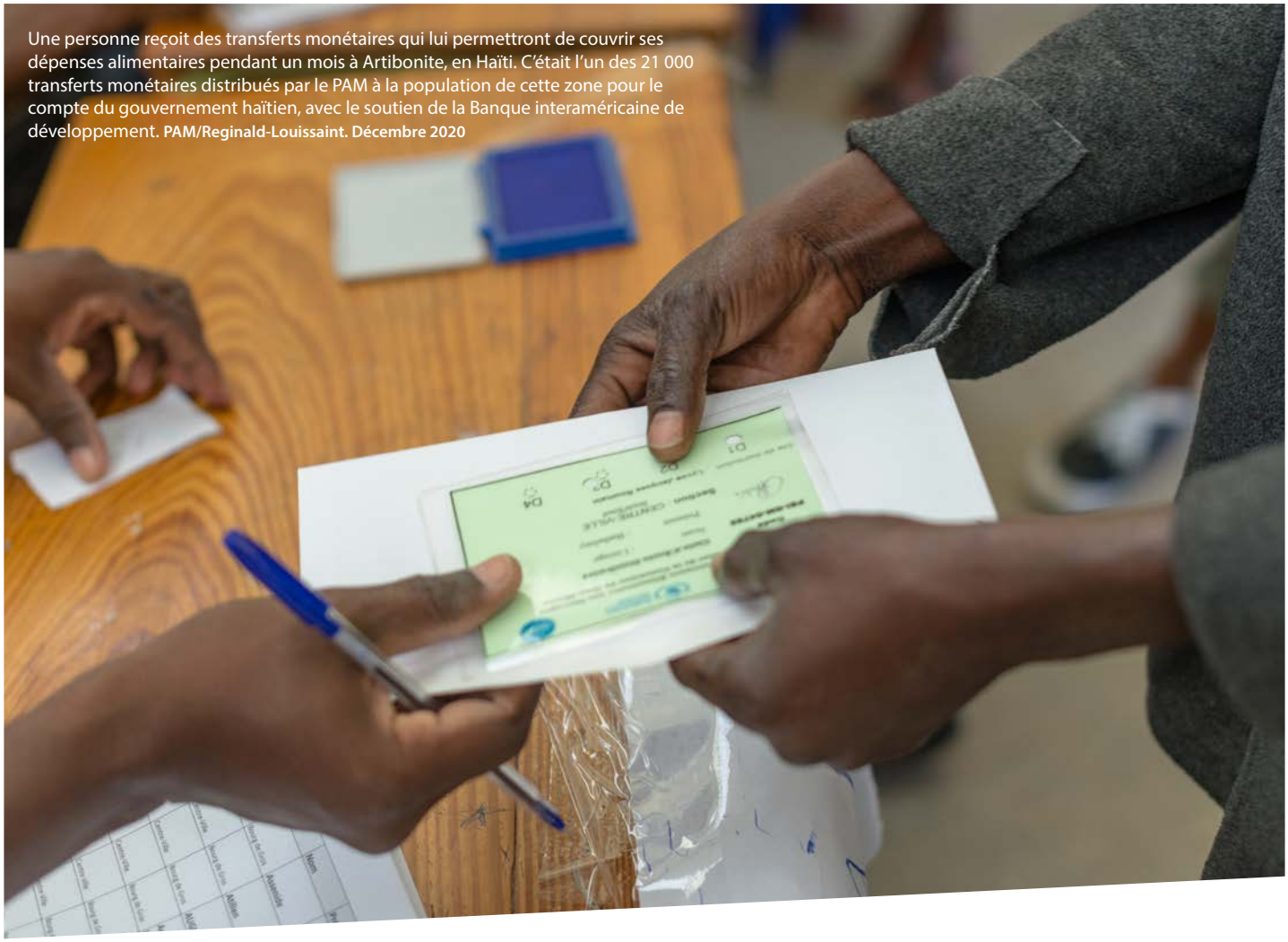
CaLP
The Cash Learning Partnership

ÉTUDE DE CAS :

PARTAGE RESPONSABLE DES DONNÉES AVEC LES GOUVERNEMENTS

PAM/Claire Nevill. Mars 2018.



Une personne reçoit des transferts monétaires qui lui permettront de couvrir ses dépenses alimentaires pendant un mois à Artibonite, en Haïti. C'était l'un des 21 000 transferts monétaires distribués par le PAM à la population de cette zone pour le compte du gouvernement haïtien, avec le soutien de la Banque interaméricaine de développement. **PAM/Reginald-Louissaint. Décembre 2020**

REMERCIEMENTS

Cette étude de cas a été commanditée par le CaLP, avec un financement du Bureau fédéral allemand des Affaires étrangères.

Les recherches utilisées pour cette publication ont été menées entre juin et septembre 2020 par Linda Raftree, consultante indépendante. La publication a été développée par Linda Raftree (@meowtree), avec l'aide et sous la supervision éditoriale et en matière de contenu d'Anna

Kondakhchyan (@akondakhchyan). Cette étude de cas a bénéficié des contributions inestimables d'un grand nombre d'organisations et de professionnel·les du secteur des transferts monétaires, qui ont apporté leur expérience vécue afin d'enrichir le processus de recherche. Leur anonymat a été préservé en raison de la nature sensible de ces recherches.

Les opinions exprimées dans la présente publication n'engagent que leurs auteur·es et ne reflètent pas nécessairement celles des bailleurs ou des organisations membres du CaLP.

Le CaLP est un réseau mondial dynamique de plus de 90 organisations effectuant un travail essentiel sur les politiques, les pratiques et la recherche dans le domaine des transferts monétaires (TM) humanitaires et de l'assistance financière dans son ensemble.

