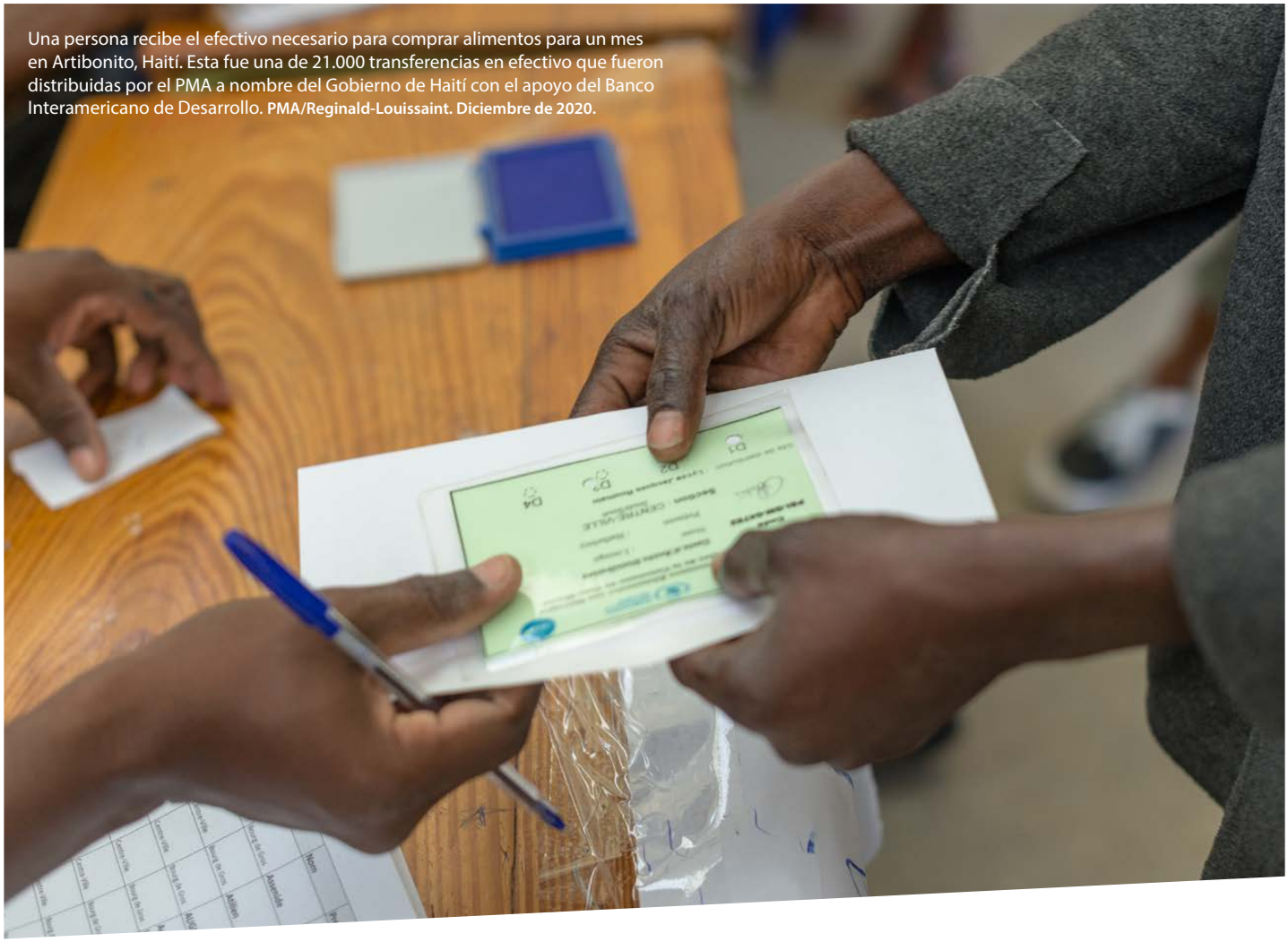
CaLP
The Cash Learning Partnership

## ESTUDIO DE CASO:

# COMPARTIENDO DATOS CON LOS GOBIERNOS DE FORMA RESPONSABLE


PAM/Claire Nevill. Mars 2018.



Una persona recibe el efectivo necesario para comprar alimentos para un mes en Artibonito, Haití. Esta fue una de 21.000 transferencias en efectivo que fueron distribuidas por el PMA a nombre del Gobierno de Haití con el apoyo del Banco Interamericano de Desarrollo. **PMA/Reginald-Louissaint. Diciembre de 2020.**

## AGRADECIMIENTOS

El presente estudio de caso fue liderado por CaLP con fondos del Ministerio Federal de Relaciones de Alemania (GFFO por sus siglas en inglés).

La fase de investigación para elaborar la presente publicación fue desarrollada desde junio a septiembre de 2020.

Linda Raftree (@meowtree), consultora independiente, desarrolló los estudios y elaboró la presente publicación bajo la supervisión y el apoyo editorial y de contenidos de Anna Kondakhchyan (@akondakhchyan). Asimismo, este estudio de caso se benefició de aportaciones de GiveDirectly y otras organizaciones y profesionales vinculados a los Programas de Transferencias Monetarias (PTM), quienes de manera generosa contribuyeron con sus experiencias y testimonios y que, debido a la naturaleza de esta investigación, permanecerán anónimos.

Los puntos de vista que se expresan en la presente publicación son únicamente de las autoras y no representan las opiniones de los donantes ni de las agencias miembro de CaLP.

CaLP es una red mundial de más de 90 organizaciones que se dedican a las políticas públicas, la implementación y la investigación sobre los Programas de Transferencias Monetarias (PTM), los programas de ayuda humanitaria y de asistencia financiera en general.

