de las personas migrantes somos incómodas en ambos lados de la frontera. Yo creo que siempre estamos a un pasito de pasar de la vigilancia masiva a la focalizada. Mi Whatsapp, por ejemplo, en ocasiones se ha comportado de manera extraña".*

**– Judith Cabrera, Border Line Crisis Center.**

En otros casos, el personal de albergues también ha sido víctima de robo de datos personales para extorsión, lo que les ha significado tiempo y recursos para solventar la situación:

*"Uno de los compañeros solicitó un préstamo personal, no sé si a través de una aplicación que bajó o si fue en línea, con un teléfono propio del albergue. Al dar clic extrajeron todos sus datos. A partir de ahí fue víctima de extorsión: le dijeron que iban a usar sus datos, su imagen y su voz de manera negativa si no depositaba una cantidad de dinero. En el albergue cancelamos la línea e hicimos la denuncia correspondiente y hasta el momento parece ser que no ha pasado a más. Anteriormente a otra compañera le pasó, aunque esa vez fue con su propio celular".*

**– César Barranco, Casa del Migrante Saltillo.**

# V. CONCLUSIONES Y RECOMENDACIONES

Los albergues y casas de acogida son lugares donde tanto en el espacio físico como en el digital convergen riesgos para la protección de las personas migrantes y del propio personal que les asiste. Estas problemáticas transcurren al mismo tiempo que se brinda acompañamiento de diversa índole a las personas en tránsito para atender una variedad de necesidades, lo que implica una carga adicional. En este contexto, la seguridad digital y la protección de datos personales son cada vez más un asunto de interés en la agenda de trabajo de muchos de estos espacios. Para incorporar buenas prácticas en estos procesos, se sugieren a continuación una serie de recomendaciones:

## Para las autoridades e instituciones públicas:

- **Cumplir con las disposiciones en materia de protección de datos personales y privacidad:** la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[35] de México establece la normativa para un tratamiento legítimo, controlado e informado de los datos personales. Sin embargo, existen preocupaciones sobre el cumplimiento de la legislación en contextos migratorios. Desde la obtención del consentimiento libre e informado para procesar los datos personales de las personas en tránsito, hasta la transparencia sobre cómo se toman las decisiones migratorias, todo el tratamiento de datos personales debe observar las disposiciones legales que lo rigen. Llamamos a las autoridades e instituciones públicas a ser rigurosas en el cumplimiento de la ley.

- **Abstenerse de solicitar o exigir información de forma arbitraria y por medios informales:** los albergues narraron que en varias ocasiones alguna autoridad se les ha acercado por medios informales e incluso bajo amenazas, para que entreguen información sobre las personas migrantes que pasan por allí. Dar acceso a estos datos sólo es legítimo a través de una orden judicial, por lo que cualquier otra vía resulta arbitraria. En ese sentido, sería una buena práctica por parte de la Fiscalía General de la República y fiscalías estatales capacitar a los agentes del orden sobre cómo proceder cuando requieren información.

[35] Cámara de Diputados del H. Congreso de la Unión. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Recuperado el 1 noviembre de 2024 de https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

- **Abstenerse de utilizar tecnología de vigilancia masiva con capacidades de recolección remota de datos biométricos:** como se mencionó anteriormente, la vigilancia remota biométrica violenta el principio de presunción de inocencia, el derecho a consentir que se procesen los datos personales -en este caso, datos sensibles-, y genera un efecto inhibitorio entre la población monitoreada. Si la medida responde al objetivo de las autoridades de mejorar la seguridad, la medida resulta desproporcionada, pues se afectan los derechos de muchas personas por la eventualidad de dar seguimiento a un prófugo de la justicia. Sumado a esto, la excesiva vigilancia en las rutas migratorias también puede empujar a las personas migrantes a buscar rutas alternas que resultan más peligrosas, lo que directamente impacta su bienestar y destino migratorio, o incluso puede significar su muerte[36].