Pour de plus amples informations, consultez le site Web du CaLP à l'adresse www.calpnetwork.org

Suivez le CaLP sur Twitter : @calpnetwork

Image de couverture : Le gouvernement ougandais, le HCR et le PAM travaillent ensemble afin de recenser de manière biométrique l'ensemble des réfugié·es avant la fin de l'année. Le PAM fournit une assistance monétaire et une aide alimentaire à plus d'un million de réfugié·es touché·es par des chocs climatiques à répétition.

Les membres du CaLP interviennent dans les contextes les plus variés, notamment dans des zones de conflits actifs, en situation de crise des réfugié·es, avec des personnes déplacées internes et lors de blocus. Dans de telles situations, les acteurs des transferts monétaires sont souvent confrontés à des questions complexes concernant le partage des données avec des partenaires dans le cadre d'un consortium, avec les bailleurs, avec des prestataires de services tiers et avec les autorités publiques. Le partage de données entre les acteurs des transferts monétaires peut se révéler délicat.

Ces derniers mois, les acteurs des transferts monétaires s'interrogent de plus en plus sur le partage de données avec les autorités publiques dans les contextes fragiles ou les zones de conflits. La tendance croissante à lier les transferts monétaires humanitaires aux systèmes gouvernementaux de protection sociale[1] soulève de plus en plus de questions concernant le partage de données avec les gouvernements. La crise de la COVID-19 vient encore renforcer l'intérêt accordé aux liens entre transferts monétaires et protection sociale en raison du recours accru à l'assistance monétaire face au marasme économique généralisé et aux pertes d'emplois dans l'économie formelle et informelle.

Les quarantaines et les confinements ont également contraint les organisations humanitaires à intégrer dans leur travail des modalités davantage axées sur le numérique.

Tandis qu'un grand nombre d'acteurs humanitaires reconnaissent l'importance de la collaboration avec les gouvernements et du renforcement de leurs systèmes, des préoccupations subsistent concernant le partage de données détaillées sur les bénéficiaires de transferts monétaires avec les gouvernements, en particulier dans les contextes où les autorités sont hostiles à certains pans de la population, comme dans les cas où les réfugié·es pourraient risquer une expulsion ou lorsque les gouvernements prennent activement parti dans un conflit.

Les transferts monétaires humanitaires et la protection sociale sont des activités qui impliquent la manipulation de grandes quantités de données personnelles et sensibles. Pour relier ces deux activités de manière efficace, il est indispensable que des accords clairs en matière de gouvernance et de partage des données existent sur l'ensemble du cycle de vie de l'intervention. Il est essentiel que les organisations défendent les meilleurs intérêts des populations affectées dans leurs prises de décisions sur le partage des données. Toutefois, les contextes d'intervention sont variés et exigent souvent que les acteurs des transferts monétaires recourent à des stratégies créatives pour relever plusieurs défis afin de déterminer quelles décisions apporteront les plus grands avantages et porteront le moins préjudice aux personnes touchées par la crise.

Ce document étudie diverses stratégies que les acteurs des transferts monétaires peuvent mettre en œuvre pour atténuer les préjudices réels et potentiels auxquels le partage de données sur les bénéficiaires de transferts monétaires avec les gouvernements pourrait exposer les populations touchées par la crise. Quelque 35 personnes membres du CaLP dans plusieurs pays ont été interrogées pour l'élaboration de ce document. S'agissant d'un sujet sensible, nous avons assuré leur anonymat. Dans certains cas, nous avons également masqué le nom des organisations et des pays.

QUELS SONT LES RISQUES ASSOCIÉS AU PARTAGE DE DONNÉES AVEC LE GOUVERNEMENT ?

Le fait de partager des données sur les bénéficiaires peut être extrêmement utile pour la planification et la budgétisation des programmes, pour prévenir les doublons, pour renforcer les liens entre les transferts monétaires et la protection sociale, le tout contribuant à accroître l'efficacité et l'impact sur la vie des personnes. Toutefois, l'exploitation de données relatives à la religion, à la sensibilité politique ou à l'origine ethnique ainsi que d'autres données démographiques peut aussi porter préjudice à des personnes ou à des groupes.

Dans de nombreux cas, les organisations recueillent des données personnelles et sensibles sur des personnes très vulnérables, comme le numéro de carte d'identité nationale, des données biométriques, le numéro de téléphone, l'adresse, le nom des enfants et des parents, le numéro de compte bancaire ou d'autres informations financières, le statut de citoyenneté, des données sur l'état de santé (par ex. pendant les réponses à la COVID-19), etc. Elles détiennent également des données sur les identités et les comportements de groupes, comme les endroits où vivent des réfugié·es, les lieux où les transferts monétaires seront distribués, les voies de migration et d'autres informations pouvant être glanées en analysant les modèles à partir de données anonymisées provenant de grandes bases de données sur la population.

> Il s'agit là d'un risque substantiel. En plus d'une forte probabilité de mauvaise gestion, les conséquences peuvent être extrêmement graves. Le risque est très élevé.

1 G. Smith (2020), Soutenir les liens entre les transferts monétaires humanitaires et les systèmes nationaux de protection sociale. Cash Learning Partnership.

Un rapport de 2020 réalisé pour la Commission de protection des données du Comité international de la Croix-Rouge (CICR) identifie les principaux risques liés à l'engagement humanitaire dans les programmes de protection sociale, notamment :

- le faible niveau des infrastructures et des normes de protection des données dans certains États ;
- l'aptitude limitée des organisations humanitaires à surveiller le partage et le traitement ultérieurs des données, notamment le partage avec d'autres organismes et l'utilisation des données à des fins autres que la protection sociale ;
- la combinaison des données de protection sociale avec d'autres ensembles de données pour révéler des informations sensibles ;
- les changements potentiels dans la sensibilité des données et l'évolution de la technologie à l'avenir[2].