Para obtener más información, puede visitar el sitio web de CaLP en el enlace www.calpnetwork.org

Siga a CaLP en Twitter: @calpnetwork

Imagen de la portada: El Gobierno de Uganda, ACNUR y el PMA trabajan juntos para verificar de manera biométrica la identidad de todos los refugiados antes de finalizar el año. El PMA ofrece dinero en efectivo y asistencia alimentaria a más de un millón de refugiados afectados por eventos climáticos.

**Los miembros del CaLP trabajan en una gran variedad de contextos, incluidos los territorios que sufren conflictos, crisis de refugiados, personas desplazadas y bloqueos internos o externos. En estas situaciones, los agentes de los Programas de Transferencias Monetarias (PTM) se enfrentan a preguntas complejas respecto al intercambio de datos con diversos interlocutores, por ejemplo, socios de un consorcio, donantes, proveedores de servicios e instancias gubernamentales. Dichas preguntas surgen porque el intercambio de datos entre cualesquiera de los agentes de los PTM puede ser un reto.**

Recientemente han surgido un número creciente de preguntas entre los agentes de los PTM sobre la práctica de compartir datos con instancias gubernamentales en entornos frágiles o que se encuentran en situaciones de conflicto. El énfasis creciente en vincular a los PTM con los sistemas de protección social que desarrollan los gobiernos[1] ha contribuido a aumentar las inquietudes sobre al intercambio de datos. En efecto, la crisis del COVID-19 ha acelerado la necesidad de vincular los PTM y la protección social debido al incremento en el uso de la asistencia en dinero efectivo que se ha producido por las recesiones económicas y por la pérdida de empleo formal e informal que se ha experimentado debido a la pandemia.

Por otra parte, las cuarentenas y los confinamientos también han presionado a los agentes que desarrollan programas humanitarios a incorporar una mayor digitalización en su trabajo. Y si bien los agentes humanitarios reconocen la importancia de colaborar con los sistemas gubernamentales y de fortalecerlos, persisten las inquietudes en relación con los datos de las personas beneficiarias de los PTM, que son sensibles e incluyen información personal. En dichos contextos, podrían ocurrir situaciones indeseadas, por ejemplo, que los gobiernos se coloquen activamente a favor de una de las partes en un conflicto o que las autoridades sean poco amistosas hacia ciertos segmentos de la población, lo que podría poner en riesgo de ser expulsados a los refugiados, por mencionar a un grupo vulnerable.

Tanto los PTM humanitarios como la protección social son actividades que requieren del manejo de grandes cantidades de datos personales y sensibles. Para lograr un vínculo eficaz entre ambos, se requieren acuerdos claros de intercambio y gobernabilidad de datos a lo largo de todo el ciclo de vida de la intervención. En dichos acuerdos, es clave que se priorice la defensa del interés superior de las poblaciones afectadas. Esto se debe a que, fundamentalmente, los contextos donde se llevan a cabo las operaciones son variados y con frecuencia requieren que los agentes de los PTM utilicen estrategias creativas para abordar los múltiples retos a la hora de tomar decisiones que garanticen un mayor beneficio y un menor daño para las personas afectadas por una crisis.

El presente documento describe estrategias a implementar por agentes de PTM para mitigar daños reales y potenciales a poblaciones afectadas por una crisis, que se podrían provocar por haber compartido datos con los gobiernos. Para elaborar este documento se entrevistó a un promedio de 35 personas que trabajan en las distintas organizaciones miembros de CaLP en varios países. Debido a que se trata de un tema sensible, las entrevistas son anónimas y los nombres de ciertas organizaciones y países se han modificado.

## ¿CUÁLES SON LOS RIESGOS DE INTERCAMBIAR DATOS CON LOS GOBIERNOS?

El intercambio de datos de las personas beneficiarias de programas humanitarios puede ser de gran utilidad para la planificación y la preparación de presupuestos de los programas, pues evita la duplicación de personas y pone de manifiesto los vínculos entre las personas beneficiarias de los PTM y de los programas de protección social, entre otros aspectos. Esto podría conducir a que los programas logren un impacto más eficiente en las vidas de las personas. Sin embargo, los datos sobre religión, afiliación política, pertenencia a un grupo étnico, entre otros, también pueden utilizarse para perjudicar a determinadas personas o grupos.

Con frecuencia, las organizaciones recopilan datos sensibles sobre personas altamente vulnerables, incluyendo, el número de identificación nacional, datos biométricos, número de teléfono, dirección, nombres de los hijos, nombres de los padres, cuenta bancaria, ciudadanía y residencia y su condición, datos sobre la salud (por ejemplo, en la respuesta a la crisis del COVID-19), entre otros. También se cuenta con datos sobre la identidad y el comportamiento de grupos, como por ejemplo, dónde viven los refugiados, las ubicaciones donde se entrega dinero o se distribuyen cupones, las rutas migratorias y otros datos que podrían deducirse del análisis de patrones en bases de datos anonimizadas con registros de grandes poblaciones.

> Compartir datos con los gobiernos es una cuestión muy sensible en la agenda humanitaria. No solo existe una alta probabilidad de que se realice una gestión inadecuada, sino que además el impacto de dicha mala gestión constituye un riesgo alto, extremadamente alto'.

1 Smith, G. (2020) 'Supporting the Linkages between Humanitarian Cash and Voucher Assistance and National Social Protection Systems.' (Respaldo a los vínculos entre los Programas de Transferencia Monetaria y los sistemas de protección social nacionales). The Cash Learning Partnership.