- **Respetar la transparencia en los procesos administrativo-legales:** utilizar la figura de notificación roja paraliza los procesos administrativos-legales que posibilitan la regularización de la situación migratoria o la naturalización de una persona. Cuando se utiliza esta medida, pero no se proporciona información a la persona migrante o a las organizaciones que le están brindando acompañamiento sobre la razón detrás de la notificación roja, se impide el derecho a la defensa de la persona afectada, quien puede ser incluso una persona refugiada o solicitante de asilo, ambas categorías que cuentan con protecciones especiales.

- **Investigar posibles filtraciones y abusos por parte de funcionarios:** a partir de sus propias experiencias, así como por las narraciones que escuchan de las personas migrantes, el personal de los albergues refirió preocupación por posibles actos de corrupción y abuso del poder por parte de funcionarios públicos. Desde el acceso ilegítimo a dispositivos móviles, hasta sospechas de colusión entre funcionarios y grupos delincuenciales, existe la posibilidad de que se estén vulnerando los datos personales de las personas migrantes por parte de autoridades e instituciones públicas. Fiscalizar este tipo de actuaciones, y tomar las medidas pertinentes cuando sea necesario, es fundamental para preservar la privacidad de dicha población.

## Para actores humanitarios y financiadores:

- **Abstenerse de solicitar información desagregada:** el contexto de vulnerabilidad que atraviesan muchas personas migrantes complejiza la opción de oponerse al procesamiento de sus datos personales, pues distintas instituciones que brindan acompañamiento -incluyendo actores humanitarios- los solicitan, en ocasiones de manera excesiva. Para una persona migrante, negarse a dicho procesamiento podría significar anular la posibilidad de aliviar alguna necesidad, dado que con frecuencia quienes brindan apoyo lo estipulan como requerimiento para brindar un servicio.

[36] The Verge. (2024). *Surveillance has a body count.* Recuperado el 23 de octubre de 2024 de https://www.theverge.com/2024/3/20/24106098/cbp-migrant-deaths-border-surveillance

De todas maneras, incluso cuando una persona haya otorgado el consentimiento para que sus datos personales recolectados en albergues u otros espacios sean compartidos con terceros, tiene que existir una razón legítima para su procesamiento. El acceso y uso indebido a datos personales que permiten la identificación o incluso el perfilamiento de una persona migrante, además de ser ilegítimo, puede acarrear implicaciones en su proceso migratorio. En ese sentido, el principio de minimización de datos es también pertinente para los actores humanitarios y los financiadores. Para el último caso, solicitar estadísticas en lugar de datos desagregados debe ser suficiente para sus fines.

- **Priorizar las donaciones económicas sobre las donaciones de productos o servicios tecnológicos:** las donaciones de productos y servicios tecnológicos son útiles para suplir algunas de las necesidades de los albergues; sin embargo, tomando en cuenta las variedad de riesgos digitales que conllevan las tecnologías, se recomienda priorizar el apoyo financiero por sobre las donaciones de equipos o servicios, de manera que sean los espacios quienes tengan el control sobre su selección y gestión. Fortalecer el financiamiento por encima de las donaciones en equipamiento también permite a los albergues poder definir dónde ubicar los recursos conforme a sus necesidades.

## Para los albergues:

- **Sistematizar y robustecer el proceso de obtención de consentimiento:** de acuerdo con los testimonios recabados, todos los espacios entrevistados recopilan información personal y demográfica de personas en tránsito en mayor o menor medida. Entre estos procesos de tratamiento de datos personales no existe un estándar. Si bien la situación de urgencia y la carga de trabajo a la que se enfrentan los albergues plantean dificultades que pueden complicar la obtención del consentimiento, se recomienda caminar hacia su estandarización debido a la sensibilidad de la información recopilada y a la necesidad de contar con un proceso que permita a las personas ejercer mayor control sobre sus datos personales. Por otro lado, el establecimiento de procesos claros e informados de obtención de consentimiento es una oportunidad para fomentar la autodeterminación informativa de la población a la que se le da acompañamiento.