Les personnes interrogées pour ce document évoquent des préjudices potentiels découlant du partage de données avec des gouvernements peu enclins à accueillir les réfugié·es, les migrant·es en situation irrégulière et les demandeurs et demandeuses d'asile. Les données sur les bénéficiaires de transferts monétaires pourraient par exemple être utilisées aux fins de suivi, d'expulsion ou de mise en détention. Il est reconnu que les données pourraient également être utilisées pour identifier des populations supposées favorables à l'une des parties à un conflit, ou partagées avec les gouvernements d'autres pays qui ont un intérêt à suivre les réfugié·es et pourraient éventuellement porter préjudice aux familles de ces réfugié·es.

Les personnes interrogées signalent également qu'une relation étroite entre une organisation et une autorité publique peut éroder la confiance entre cette organisation et ses partenaires si ces derniers s'inquiètent de la manière dont les autorités pourraient utiliser les données. Comme le souligne une personne, même dans les cas où le partage de données est légitime, la composition des gouvernements évolue. La plus grande prudence est donc de mise, et les données ne doivent être partagées que dans les situations où cela est clairement justifié et où des mesures de minimisation des données et d'autres mécanismes de protection des données sont en place pour protéger les personnes et les groupes. Des mécanismes de redevabilité clairs sont également nécessaires en cas de violation des accords.

> Le gouvernement de demain ne sera pas le même que le gouvernement d'aujourd'hui. Vous devez partir du principe que les données seront utilisées pour porter préjudice.

Dans certains cas, les destinataires de transferts monétaires ont conscience que des informations les concernant peuvent les exposer à des risques, mais la majorité des bénéficiaires comprennent mal les implications du partage de données et les problèmes de coercition. En Iraq, par exemple, une initiative est en cours depuis plusieurs années pour basculer les dossiers des personnes les plus vulnérables des programmes de transferts monétaires humanitaires vers les programmes gouvernementaux de protection sociale. Le Cash Consortium for Iraq (CCI)[3] a engagé le dialogue avec les populations touchées concernant leurs données et la possibilité que les acteurs humanitaires les orientent vers une aide du gouvernement. Le CCI a inclus une question sur la « disposition à être orienté·e » dans ses enquêtes de feedback menées régulièrement auprès des populations touchées. Celle-ci est globalement supérieure aux prévisions, mais on observe certaines variations selon les zones géographiques. Le Consortium prévoit de mener des recherches supplémentaires auprès des populations cibles afin de mieux comprendre leur conscience des risques et leur attitude vis-à-vis de différents types et niveaux de partage des données.

POURQUOI LES AGENCES DE MISE EN ŒUVRE PEUVENT-ELLES ÊTRE AMENÉES À PARTAGER DES DONNÉES AVEC LES GOUVERNEMENTS ?

Les gouvernements peuvent évoquer différents motifs pour demander à accéder à des données non personnelles sur les programmes mis en œuvre par les organisations humanitaires, comme la zone géographique des programmes ou des informations sur les partenaires locaux. Les autorités publiques peuvent également demander des données personnelles sur les bénéficiaires de transferts monétaires pour différentes raisons.

- Certaines de ces demandes de partage de données peuvent être considérées comme étant *légitimes*, avec des objectifs et des finalités conformes aux mandats humanitaires et aux cadres légaux. Dans de tels cas, les organisations considéreront comme raisonnable le fait de partager des données selon un certain niveau d'agrégation, dans des conditions appropriées et dans le respect des accords conclus[4].
- Lorsque la motivation n'est pas aussi claire, les demandes de partage de données peuvent être classées comme *semi-légitimes* ou floues et nécessiter des précisions et une discussion supplémentaire avant toute prise de décision concernant le partage (ou non) des données.

2 R. Xu, C. Quijano Carrasco, J. Capotosto (2020), Data protection risks of humanitarian engagement in social protection. Commission de protection des données du CICR.
3 Le CCI est un partenariat entre le Conseil danois pour les réfugiés, l'International Rescue Committee, le Conseil norvégien pour les réfugiés, Oxfam et Mercy Corps en tant qu'organisation cheffe de file.
4 La GSMA a publié un ensemble de directives à l'usage des opérateurs de téléphonie mobile pour orienter le partage de données pendant la pandémie de COVID-19, par exemple.

- Enfin, d'autres demandes peuvent être considérées comme *illégitimes*, et les organisations éviteront de partager des données risquant d'être utilisées pour porter préjudice à des personnes et des groupes vulnérables ou touchés par une crise, ou des données qui pourraient être utilisées à des fins non conformes aux principes humanitaires ou aux mécanismes de bonne gouvernance.

La liste ci-dessous fournit des exemples pour les trois catégories de demandes de données :

Motifs légitimes de demandes de partage de données :

- Lorsque des populations éligibles sont incluses dans un registre social géré par un gouvernement
- Pour éviter le chevauchement des prestations entre différents programmes/agences/organisations
- Lors d'un transfert de responsabilité pour une population précédemment prise en charge par des acteurs humanitaires et/ou dans le cadre d'une stratégie de transmission ou de sortie
- Pour se conformer aux exigences en matière de Connaissance de la clientèle (Know your customer) et aux recommandations globales du Groupe d'action financière (GAFI)[5]
- Lorsque des acteurs humanitaires ou d'autres organisations sont suspecté·es de corruption ou de pots-de-vin et que le gouvernement veut réaliser un audit

ENCADRÉ 1 : PARTAGE DE DONNÉES POUR FAIRE LE LIEN ENTRE TRANSFERTS MONÉTAIRES ET PROTECTION SOCIALE

Certains gouvernements peuvent être en train de constituer leur liste de bénéficiaires pour des programmes de protection sociale. Leur objectif est d'identifier les personnes ayant besoin de protection sociale (par exemple, les personnes handicapées ou âgées) qui bénéficieront d'une aide en la matière. En cas d'urgence, le gouvernement doit être en mesure d'identifier dans le registre social les personnes qui ne bénéficient d'aucune protection sociale pour des raisons préexistantes. Il devra pour ce faire croiser ses listes avec les listes détenues par les organisations humanitaires afin que ces dernières puissent fournir des transferts monétaires aux personnes qui ne reçoivent pas encore de prestations du gouvernement.