En 2020 un documento de la Oficina de Protección de los Datos del Comité Internacional de la Cruz Roja (ICRC, por sus siglas en inglés) identificó los riesgos más importantes relacionados con la participación de organizaciones humanitarias en los programas de protección social, a saber:

- bajos estándares e infraestructura deficiente para la protección de datos en algunos gobiernos;
- limitada habilidad de las organizaciones humanitarias para monitorear el intercambio y procesamiento progresivo de datos, esto incluye el intercambio posterior con otras entidades y el uso de los datos para fines distintos a la protección social;
- la combinación de datos de protección social con otras bases de datos con el fin de revelar información sensible;
- posibles cambios a futuro en la sensibilidad y tecnología de los datos.[2]

Las personas entrevistadas para el presente documento citaron ejemplos de posibles riesgos provenientes del intercambio de los datos con gobiernos, como por ejemplo, que los datos de las personas beneficiarias de los PTM se utilicen para fines de rastreo, deportación o detención. Además, se mencionó que los datos podrían utilizarse para identificar a poblaciones a favor de un bando específico en un conflicto o que los datos sean compartidos con gobiernos de otros países que tienen interés en rastrear a refugiados y quienes podrían provocar algún daño a las familias de dichos refugiados.

Los entrevistados también observaron que compartir datos con gobiernos puede debilitar la confianza entre la agencia y sus socios, si estos socios tienen inquietudes sobre cómo los gobiernos utilizarán los datos. Una persona señaló que, incluso en los casos en que el intercambio de datos sea legítimo, las autoridades rotan, por lo que hay que compartir datos únicamente cuando exista una justificación clara y cuando se hayan puesto en marcha los mecanismos de protección y minimización de datos para proteger a las personas y a los grupos. También se deben prever mecanismos de rendición de cuentas, para casos de incumplimiento de los acuerdos.

> Las autoridades del gobierno actual cambiarán en el futuro. Es necesario partir de la presunción de que los datos serán usados para causar daño'.

En algunos casos, las personas beneficiarias de los PTM son conscientes de que sus datos pueden ponerlos en riesgo, pero la mayoría de las personas beneficiarias no tienen un entendimiento claro sobre los riesgos del intercambio de datos y los problemas en torno a la coerción que pueden llegar a existir. Por ejemplo, en Irak, en los últimos años los segmentos más vulnerables de los programas humanitarios han hecho una transición a los programas de protección social gubernamentales. The Cash Consortium for Iraq (CCI, por sus siglas en inglés)[3] mantuvo conversaciones con las poblaciones afectadas sobre el uso de sus datos y la posibilidad de que los programas humanitarios los refieran a otros programas de asistencia gubernamental. El CCI incluyó una pregunta sobre la 'disposición a ser referido' en sus encuestas de retroalimentación con las poblaciones afectadas. La disposición general era mucho más alta que lo esperado; no obstante, hubo variaciones entre diversas zonas geográficas. El CCI tiene planes de realizar investigaciones adicionales con las poblaciones destinatarias para comprender mejor su entendimiento de los riesgos y su posición sobre el intercambio de datos.

## ¿POR QUÉ A LAS AGENCIAS IMPLEMENTADORAS SE LES PUEDE REQUERIR COMPARTIR DATOS CON LOS GOBIERNOS?

Existe una serie de razones por las que los gobiernos podrían solicitar acceso a datos no personales sobre los programas que están implementando las organizaciones humanitarias, por ejemplo, la ubicación geográfica de los programas o información sobre los socios locales. Las instancias gubernamentales también podrían solicitar datos de carácter personal sobre las personas beneficiarias de PTM por varias razones:

- Algunas de las solicitudes de datos pueden considerarse legítimas, y contar con objetivos alineados con los mandatos y marcos legales de las organizaciones humanitarias. En estos casos, a las organizaciones les parecerá razonable compartir datos a niveles específicos de agregación en condiciones idóneas y dentro de un marco de acuerdos claros.[4]

2 Xu, R., Quijano Carrasco, C., Capotosto, J. (2020) 'Data protection risks of humanitarian engagement in social protection' (Riesgos en la protección de datos durante la participación de organizaciones humanitarias en aspectos de protección social). Oficina de Protección de datos del ICRC.
3 El CCI es una asociación entre el Danish Refugee Council, el International Rescue Committee, el Norwegian Refugee Council, Oxfam y Mercy Corps como organismo principal.
4 Por ejemplo, el GSMA ha publicado un conjunto de lineamientos guía para el intercambio de datos durante la pandemia de la COVID-19 para operadores de redes móviles.

- En casos donde la motivación sea menos clara, las solicitudes de datos pueden categorizarse como semi- legítimas o confusas y requieren más información y diálogo antes de tomar una decisión.
- Algunas solicitudes podrían considerarse ilegítimas. En estos casos, las agencias evitarán intercambiar datos que podrían ser usados para perjudicar a personas o a grupos vulnerables o para objetivos no alineados con los principios humanitarios ni con los mecanismos de buena gobernanza.

A continuación, se incluyen ejemplos de las tres categorías mencionadas:

**Razones legítimas de una solicitud de intercambio de datos:**

- Cuando se incluyen poblaciones que cumplen con los requisitos del registro social de un gobierno;
- Cuando es necesario evitar la duplicación de beneficios entre programas/agencias/organizaciones;
- Cuando se asume la responsabilidad sobre una población que antes recibía servicios de organizaciones humanitarias o como parte de una estrategia de delegación o de salida;
- Cuando se cumplen las recomendaciones de "Conoce a tu cliente" (KYC, por sus siglas en inglés) y del Grupo de Acción Financiera (GAFI);[5]
- Cuando se sospecha que las organizaciones humanitarias u otras agencias son corruptas y los gobiernos quieren realizar una auditoría.