- **Minimizar la cantidad de datos recolectados:** los albergues recopilan una diversidad de datos personales cuando una persona se acerca a recibir sus servicios. Con el fin de reducir los riesgos de vulneración de los datos recopilados, es trascendental que los albergues evalúen y establezcan la necesidad de recolectar cada uno de ellos. El principio de minimización de datos establece que solo se deben recopilar datos para un fin específico y necesario, sin acumularlos por la incierta posibilidad de que sean útiles más adelante. Además de limitar su recolección, se debe evaluar y definir por cuánto tiempo es necesario para un albergue conservar dichos datos, de manera que estos se destruyan una vez que no sean requeridos para la prestación de sus servicios al titular de los mismos. De esta manera se puede mitigar el impacto de una eventual extracción de información, al reducir la cantidad de información que potencialmente está disponible y el número de personas potencialmente afectadas.

- **Desarrollar políticas y protocolos institucionales para el almacenamiento y gestión segura de los datos personales:** no todos los albergues cuentan con este tipo de herramientas. En función de fortalecer y estandarizar procesos que garanticen el mayor grado de seguridad posible a los datos personales que se procesan en los albergues, es necesario que dichos espacios desenvuelvan políticas y protocolos internos que establezcan no sólo la plataforma a utilizar, sino quiénes tendrán acceso a esta información y de qué forma.

En ese sentido, constituyen buenas prácticas seudonomizar los datos personales cuando sea posible, limitar la cantidad de personas que cuentan con acceso a la base, implementar contraseñas alfanuméricas sólidas -tanto para el acceso a la plataforma, como para el dispositivo desde el cual se accederá-, garantizar que los dispositivos en los que la información se va a almacenar estén encriptados y garantizar la autenticación de dos pasos, aunque un protocolo debe ser mucho más exhaustivo.

La determinación sobre qué plataforma y mecanismo son los más adecuados para el resguardo de la información debe responder tanto al mapeo de las necesidades de cada albergue, como a la evaluación de los riesgos asociados según el contexto particular y los recursos disponibles. Contar con plataformas y servidores seguros para el procesamiento y almacenamiento de la información es indispensable, pero la seguridad que revierten estos sistemas se ve disminuida si no se acompaña de la implementación de procesos claros sobre cómo usar la herramienta.

- **Definir e implementar una metodología de identificación de riesgos digitales:** la prevención en materia de seguridad digital es siempre menos costosa y más efectiva que reaccionar a los incidentes cuando estos ocurren. Para elaborar una evaluación de riesgos digitales es necesaria la articulación de quienes trabajan directamente con la población atendida, en conjunto con el equipo que brinda apoyo en tecnologías de la información, y de especialistas en materia de seguridad digital. El análisis de riesgos digitales debe identificar qué información y equipos se desea proteger, y determinar cuáles amenazas y cuáles actores representan un mayor riesgo para cada albergue. A partir de los hallazgos, se debe establecer la prioridad de estos riesgos según su gravedad para atenderlos en consecuencia.

- **Desarrollar protocolos de documentación y respuesta a incidentes digitales:** si bien la gran mayoría de los albergues entrevistados afirmó contar con protocolos ante incidentes de seguridad, ninguno de ellos cuenta con protocolos específicos ante incidentes de seguridad digital. La adopción de metodologías para documentar y responder a las amenazas digitales es útil para identificar patrones y posibles perpetradores, facilitar procesos de denuncia y responder de manera sistematizada a los incidentes. El proceso de adopción de seguridad digital debe ser desarrollado a partir de las necesidades y capacidades de cada albergue.

# #MIGRAR SIN VIGILANCIA

Coalición Latinoamericana