Le scénario décrit dans l'Encadré 1 est un exemple de partage de données légitime entre les acteurs humanitaires et le gouvernement afin de faire le lien entre transferts monétaires et protection sociale. Lorsqu'ils élaborent leurs programmes de protection sociale et qu'il n'existe aucun recensement ou autre ensemble de données administratives fiable sur lequel s'appuyer, les gouvernements peuvent demander à accéder aux données des organisations humanitaires pour compléter les informations manquantes. Bien qu'un grand nombre d'acteurs humanitaires reconnaissent maintenant le bien-fondé du renforcement des liens entre transferts monétaires humanitaires et protection sociale, les acteurs des transferts monétaires se montrent plus ou moins enclins à partager avec les autorités publiques des données comme les noms, les numéros de carte d'identité nationale, les numéros de téléphone et d'autres données démographiques. Au sein des groupes de travail sur les transferts monétaires et autres consortiums, cela peut rendre difficile toute décision unifiée quant à la question de savoir si l'ensemble des acteurs du secteur des transferts monétaires participant à une intervention particulière partageront des données avec les autorités publiques, même lorsque les finalités sont jugées légitimes.

Si vous travaillez au siège, vous ne serez pas autant préoccupé·e par le partage des données que si vous travaillez au sein d'une communauté dans le cadre d'une intervention humanitaire, où les problèmes sont bien plus concrets et inquiétants.

5 Groupe d'action financière (2012), Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération : Les Recommandations du GAFI.

Parmi les motifs semi-légitimes ou « flous » pour le partage de données avec les gouvernements, on peut citer les cas suivants :

- Le motif de la demande de partage de données n'est pas clair ou des informations supplémentaires sont requises pour déterminer si elle est justifiée.
- La raison avancée pour le partage de données sur les bénéficiaires est suspectée d'être liée à des motivations politiques (que le partage des données soit proposé par une organisation, une agence ou une tierce partie ou qu'il soit demandé par un gouvernement).
- Un manque de clarté concernant les activités de transferts monétaires et les processus associés conduit à des préoccupations légitimes du gouvernement, mais celles-ci s'accompagnent de demandes illégitimes concernant les données sur les bénéficiaires de transferts monétaires.

ENCADRÉ 2 : PRÉOCCUPATIONS DU GOUVERNEMENT CONCERNANT LES ACTIVITÉS DE TRANSFERTS MONÉTAIRES

En mars 2019, la Commission nigériane contre les délits économiques et financiers (EFCC) a interpelé et placé en détention des membres du personnel de Mercy Corp et des prestataires pour avoir effectué des transferts monétaires dans une zone rurale. L'EFCC voulait accéder à la liste des bénéficiaires et à d'autres documents opérationnels avant de relâcher les membres du personnel. Mercy Corps n'a pas partagé la liste des bénéficiaires, s'inquiétant de la manière dont l'EFCC pourrait gérer les données et de la possibilité que celles-ci soient partagées avec d'autres organismes de sécurité. De plus, Mercy Corps considérait que le fait de partager ces données allait à l'encontre du principe humanitaire d'indépendance, car cela compromettait sa capacité à travailler de manière autonome vis-à-vis de l'agence gouvernementale, ainsi que des principes et normes d'utilisation sûre des données personnelles dans les programmes de transferts monétaires et de transferts électroniques.

Des négociations préliminaires se sont tenues avec l'EFCC pour libérer les membres du personnel en détention. Une position a été élaborée pour guider l'équipe humanitaire pays dans les négociations et le plaidoyer de haut niveau auprès du gouvernement fédéral et des ministères concernés afin d'améliorer l'environnement opérationnel pour les transferts monétaires. Les membres du personnel détenus ont été libérés et les sommes confisquées ont été restituées. Le groupe de travail sur les transferts monétaires a rédigé une synthèse de la loi sur le blanchiment d'argent invoquée par l'EFCC lorsqu'elle a interrompu la distribution monétaire. Cela a aidé l'équipe humanitaire pays et les bailleurs à mieux comprendre cette loi, ainsi que la loi contre le financement du terrorisme. Le groupe de travail sur les transferts monétaires a formé des partenaires sur les réglementations financières et a continué à échanger avec l'EFCC. Il a également organisé une session de présentation des transferts monétaires et de leurs principes, ainsi que des partenaires.

Le groupe de travail sur les transferts monétaires et l'EFCC se sont entendus sur des lignes directrices et sur les formes de mouvements monétaires qui exigent la contresignature du partenaire chargé de ces déplacements, ainsi que de plusieurs autres parties prenantes. Le groupe de travail sur les transferts monétaires a fourni à l'EFCC une synthèse des différentes lois en vigueur au Nigeria concernant la protection des données et s'en est servi pour encadrer quelles données pouvaient être partagées et lesquelles ne pouvaient pas l'être. Il a également rédigé une note conceptuelle pour l'élaboration d'une politique nationale en matière de transferts monétaires, visant à renforcer l'environnement opérationnel pour les transferts monétaires au Nigeria, ainsi que des termes de référence à l'usage du groupe de travail qui sera amené à piloter l'élaboration de la politique nationale sur les transferts monétaires[6].