### CASO 1: INTERCAMBIO DE DATOS PARA VINCULAR LOS PTM CON LOS PROGRAMAS DE PROTECCIÓN SOCIAL

Es posible que un gobierno esté creando una lista de personas beneficiarias para los programas de protección social. Su objetivo será identificar a personas que necesitan protección social y recibirán asistencia de manera consistente (personas con discapacidad, personas mayores, entre otras). Sin embargo, si surge una emergencia, el gobierno debe poder identificar a las personas que no están recibiendo protección social por motivos preexistentes. Así, tendrán que efectuar una referencia cruzada de sus listas con aquellas que tienen las agencias humanitarias.

El escenario del Caso 1 es un ejemplo de intercambio de datos legítimo entre organizaciones humanitarias y el gobierno para vincular a los PTM con la protección social. Cuando los gobiernos están desarrollando sus programas de protección social y no existe un censo confiable u otros datos administrativos, podrían solicitar a las agencias humanitarias acceso a datos para completar información faltante. A pesar de que en la actualidad los agentes humanitarios aceptan compartir datos con mayor frecuencia, existen distintos niveles de disposición entre los agentes respecto a ciertos tipos de datos, como por ejemplo, nombres, número de identificación nacional, números de teléfono y otros datos demográficos sensibles. Esto podría dificultar una toma de decisiones unificada al respecto de compartir datos incluso para fines legítimos dentro de los Grupos de Trabajo de Transferencias Monetarias o en el marco de otros consorcios.

> "Si trabajas en una oficina central tendrás menos inquietudes respecto al intercambio de datos, pero en las comunidades donde estén realizando una acción humanitaria, los problemas serán mucho más inmediatos y preocupantes'.

5 Financial Action Task Force (2020) 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations' (Normas internacionales para combatir el lavado de dinero y la financiación del terrorismo y su proliferación: recomendaciones del FATF).

Algunas **razones semi- legítimas o 'confusas'** para intercambiar datos con los gobiernos incluyen:

- Cuando la motivación detrás de una solicitud de intercambio de datos no es clara y se requiere más información para determinar si es justificable;
- Cuando el intercambio de datos encubre una sospecha de que la motivación real es un beneficio político (ya sea que el intercambio lo ofrezca una organización, una agencia, un tercero, o lo solicite el gobierno);
- Cuando la falta de claridad en las actividades de los PTM y sus procesos conduce a inquietudes legítimas por parte del gobierno, sin embargo, estas inquietudes vienen acompañadas de solicitudes ilegítimas de datos de personas beneficiarias de los PTM.

### CASO 2: INQUIETUDES DE LOS GOBIERNOS RESPECTO A LAS ACTIVIDADES DE LOS PTM

En marzo de 2019, la Economic and Financial Crime Commission (EFCC, por sus siglas en inglés) de Nigeria arrestó y detuvo al personal de Mercy Corps por entregar dinero efectivo en una zona rural. La EFCC insistió en acceder a la lista de población beneficiaria y otros documentos antes de poner en libertad al personal. Mercy Corps no ofreció acceso a la lista de personas beneficiarias, pues le preocupaba el modo en que la EFCC podría manejar los datos y la posibilidad de que estos pudieran ser compartidos con otras agencias de seguridad. Además, Mercy Corps consideró que ofrecer acceso a estos datos era una violación al principio humanitario de la independencia, pues comprometía su habilidad de trabajar de una manera autónoma. También se verían comprometidos los principios y las normas sobre el uso seguro de datos personales en programas de transferencia de efectivo y transferencias electrónicas.

Mercy Corps llevó a cabo negociaciones con la EFCC para liberar al personal detenido. Se creó una posición para el Equipo Nacional Humanitario que serviría de guía en las negociaciones y la defensoría con el gobierno federal y los ministerios pertinentes para mejorar el entorno de operación de los PTM. El personal detenido fue puesto en libertad y el dinero confiscado fue devuelto. El Grupo de Trabajo de Transferencias Monetarias (GTM) escribió una versión resumida y accesible de la Ley Contra el Blanqueo de Dinero, la cual había sido invocada por la EFCC cuando frenó la distribución de efectivo. Esto ayudó al Equipo Nacional Humanitario y a los donantes a comprender mejor la Ley Contra el Blanqueo de Dinero y la Ley Contra el Financiamiento del Terrorismo. El GTM brindó capacitaciones en temas de regulaciones financieras y continuó reuniéndose con la EFCC, además sostuvo una sesión para presentar a los PTM y a sus socios.

El GTM y la EFCC acordaron lineamientos y formas de realizar el movimiento de dinero en efectivo para los socios del programa y otros actores vinculados. El GTM le proporcionó a la EFCC un resumen de las distintas leyes en Nigeria sobre la protección de datos y utilizó ese resumen para aclarar qué datos podían compartir y cuáles no. También creó una nota conceptual para desarrollar una Política Nacional de PTM, dirigida a fortalecer el entorno operativo de los PTM en Nigeria, así como los Términos de Referencia para el equipo de trabajo que guiará el desarrollo de dicha política.[6]

En el Caso 2, las motivaciones de la agencia anticorrupción (la EFCC) no eran totalmente claras y había razones para que surgieran inquietudes respecto al intercambio de datos personales y sensibles con agencias gubernamentales. El Grupo de Trabajo de Transferencias Monetarias realizó una serie de reuniones y trabajó con el gobierno federal para lograr un mayor entendimiento sobre la protección que se haría de los datos y si seguiría los lineamientos de la ley y de los principios humanitarios. Esto permitió una mayor participación de la EFCC en el proceso y evitó que se intercambiaran ciertos datos de los beneficiarios que hubieran puesto en riesgo a los beneficiarios de los PTM.