Dans le deuxième exemple présenté dans l'Encadré 2, les motivations de l'agence anti-corruption (EFCC) n'étaient pas tout à fait claires, et il y avait lieu de s'inquiéter du partage de données personnelles et sensibles sur les populations touchées avec les organismes publics. Le groupe de travail sur les transferts monétaires a organisé plusieurs réunions et collaboré avec le gouvernement fédéral pour renforcer la compréhension de la protection des données au regard de la loi et des principes humanitaires. Cela a permis de poursuivre le travail avec une plus grande implication de l'EFCC dans le processus et sans avoir à partager certaines données sur les bénéficiaires de transferts monétaires qui auraient pu compromettre leur sécurité.

Les motifs illégitimes pour le partage de données incluent le partage de données hors de tout cadre légal, ainsi que le partage de données légitime, mais non éthique[7], par exemple :

- Lorsqu'une autorité publique demande des listes de bénéficiaires afin d'ajouter des personnes non éligibles aux registres
- Lorsqu'une autorité publique exige que des données sur les bénéficiaires ou d'autres informations soient partagées pour donner son aval à un programme de transferts monétaires
- Lorsqu'une organisation ou un organisme acquiert un certain pouvoir ou gagne en influence en partageant avec les autorités publiques des informations sur les bénéficiaires de transferts monétaires sans que ces derniers/dernières aient donné leur consentement ou lorsque d'autres organisations ou organismes ont refusé de les partager

6 Groupe de travail sur les transferts monétaires, Nigeria (2020), Exposé de position soumis à l'équipe humanitaire pays.
7 Alors que les cadres légaux aident à répondre à la question « pouvons-nous faire cela ? », les cadres éthiques apportent des éléments de réponse à la question « devrions-nous faire cela ? ».

- Lorsque des données sur les bénéficiaires sont demandées dans le but de sélectionner et d'exclure certaines personnes ou certains groupes éligibles de la liste des destinataires de l'aide humanitaire (comme les transferts monétaires)
- Lorsqu'une demande de partage de données pourrait découler sur le ciblage ou porter activement préjudice à un groupe de personnes en particulier (PDI, réfugié·es, groupe ethnique, groupe politique) ou lorsque l'on suspecte que les données seront transmises à d'autres personnes susceptibles de porter préjudice à un groupe particulier
- Lorsque le partage de données n'est pas transparent ou n'est pas conforme à la finalité initiale de la collecte de données
- Lorsque les demandes de partage de données sont utilisées pour bénéficier d'un avantage financier ou politique ou comme un moyen d'exercer un pouvoir et un contrôle

Les demandes officielles de partage de données peuvent être gérées de manière formelle. Toutefois, en situation de conflit, les demandes de partage de données peuvent émaner de différents échelons du gouvernement et peuvent poser problème aux acteurs des transferts monétaires. Si certaines demandes illégitimes peuvent être formulées par des voies officielles, d'autres s'apparentent clairement à des demandes forcées ou à de la coercition. Cela appelle des stratégies distinctes.

> Ce sont des sujets sensibles qui ne sont pas abordés. Bien qu'il s'agisse de points absolument essentiels, le fait de ne pas s'y plier peut parfois compromettre tout travail dans une zone donnée. Il arrive que ce soient les autorités locales (au niveau du district, et non le gouvernement central) qui cherchent à pousser les organisations à contourner leurs propres règles. Il s'agira là encore de recourir à la négociation et à la diplomatie. Nous plaçons les bénéficiaires au cœur de tout dialogue que nous engageons.
>
> À [...] et [...], les personnes sont vraiment réticentes à partager des informations. Les gouvernements et d'autres groupes s'affrontent, et nous ne savons pas quoi faire concernant le partage et l'accès aux informations. Si la situation dégénère et que des vies sont en jeu, nous n'avons d'autre choix que de fournir les données si nous voulons être autorisé·es à accéder à la zone.

Il est courant que des données soient partagées pour des motifs illégitimes lors des interventions humanitaires. Dans certains cas, l'obligation de partager certaines données avec les autorités publiques est considérée comme le prix à payer pour pouvoir travailler. Cela peut toutefois avoir des conséquences désastreuses pour les destinataires de transferts monétaires. Certain·es praticien·nes de terrain interrogé·es pour ce document se déclarent préoccupé·es par la question de savoir s'il est possible de refuser des demandes de données. Ils et elles s'inquiètent du fait que la direction de l'organisation ne soit pas à même de refuser de partager des données dans les contextes difficiles avec des rapports de force déséquilibrés.

Le partage de données illégitime ou contraint et la coercition constituent des incidents critiques en matière de données[8]. Une violation de données à caractère personnel désigne « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel [...] ou l'accès non autorisé à de telles données »[9]. Lorsque le partage de données est contraint ou forcé, ou lorsque les listes de bénéficiaires sont altérées ou divulguées de force, il s'agit techniquement d'un incident critique en matière de données ou d'une violation, qu'il convient de traiter en conséquence. (Remarque : le CaLP publiera prochainement une **proposition pour la gestion des incidents critiques en matière de données dans les communautés**.)

8 Voir le travail de l'OCHA sur les incidents critiques en matière de données.
9 Union européenne (2018), Règlement général sur la protection des données.

UN COMBAT DIFFICILE ?

Le partage des données avec le gouvernement, tout comme le partage des données de manière générale dans le cadre des programmes de transferts monétaires, est semé d'embûches et de défis, avec très peu de solutions ou de bonnes pratiques prêtes à l'emploi. En refusant de partager des données, le personnel de première ligne et les recenseurs/euses peuvent risquer leur vie ou se voir interdire l'accès à certaines zones d'un pays.

> Il est très délicat de ne pas partager des données avec le gouvernement. Lorsque vous êtes censé·e travailler dans un pays particulier, il y a une limite à ce que vous pouvez refuser.

Pour certain·es praticien·nes des transferts monétaires, le fait de respecter des normes élevées peut être source de frustration car, alors qu'ils et elles refusent peut-être de partager des données sur les bénéficiaires, d'autres entités peuvent opposer moins de résistance.

> … Certaines organisations partagent des données avec les autorités en invoquant différents prétextes, hors de tout accord de partage des données. Il arrive que je refuse de partager certaines données et que des représentant·es du gouvernement reviennent me narguer en brandissant sous mon nez la liste de distribution fournie par un bailleur.

Dans d'autres cas, la dynamique de pouvoir peut rendre difficile la mise en œuvre des programmes.

> Une autorité publique a harcelé l'ONG qui gère le camp relevant de sa compétence jusqu'à ce qu'elle envoie un e-mail de demande de données sensibles au nom de cette autorité publique aux autres ONG travaillant dans le camp. Si je me souviens bien, une ou deux organisations ont suspendu leurs programmes en raison de cette demande. J'ai parlé avec nos homologues au sein d'autres organisations, dont une agence des Nations Unies, qui ont déclaré avoir fait l'objet d'intimidations par cette même autorité très puissante.

Il arrive que les accords de partage des données entre les organisations humanitaires et les autorités publiques entraînent des failles dans la protection des données. Certaines organisations mènent des évaluations des besoins en collaboration avec des gouvernements qui valident et certifient des listes de bénéficiaires. Plusieurs personnes interrogées pour l'élaboration de ce court document ont évoqué la capacité restreinte des organisations humanitaires à suivre le partage et le traitement ultérieurs des données initialement partagées avec les gouvernements. Ce point est également mis en avant dans une récente étude de la Fédération internationale de la Croix-Rouge sur les risques de protection des données liés à l'engagement humanitaire dans la protection sociale[10].

> C'est un petit jeu dans lequel les gouvernements cherchent à faire céder les ONG ou à influencer les listes de bénéficiaires… Du fait des données biométriques et d'autres types de mécanismes de redevabilité, il est plus difficile de modifier les listes de bénéficiaires… Dans les contextes fragiles, les compétences de négociation sont essentielles.

10 R. Xu, C. Quijano Carrasco et J. Capotosto, Data protection risks.

STRATÉGIES DE GESTION DES DEMANDES DE PARTAGE DE DONNÉES ÉMANANT D'AUTORITÉS PUBLIQUES

Priorité aux intérêts des bénéficiaires de transferts monétaires

Dans la mesure du possible, les organisations doivent plaider pour des cadres clairs qui stipulent les conditions dans lesquelles les autorités publiques peuvent demander des données et spécifient tous pouvoirs et contrepouvoirs ou facteurs compensatoires susceptibles de leur permettre de refuser une demande de partage de données si celle-ci est jugée inappropriée ou contraire aux intérêts des bénéficiaires. En l'absence de tels cadres, les organisations de mise en œuvre des transferts monétaires devront déterminer si elles sont disposées à partager des données, en fonction de leur mandat et de leur rôle, ainsi que des dispositions prises pour être présentes dans un pays ou pour collecter des données dans le cadre d'un programme de transferts monétaires.

Les organisations doivent suivre une approche qui privilégie l'intérêt de la population concernée et mener une évaluation afin de pondérer les risques qu'un partage des données pourrait faire courir aux populations concernées par rapport aux risques découlant d'un refus de partager ces données. Cela doit faire partie intégrante des processus d'obtention du consentement, car les destinataires de transferts monétaires doivent savoir s'il est possible que leurs données soient partagées avec les gouvernements et connaître les risques éventuels associés, afin de pouvoir décider de fournir ou non leurs données. Des compétences de négociation et d'autres aptitudes relationnelles seront requises pour interagir avec les différents échelons du gouvernement afin de déterminer comment préserver la sécurité des données et protéger la population concernée de manière plus large, mais aussi pour faire la part entre les avantages de la mise en œuvre et les préjudices découlant de la fermeture d'un programme existant qui fournit déjà des transferts monétaires. Lors des premières phases de la planification de la mise en œuvre des transferts monétaires, au moment de réaliser l'analyse du contexte, il est important d'évaluer l'économie politique des données (Qui peut vouloir accéder aux données et pourquoi ? Quelle valeur les données revêtent-elles pour qui dans ce contexte ?) et d'intégrer ces conclusions dans l'évaluation des risques et la planification.

Connaissance du statut et des principes de votre organisation

Les lois nationales sur la confidentialité des données, si elles existent, régiront probablement quelles données peuvent être partagées, et dans quelles circonstances. Certaines organisations jouissent de certains privilèges et immunités faisant l'objet d'un accord avec le gouvernement d'un pays. De nombreuses organisations ont leurs propres principes en matière de protection des données, qu'il convient alors de respecter. Toutefois, en l'absence de tels principes propres à une organisation, les normes en vigueur dans le secteur peuvent être utilisées. Par exemple, les directives de l'OCHA concernant la gestion responsable des données stipulent notamment les principes suivants : le traitement équitable et légitime des données ; la spécification de finalités conformes au mandat et contrebalancées par des droits, libertés et intérêts pertinents ; la nécessité, la pertinence et l'adéquation du traitement des données par rapport aux finalités identifiées ; des périodes de conservation claires et raisonnables ; l'exactitude des données ; la confidentialité des données ; la sécurité des données ; la transparence vis-à-vis des personnes concernées, y compris concernant la raison pour laquelle les informations sont partagées et comment porter réclamation ou retirer des données ; la limitation des transferts de données aux seuls cas où une protection appropriée est assurée ; et des mécanismes de redevabilité qui peuvent garantir le respect de ce qui précède[11].