Algunas **razones ilegítimas para intercambiar datos** incluyen el intercambio fuera de los marcos legales y el intercambio de datos que es legítimo,[7] pero poco ético, por ejemplo:

- Cuando una autoridad de gobierno solicita listas de personas beneficiarias para poder integrar personas no cualificadas a sus registros;
- Cuando una autoridad de gobierno exige que se intercambien datos de personas beneficiarias u otros datos como condición para que los PTM se pongan en marcha;
- Cuando una organización o agencia obtiene poder e influencia al intercambiar datos de personas beneficiarias de PTM con instancias gubernamentales sin el consentimiento de las personas beneficiarias o cuando otras organizaciones o agencias ya negaron el acceso a dichos datos;

6 Grupos de Trabajo de Transferencias Monetarias, Nigeria (2020). 'Documento de posición presentado al Equipo Nacional Humanitario'.
7 Si bien los marcos legales ayudan a responder a la pregunta '¿podemos hacer esto?', los marcos éticos ayudan a responder la pregunta '¿deberíamos hacer esto?'

- Cuando se solicitan datos de personas beneficiarias con el propósito de filtrar y excluir a personas o grupos de recibir ayuda humanitaria (como los PTM);
- Cuando el intercambio de datos podría resultar en la identificación o el daño a un grupo específico (desplazados, refugiados, grupos étnicos, grupos políticos) o cuando se sospecha que los datos se transferirán a otros actores quienes podrían utilizarlos para perjudicar a un grupo determinado;
- Cuando el intercambio de datos no es transparente o no está alineado con el propósito para el que fueron recopilados;
- Cuando las solicitudes de intercambio de datos se utilizan para obtener un beneficio financiero, ventaja política o como medio para ejercer poder y control.

Las solicitudes oficiales de intercambio de datos suelen presentarse a través de medios formales. No obstante, en situaciones de conflicto, las solicitudes podrían provenir desde distintos niveles del gobierno y estos podrían plantear retos adicionales para los agentes de los PTM. Aunque algunas solicitudes ilegítimas podrían presentarse a través de canales oficiales, otras podrían entrar en la categoría de solicitudes forzadas o coercitivas y, por ello, requieren estrategias de abordaje diferentes.

> “Estos son temas sensibles que no se están abordando.
>
> En algunos lugares, si haces presión no puedes trabajar en esa localidad. A veces son las autoridades locales —a nivel de distrito— quienes intentan que las organizaciones ignoren sus propias reglas. En este caso se requiere negociación y diplomacia. Nosotros colocamos a los beneficiarios en el centro de toda conversación que iniciamos.
>
> En general, las personas son reacias al intercambio. Los gobiernos y otros grupos están luchando y nosotros no sabemos qué hacer respecto al intercambio de información. Si la situación se torna crítica y se vuelve una amenaza vital, tenemos que entregar los datos o puede ocurrir que se nos prohíba acceder a la zona’.

En todas las acciones humanitarias es común compartir datos por razones ilegítimas. En algunos casos, es ‘el coste de hacer negocios’. Sin embargo, el intercambio de datos puede tener consecuencias graves para las personas beneficiarias de los PTM. Algunos profesionales en el terreno que fueron entrevistados para el presente documento expresaron inquietudes sobre qué posibilidades reales existen para responder negativamente ante una solicitud de datos. El punto más inquietante es cuan bien preparada está la organización para negarse a compartir datos en contextos donde entran en juego los desequilibrios de poder.

El intercambio de datos ilegítimo, forzado y coercitivo son incidentes críticos.[8] La definición de filtración de información personal es ‘una falla de seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada, y acceso accidental o ilegal a datos personales’.[9] Cuando el intercambio de datos es forzado o coercitivo, o las listas de beneficiarios son alteradas o divulgadas a la fuerza, se trata de un incidente crítico o una falla de seguridad crítica de datos y deberá ser tratada como tal. (Se realizará una próxima publicación del CaLP: **proposal for community critical data incident management** -Propuesta para la gestión de incidentes críticos con datos de carácter comunitarios).

8 Véase la labor de la OCHA sobre Critical Data Incidents (Incidentes con datos críticos).
9 Reglamento general de protección de datos de la Unión Europea (2018).

## ¿UN CAMINO CUESTA ARRIBA?

El intercambio de datos con un gobierno puede ser una tarea tensa y desafiante, con pocas soluciones preconcebidas o buenas prácticas estudiadas. El personal de primera línea y los encuestadores, al negarse a compartir datos, podrían poner en juego sus vidas o tener restricciones para acceder a zonas específicas en un país.

> No compartir datos con el gobierno puede ser complicado. Si se planea trabajar en un país específico, hay un límite en los aspectos en los que uno se puede oponer'.

Según algunos profesionales de los PTM, cumplir con altos estándares puede ser frustrante porque, aunque ellos se nieguen a compartir los datos de las personas beneficiarias, otras entidades quizás ofrezcan menos resistencia.

> …las agencias intercambian datos con los gobiernos por diferentes razones sin que haya un consenso o comportamiento común. Yo hacía presión para no compartir datos pero los funcionarios gubernamentales regresaban a decirme que habían conseguido la lista de distribución de uno de nuestros donantes, burlándose de mí'.

En algunas ocasiones, el desequilibrio en las dinámicas de poder dificulta la operación de los PTM.