Plan de gestion des situations de partage de données et répétitions

D'après le statut et les principes ci-dessus, les organisations doivent mettre en place et observer des politiques et des procédures solides, répétées et soumises à une gouvernance forte afin d'orienter le traitement des demandes de partage de données. De telles mesures peuvent aider l'organisation à déterminer comment aborder les demandes de partage de données avec les gouvernements. Le *Manuel des politiques de communications mobiles* de la GSMA[12], par exemple, fixe plusieurs restrictions, pouvoirs et contrepouvoirs concernant les demandes d'accès des gouvernements, auxquels les opérateurs de téléphonie mobile doivent se conformer lorsque des lois et/ou conditions de licence exigent qu'ils appuient les activités d'application de la loi et de sécurité dans les pays où ils opèrent. Le fait de se prêter à des jeux de rôle sur la mise en œuvre de telles politiques aide le personnel et la direction à parfaire leur aptitude à prendre en temps réel des décisions difficiles sur le plan moral. Les répétitions ou les simulations par lesquelles le personnel se familiarise avec la gestion de différents types de situations de partage de données, y compris l'utilisation d'une matrice d'escalade, peut renforcer la réactivité du personnel et améliorer sa capacité à effectuer des évaluations en temps réel, y compris au plus fort d'une situation très stressante. Le fait d'établir au préalable des réflexions, des limites, des stratégies et des procédures d'escalade aide le personnel à interpréter et à appliquer les principes.

Établissement de politiques et d'accords de partage de données

Le fait d'établir une politique et des accords de partage de données peut éclairer la définition de paramètres pour identifier les données pouvant être partagées avec les gouvernements et les procédures associées. Ces politiques et ces accords peuvent servir de référence ou de point de départ pour les demandes légitimes de partage de données émanant des gouvernements et peuvent faciliter la prise de position lors des négociations en cas de demandes semi-légitimes ou illégitimes. De plus, l'ajout de clauses de notification dans les accords avec les prestataires de services financiers (PSF) peut être utile dans les situations où les PSF sont contraints de fournir des données à une banque centrale.

11 OCHA (2019) 'Data Responsibility Guidelines: Working Draft'.
12 GSMA (2019), Manuel des politiques de communications mobiles : Guide pour les initiés traitant des grands enjeux.

Intégration à dessein de la minimisation des données, de la sécurité des données et de la confidentialité

Moins il y a de données collectées, moins il y en a pouvant être partagées. Bien que certaines données personnelles et sensibles soient requises pour proposer des programmes de transferts monétaires, la minimisation des données (par ex. en recueillant le moins de données possible, en ne les conservant que pour la durée strictement nécessaire et en les anonymisant dès que possible) est l'un des moyens permettant de minimiser l'impact potentiel du partage de données, qu'il soit légitime, semi-légitime ou illégitime. Les mesures de sécurité des données, comme le chiffrement, la tokenisation ou la pseudonymisation, peuvent également contribuer à la protection des données, en particulier en cas de demandes illégitimes de partage des données.

Utilisation de technologies qui préservent la confidentialité

Le fait de concevoir la collecte des données d'une manière qui respecte la vie privée permettra de minimiser la quantité de données pouvant être partagées, car les données ne seront tout simplement pas accessibles pour une utilisation non prévue ou non autorisée. L'une des options consiste à transférer les données des appareils locaux vers le cloud (à condition que cela soit faisable et que les risques pour les données soient moins élevés sur le cloud que sur un appareil local). Le chiffrement des téléphones et des appareils est un autre moyen de protéger les données. Certaines organisations explorent l'utilisation de technologies de registres partagés et de la blockchain pour conserver les données personnelles en lien avec les programmes de transferts monétaires. Les bénéficiaires de transferts monétaires auraient ainsi le contrôle sur leurs données financières personnelles sur la blockchain, permettant la portabilité des données[13]. Cela pourrait atténuer certains des problèmes inhérents au partage de données dans les programmes de transferts monétaires. Il y a toutefois encore de nombreux défis à relever concernant ces technologies émergentes.

Choix possible entre différentes modalités

Si l'on craint que certaines données partagées avec les gouvernements puissent porter préjudice, les personnes concernées doivent être informées de manière exhaustive et transparente dans le cadre du processus d'obtention du consentement. Bien que les processus de transferts monétaires deviennent de plus en plus numériques, il est possible de réduire la quantité de données requises en proposant des alternatives. Les destinataires de transferts monétaires doivent pouvoir choisir de fournir ou non leurs données et, dans le dernier cas, avoir la possibilité de s'inscrire à un programme de transferts monétaires selon un mécanisme qui requiert une collecte minimale de données ou de recevoir une aide qui ne s'accompagne pas d'obligations de connaissance de la clientèle (Know your customer) ni de collecte de données du même type. En Libye, par exemple, le CICR a négocié un accord avec un prestataire de services financiers pour utiliser des sous-comptes. Avec cette formule, la diligence raisonnable et les obligations de connaissance de la clientèle sont uniquement réalisées sur le/la titulaire du compte principal, mais pas sur les personnes qui accèdent aux sous-comptes. L'accès aux sous-comptes s'effectue ensuite par exemple au moyen de cartes à puce (comme des cartes prépayées ou des cartes de retrait) uniquement associées à des numéros de référence, sans aucun détail personnel.

Les bénéficiaires peuvent alors retirer des espèces sans que leurs données personnelles soient fournies au prestataire de services financiers. Seule la personne titulaire du compte principal a accès aux informations permettant de faire le lien entre la carte ou le compte et le/la bénéficiaire. Une autre option consiste à faire appel à des prestataires de services financiers chez lesquels les personnes ont déjà un compte, si bien que les obligations de connaissance de la clientèle sont déjà remplies. Toutefois, certaines organisations ne sont pas en mesure de proposer ces options du fait de leur structure, de leur taille et de leur dépendance vis-à-vis d'autres agences pour les systèmes et le financement.

Établissement de systèmes sûrs avec un accès limité

La conception des systèmes peut contribuer à réduire la quantité de données partagées avec les gouvernements, qu'il s'agisse de demandes légitimes, semi-légitimes ou illégitimes. Au Yémen, par exemple, une base de données a été conçue pour n'être accessible que par les personnes autorisées, en fonction de leur rôle. Les responsables à l'échelle du district ne peuvent pas accéder aux données du niveau global. Les recenseurs/euses peuvent uniquement charger des données sur le système, mais pas les télécharger depuis le système. Le système intègre des déclencheurs et des mesures de sécurité, comme des horodatages et un suivi de ce que font et consultent les personnes sur le système. Les niveaux d'accès sont contrôlés par le Cash Consortium of Yemen. Les informations sont unifiées et la sécurité est définie de telle sorte que personne ne puisse télécharger des données sans approbation préalable.

Protection du personnel de première ligne et des recenseurs/euses

Le personnel de première ligne et les recenseurs/euses sont parfois confrontés à de nombreuses demandes illégitimes de partage de données. Il est important de contribuer à leur sécurité en concevant la collecte des données de manière à réduire l'accès direct aux données personnelles ou sensibles. En Iraq, les données au niveau des ménages sont collectées à l'aide d'une application mobile de collecte de données. Dès que le ou la recenseur/euse appuie sur « Envoyer », les données sont envoyées vers le cloud et rien n'est enregistré sur le téléphone. En cas de vol d'un téléphone ou si un·e recenseur/euse est menacé·e, aucune donnée ne peut être récupérée, même si le téléphone est déverrouillé ou si la personne est contrainte de montrer le contenu du téléphone. Dans les zones où le personnel de première ligne est sous pression ou doit négocier et dissuader le partage illégitime de données avec les entités gouvernementales locales, des formations et un soutien seront

13 La portabilité des données désigne « le principe selon lequel les personnes ont le droit d'obtenir, de copier et de réutiliser leurs propres données personnelles et de les transférer d'une plateforme ou d'un service informatique à l'autre pour leur propre usage ».

nécessaires. (Il convient toutefois de noter qu'en cas d'utilisation de services cloud, les données transitent par-delà les frontières internationales, ce qui peut engendrer d'autres défis en lien avec la transmission transfrontalière de données.) Dans certains cas, il est préférable que les négociations soient confiées au personnel international, car il peut être moins vulnérable aux mesures de rétorsion que le personnel national. Les conditions peuvent être telles que le personnel local ne doit pas intervenir dans les communautés dont il est issu, où il pourrait être identifié et faire l'objet de diverses formes de pressions ou d'intimidations pour partager des données, ou même voir son intégrité physique menacée.

Mobilisation en front uni au sein des organes de coordination humanitaire

Les organes de coordination humanitaire formels et informels comme les groupes de travail sur les transferts monétaires, les équipes humanitaires pays ou le groupe inter-cluster de coordination peuvent contribuer à la convergence des positions et conseiller leurs différent·es membres. Par exemple, ils peuvent :

- sensibiliser les membres et renforcer leur compréhension de la gestion responsable des données ;
- envisager des scénarios dans lesquels les gouvernements peuvent demander des données et déterminer lesquels de ces scénarios sont légitimes, semi-légitimes ou illégitimes ;
- s'entendre sur une approche coordonnée et un message unifié au niveau national concernant le partage de données avec les gouvernements ;
- assurer une « gouvernance souple » en poussant les responsables de l'élaboration des politiques à définir des lignes directrices ;
- aider les équipes humanitaires pays à prendre position et à fixer des limites concernant le partage de données avec les gouvernements ;
- convenir de normes et d'une harmonisation entre l'ensemble des acteurs.

Information des autres organisations

Chaque organisation doit :

- informer l'organe de coordination humanitaire (groupe de travail sur les transferts monétaires, groupe inter-cluster de coordination, équipe humanitaire pays) si elle partage déjà des données avec des gouvernements ou prévoit de le faire ;
- informer l'organe de coordination si elle est sollicitée pour partager des données ;
- travailler dans le respect des principes humanitaires et des lignes directrices en matière de protection, comme le principe fondamental de « ne pas nuire », et suivre les principes de gestion éthique et responsable des données (propres ou empruntés à une autre organisation appliquant des politiques fortes comme le CICR[14] ou l'OCHA[15]) ;
- être transparente concernant les demandes d'informations de la part des gouvernements. Les opérateurs de téléphonie mobile, en particulier, déclarent être régulièrement confrontés à de nombreuses demandes d'informations sur les client·es de la part des gouvernements. Bien que les opérateurs de téléphonie mobile puissent ne pas avoir d'autre choix que d'obtempérer, ils ont de plus en plus besoin d'une transparence accrue quant à la nature et à l'ampleur de l'accès des gouvernements[16].

CONCLUSION

Les gouvernements hôtes jouent un rôle de plus en plus déterminant dans les interventions d'urgence, tant en termes de protection sociale que de transferts monétaires humanitaires. Dans ce monde où les données sont omniprésentes, les demandes de données auprès des organisations humanitaires ne feront que se multiplier à l'avenir, et les gouvernements hôtes recourent à des approches toujours plus sophistiquées pour les obtenir. Les différents membres de la communauté des transferts monétaires doivent apprendre les uns des autres et s'orienter mutuellement, y compris « en temps réel », lorsque ces demandes leur parviennent, de sorte à convenir d'approches cohérentes au sein des équipes pays, des groupes de travail sur les transferts monétaires et des consortiums.

Dans tous les cas, l'essentiel est de placer l'intérêt des populations concernées au cœur de toute décision sur le partage des données avec les gouvernements.

14 CICR (2020) 'Data Protection in Humanitarian Action' deuxième édition.
15 OCHA (2019) 'Data Responsibility Guidelines: Working Draft'.
16 GSMA (2019) Manuel des politiques de communications mobiles : Guide pour les initiés traitant des grands enjeux.

www.calpnetwork.org

Mars 2021