> Una autoridad de gobierno ha intimidado a la ONG que maneja un campamento bajo su jurisdicción territorial amenazando con enviar una solicitud de datos sensibles vía correo electrónico a otras ONG que trabajan en el mismo campamento. Si no recuerdo mal, una o dos agencias han detenido sus programas debido a esta exigencia. Entonces, hablé con otras agencias, incluido un programa de la ONU, y ellos mismos han sido intimidados por esta autoridad, que tiene mucho poder'.

En algunos casos, los acuerdos de intercambio de datos entre agencias humanitarias e instancias gubernamentales dejan una brecha en la protección de los datos. Algunas organizaciones realizan evaluaciones de necesidades en conjunto con los gobiernos, quienes aprueban y certifican las listas de las personas beneficiarias. Los entrevistados para este documento plantearon inquietudes sobre la limitada capacidad que tienen las organizaciones humanitarias de supervisar con posterioridad el procesamiento y difusión que se hace de los datos por parte de los gobiernos, resaltando los riesgos en la protección de los datos que esto puede significar. El mismo punto fue señalado como un riesgo importante en un reciente estudio de la Federación Internacional de la Cruz Roja y la Media Luna Roja (IFRC, por sus siglas en inglés).[10]

> Se vuelve un juego entre las ONG y los gobiernos en términos de darse por vencido o de influir en las listas de beneficiarios… Afortunadamente, la biometría y otros tipos de mecanismos de rendición de cuentas podrían dificultar la alteración de las listas de beneficiarios… En los contextos frágiles, es importante tener las habilidades para negociar el uso de este tipo de mecanismos.

10 Xu, Quijano Carrasco, y Capotosto, J. 'Data protection risks' (Riesgos en la protección de los datos).

## ESTRATEGIAS PARA GESTIONAR LAS SOLICITUDES DE INTERCAMBIO DE DATOS PROVENIENTES DEL GOBIERNO

**Priorizar el interés superior de las personas beneficiarias de los PTM**

En la medida de lo posible, las agencias deben establecer marcos que definan claramente las condiciones en que los gobiernos pueden solicitar datos y que, además, diseñen un sistema de equilibrio de poderes incluyendo la posibilidad de negarse a aceptar una solicitud, si es inapropiada o contraria a los intereses del beneficiario. A falta de estos marcos, las agencias implementadoras de los PTM tienen que determinar si están dispuestas a compartir datos, según el papel que desempeñan y los acuerdos para actuar en un país y recopilar datos como parte de los procedimientos de sus PTM.

Las organizaciones tienen que priorizar el 'interés superior de la población afectada' y realizar una evaluación para valorar los riesgos que podría causar el hecho de compartir datos de poblaciones afectadas versus los riesgos de negarse a entregarlos. La posibilidad de compartir datos debe ser incorporada a los procesos y formularios de consentimiento, pues los destinatarios de los PTM deben saber que existe la posibilidad de que sus datos sean intercambiados con gobiernos y entender los riesgos potenciales asociados.

Es necesario saber negociar y desarrollar 'aptitudes interpersonales' para dialogar con los diversos niveles de gobierno para consensuar el modo en que los datos se mantendrán seguros y se resguardará a la población afectada. En casos más extremos es necesario valorar los beneficios contra los daños que podría provocar cerrar un programa que proporciona transferencias monetarias. En la fase de planificación de los PTM, mientras se realiza el análisis del contexto, es importante evaluar la "economía política de los datos" —quién podría querer los datos y por qué, qué valor tiene esta información y para quién es valiosa— e incorporar los resultados de dicho análisis en la evaluación de riesgos y la planificación del programa.

**Conocer los principios de su organización**

Las leyes nacionales de protección de datos personales, si existen, posiblemente regulen qué datos pueden intercambiarse y bajo qué circunstancias. Algunas organizaciones cuentan con sus propios principios sobre la protección de los datos personales. Sin embargo, a falta de dichos principios, se pueden utilizar los estándares del sector. Por ejemplo, los Data Responsibility Guidelines (Lineamientos de gestión responsable de datos) de la Oficina de la ONU para la Coordinación de Asuntos Humanitarios (OCHA) estipulan los siguientes puntos: a) procesamiento justo y legítimo; b) especificación del propósito coherente con la misión; c) respeto de los derechos de las personas, su libertad e intereses; d) pertinencia e idoneidad del procesamiento de los datos en relación con el propósito identificado; e) períodos de retención claros y razonables; f) confidencialidad de los datos; g) exactitud de los datos; h) confidencialidad; i) seguridad; j) transparencia ante las personas a las que se refieren los datos, incluyendo por qué se intercambia la información y cómo plantear quejas o retirar datos; y l) transferencia de datos únicamente cuando se asegure una adecuada protección y se cuente con mecanismos de rendición de cuentas que puedan garantizar el cumplimiento de los aspectos anteriores.[11]

**Planificar y simular situaciones para la gestión del intercambio de datos**

Basándose en los principios anteriormente mencionados -los Data Responsibility Guidelines de la OCHA-, las agencias humanitarias deben preparar políticas y procedimientos de gobernabilidad, que ofrezcan lineamientos para manejar las solicitudes de intercambio de datos que reciben de parte de los gobiernos. La publicación de GSMA, el Mobile Policy Handbook (Manual de políticas públicas de comunicaciones móviles),[12] por ejemplo, establece restricciones y un sistema de equilibrio de poderes para gestionar las solicitudes que reciben los operadores de redes móviles (MNO, por sus siglas en inglés) de parte de los gobiernos y que se deben cumplir para evidenciar el cumplimiento de la ley en los países donde operan. Asimismo, las simulaciones en tiempo real pueden permitir ejercitar la toma de decisiones sobre aspectos moralmente delicados. Ensayar o realizar simulacros que guíen al personal a través del proceso de gestión de distintos tipos de situaciones de intercambio de datos -incluyendo trabajar con una matriz de progresividad-, puede mejorar la capacidad del personal para realizar evaluaciones en tiempo real, incluso en medio de una situación de alta tensión. Predefinir pensamientos, respuestas, estrategias y vías de escalada de una decisión, ayudan al personal a entender e implementar los principios más relevantes para cuidar y gestionar responsablemente el intercambio de datos.

**Establecer políticas y acuerdos para el intercambio de datos**

Establecer una política para el intercambio de datos y desarrollar acuerdos escritos puede ayudar a fijar los parámetros sobre los cuáles se pueden compartir datos con los gobiernos y la manera en que se debe realizar. Dichos parámetros pueden servir de línea de base o punto de partida para las solicitudes legítimas y pueden colaborar para definir una posición en una negociación, en caso de demandas semi-legítimas o ilegítimas. Finalmente, es importante insertar cláusulas para el envío de notificaciones en los acuerdos con los Proveedores de Servicios Financieros (PSF) ya que éstos se podrían ver forzados a proporcionar datos a un banco central, con poca claridad de los riesgos y resultados involucrados.

11 OCHA (2019) 'Data Responsibility Guidelines: Working Draft' (Lineamientos sobre la gestión responsable de datos: borrador de trabajo).
12 GSMA (2019) Manuel des politiques de communications mobiles : Guide pour les initiés traitant des grands enjeux (Manual de políticas públicas de comunicaciones móviles: un guía de temas clave).

**Incorporar la minimización, seguridad y privacidad de datos en el diseño de los PTM**

Mientras menos datos se recopilen, menos datos pueden intercambiarse. Si bien la prestación de los PTM requiere datos personales y sensibles, practicar la minimización de datos (recopilar la menor cantidad de datos posible, retenerlos por el menor tiempo necesario, des-identificar los datos tan pronto como sea posible) ayuda a reducir el posible impacto del intercambio de datos, ya sea legítimo, semi- legítimo o ilegítimo. Las medidas de seguridad de datos, como el cifrado, el uso de tokens o el uso de datos disociados, también pueden ayudar a proteger los datos, en especial en casos de solicitudes de intercambio ilegítimas.

**Utilizar tecnologías que preservan la privacidad**

Un diseño que favorezca la preservación de la privacidad en la recopilación de datos minimizará la cantidad de datos que se puedan intercambiar, porque los datos simplemente no estarán accesibles para fines no previstos o no autorizados. Una opción en este sentido, es sacar los datos de las computadoras locales y llevarlos a una nube (asumiendo que esto sea factible, y que los riesgos a los que se enfrentan los datos en la nube sean menores que los riesgos a los que se enfrentan los datos en las computadoras locales). Cifrar los teléfonos y aparatos es otra manera de proteger los datos. Algunas organizaciones exploran el uso de la tecnología de registro distribuido y la tecnología de cadena de bloques para almacenar datos personales de los PTM.[13] Los datos financieros personales en la cadena de bloques están bajo el control de las personas beneficiarias de los PTM, lo cual podría mitigar algunos de los desafíos relacionados con el intercambio de datos; sin embargo, todavía quedan muchos retos por resolver en relación con estas tecnologías emergentes.

**Ofrecer diversas modalidades para registrarse en un PTM**

Cuando existan inquietudes sobre un intercambio de datos con el gobierno que pudiera ser perjudicial, debe informarse de un modo transparente a las personas afectadas como parte del proceso de consentimiento. A pesar de que los PTM se vuelven cada vez más digitales, es posible reducir la cantidad de datos que se solicitan. A las personas beneficiarias de los PTM se debe ofrecer la opción de proporcionar o no sus datos, y en caso negativo, debe haber una opción para inscribirse en los PTM bajo un mecanismo que requiera una recopilación de datos mínima o que permita recibir ayuda sin cumplir con los requisitos de "Conoce a tu cliente" (KYC por sus siglas en inglés). En Libia, por ejemplo, el ICRC negoció un acuerdo con un PSF para utilizar sub-cuentas donde las diligencias debidas y los requisitos del KYC solo aplican al primer titular de la cuenta, y no de quienes acceden a las subcuentas). Así, las personas beneficiarias acceden a su cuenta a través de tarjetas inteligentes (prepagas o de cajeros automáticos) que únicamente tienen vinculados números de referencias y no detalles personales. De este modo, se les permite a las personas beneficiarias asociadas retirar efectivo sin proporcionar sus datos personales al PSF. Solamente el primer titular de la cuenta tiene acceso a la información que vincula la tarjeta o la cuenta con la persona beneficiaria. Otra opción es utilizar a los PSF cuando las personas ya tienen cuentas, lo que significa que ya se ha realizado el proceso de KYC. Si bien estas opciones pueden ser buenas alternativas, hay que tener en cuenta que no todas las agencias pueden ofrecerlas, ya sea debido a su estructura, tamaño, o dependencia de otras agencias para acceder a los fondos.

**Establecer sistemas con acceso limitado**

El diseño de los sistemas puede reducir la cantidad de datos que se comparten con los gobiernos. En Yemen, por ejemplo, se diseñó una base de datos a la que únicamente pueden acceder personas autorizadas según su rol. Los gerentes a nivel de distrito no pueden acceder a datos de nivel global. Los encuestadores únicamente pueden subir datos al sistema, no descargarlos. El sistema está diseñado con activadores y medidas de seguridad, por ejemplo, sellos de tiempo y rastreo de lo que una persona hace y ve dentro del sistema. El Consorcio de Efectivo de Yemen controla el acceso a los diversos niveles de información que está configurada de modo que nadie pueda descargar datos sin aprobación.

**Proteger al personal de primera línea y a los encuestadores**

A veces, el personal de primera línea y los encuestadores se ven enfrentados a una gran cantidad de solicitudes de intercambio de datos ilegítimos. Por ello, es importante lograr su protección, diseñando una recopilación de datos para que se reduzca su acceso directo a datos personales o sensibles. En Iraq, los datos a nivel domiciliario se recogen utilizando una aplicación de recopilación de datos móviles, y tan pronto como un encuestador presiona 'enviar', los datos van a una nube y no es posible guardarlos en el teléfono. Si un teléfono es robado o un encuestador recibe amenazas, no puede proporcionar datos, incluso si se desbloquea el teléfono o si se le obliga a mostrar el contenido del mismo. Cuando el personal de primera línea está bajo presión o debe negociar y disuadir el intercambio de datos ilegítimo con entidades de gobierno locales, es necesario ofrecer capacitación y respaldo. No obstante, se debe señalar que cuando se utilizan servicios en la nube, los datos atraviesan fronteras internacionales, lo cual puede crear otros retos asociados con la transmisión transfronteriza de datos.

En algunos casos, lo más oportuno es que el personal internacional asuma el papel de la negociación, pues podrían ser menos vulnerables a respuestas de represalia que el personal nacional o local. Los riesgos podrían incluir que el personal local deba evitar operar en sus comunidades de interés, porque podrían ser identificados y presionados, intimidados o lastimados para compartir datos con una entidad gubernamental.

13 Portabilidad de datos 'es el principio de que las personas tienen el derecho a obtener, copiar y reutilizar sus propios datos personales y a transferirlos de una plataforma o servicio de TI a otra para sus propios fines'.

**Lograr la colaboración y el trabajo conjunto de los órganos de coordinación humanitaria**

Los órganos de coordinación humanitaria formales e informales, como los Grupos de Trabajo de Transferencias Monetarias (GTM), los equipos de asistencia humanitaria en el país (HCT por sus siglas en inglés) o el grupo de coordinación entre los grupos (ICCG por sus siglas en inglés), pueden desempeñar un papel clave para alinear las posiciones y ofrecer orientación a las organizaciones individuales. Los organismos de coordinación humanitaria pueden por ejemplo:

- Trabajar para despertar la conciencia y el entendimiento de la responsabilidad en la gestión de datos entre sus miembros;
- Conversar sobre situaciones en las cuales los gobiernos podrían solicitar datos y determinar cuáles de estas situaciones son legítimas, semi- legítimas o ilegítimas;
- Consensuar un enfoque coordinado y un mensaje unificado a nivel nacional sobre el intercambio de datos con los gobiernos;
- Ofrecer una 'gobernabilidad blanda' para orientar a los encargados de formular políticas y lineamientos;
- Apoyar a los Equipos Humanitarios Nacionales a asumir una postura y establecer un límite en torno al intercambio de datos con los gobiernos;
- Acordar estándares y mantener la coherencia entre los agentes humanitarios.

**Mantener informadas a las demás organizaciones**

Las organizaciones individuales deberán:

- Informar al órgano de coordinación de la asistencia humanitaria (GTM, ICCG, HCT) si ya intercambian datos con los gobiernos o si tienen planes de hacerlo;
- Informar al órgano de coordinación si se les solicita el intercambio de datos;
- Trabajar dentro de los principios y lineamientos de protección de asistencia humanitaria, por ejemplo, el principio fundamental de 'no causar daño' y el principio de responsabilidad y ética en la gestión de datos (principios que pueden ser propios o de otra organización como por ejemplo el ICRC[14] o la OCHA que han demostrado tener políticas robustas[15]);
- Ser transparentes respecto a las solicitudes de información que reciben de parte del gobierno. Los operadores de redes móviles (MNO por sus siglas en inglés) reportan que, frecuentemente, deben lidiar con varias solicitudes de información de sus clientes por parte del gobierno. Si bien los operadores de redes móviles no tienen otra opción que cumplir con dichas solicitudes, cada vez es más necesario la transparencia sobre la naturaleza y la escala de acceso a información a la que acceden los gobiernos.[16]

## REFLEXIONES FINALES

El rol de los gobiernos que reciben ayuda en la emergencia está aumentando tanto desde la protección social como a nivel de los PTM humanitarios. En un mundo rico en datos, las exigencias de acceso a los mismos que reciben las organizaciones humanitarias se incrementarán en el futuro y los gobiernos anfitriones emplearán enfoques cada vez más sofisticados para obtener acceso a dicha información. La comunidad de los PTM debe aprender conjuntamente y guiarse colaborativamente, 'en tiempo real', a medida que ocurren estas solicitudes, de modo que puedan acordarse enfoques coherentes dentro de los equipos nacionales, los grupos de trabajo de transferencias monetarias y los consorcios internacionales.

**Colocar el interés superior de la población afectada en el centro de las decisiones sobre el intercambio de datos con los gobiernos es de suma importancia y se debe tener presente en todos los casos.**

14 ICRC (2020) 'Data Protection in Humanitarian Action' (Protección de los datos en las acciones de asistencia humanitaria) Segunda edición.
15 OCHA (2019) 'Data Responsibility Guidelines: Working Draft' (Lineamientos sobre la responsabilidad en la gestión de datos: borrador de trabajo).
16 GSMA (2019) 'Mobile Policy Handbook: An Insider's Guide to the Issues' (Manual de políticas móviles: guía de informador sobre los problemas).



www.calpnetwork.org

**Marzo de 2021**