WFP
wfp.org

vam
food security analysis

Réaliser des enquêtes par téléphone portable de manière responsable

Marie Enlund,WFP

Manuel de terrain pour le personnel du PAM

Ce manuel de terrain présente les principaux risques que comporte une collecte de données par téléphone et aide à promouvoir le principe de responsabilité pour la collecte, la conservation et le partage des données dans l'environnement très complexe dans lequel le PAM intervient.

En collaboration avec le Groupe International sur la Responsabilité en matière de Données (International Data Responsibility Group)

Mai 2017

Réaliser des enquêtes par téléphone portable de manière responsable - Manuel de terrain pour le personnel du PAM

Programme alimentaire mondial des Nations Unies (PAM)
Via Cesare Giulio Viola 68/70, Parco de' Medici 00148, Rome - Italie

Service de l'analyse de la securite alimentaire
Directeur: Arif Husain
Tel: + 39 06 6513 2014
e-mail: arif.husain@wfp.org

Remerciements: ont contribué Jos Berens (Université de Leiden), Jean-Martin Bauer, Michela Bonsignore, Perena Sekhri et Angie Lee (PAM).

Table des matières

Introduction et contexte

1

La collecte de données à travers la téléphonie mobile ...

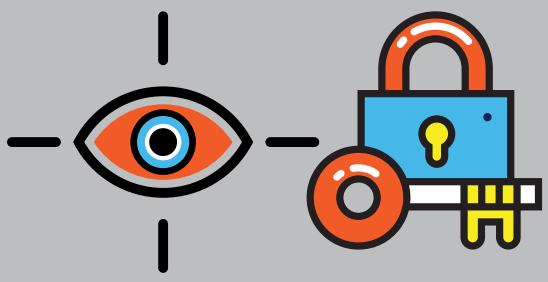
Plus rapide

Moins chère

Plus Sécuritaire

en 2016, mVAM a mené ***250 000 enquêtes*** dans plus de ***30 pays*** et posé presque ***4 millions de questions.***

...ces nouvelles possibilités comportent aussi des risques en matière de confidentialité et de sécurité.



Ce manuel de terrain présente les principaux risques que comporte une collecte de données par téléphone et aide à promouvoir le principe de responsabilité pour la collecte, la conservation et le partage des données dans l'environnement très complexe dans lequel le PAM intervient.

SECTION I Introduction et contexte

La collecte de données à travers la téléphonie mobile est généralement plus rapide et moins chère que les alternatives avec des entretiens en personne. Grâce aux technologies mobiles, le PAM et les autres agences humanitaires sont maintenant capables de collecter une quantité d'informations plus importante que jamais. Le PAM collecte des quantités croissantes d'informations grâce à la téléphone mobile dans le cadre de son projet Analyse et cartographie de la vulnérabilité fondé sur la téléphonie mobile (mVAM)[i] : en 2016, mVAM a mené 250 000 enquêtes dans plus de 30 pays et posé presque 4 millions de questions. La technologie mobile représente une immense opportunité de mieux communiquer avec les personnes dans un contexte humanitaire. Cependant, ces nouvelles possibilités comportent aussi des risques en matière de confidentialité et de sécurité pour les personnes et les communautés dans lesquelles des enquêtes par téléphone sont conduites.

Des 'atteintes à la protection des données' sont souvent signalées dans les médias quand une tierce partie non autorisée a pu accéder à des données, les copier et/ou les détruire. En Décembre 2016, les médias ont révélé les détails de la plus grande violation de données qui ait eu lieu jusqu'à présent: l'atteinte aux données de plus d'un milliard d'utilisateurs de yahoo en 2013[ii]. Une atteinte, seulement d'une fraction de cette taille, serait complètement inacceptable pour une organisation humanitaire dont la mission est de protéger les personnes les plus vulnérables de la planète.

Sans parler de divulgation de données brutes sensibles, il existe d'autres risques associés à la collecte, la conservation, le traitement et la distribution de données digitales sur les personnes vulnérables.

Si les données comportent des défauts et sont biaisées, elles n'apportent pas d'informations correctes pour les opérations. Si les informations sur le lieu de présence des bénéficiaires du PAM sont partagées à un niveau trop bas d'agrégation dans un environnement instable, les bénéficiaires du PAM ou son personnel peuvent être la cible d'acteurs malveillants. L'incertitude concernant les capacités futures et les limites des outils analytiques fait qu'il est de plus en plus difficile d'évaluer initialement la sensibilité des jeux de données.

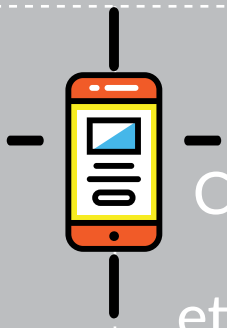
Le PAM a adopté une politique institutionnelle sur la confidentialité et la sécurité des données en 2016. Pour assurer sa mise en œuvre au niveau du terrain, l'organisation a publié ce guide destiné au personnel sur le terrain. Ce manuel de terrain[iii] présente les principaux risques que comporte une collecte de données par téléphone et aide à promouvoir le principe de responsabilité pour la collecte, la conservation et le partage des données dans l'environnement très complexe dans lequel le PAM intervient.

Principes et définitions clefs

2

Principes et définitions clefs

1.



Collecte et traitement des données justes et respectueux de la loi

2.

Information personnelle identifiable (Personally Identifiable Information ou PII) ou donnée personnelle

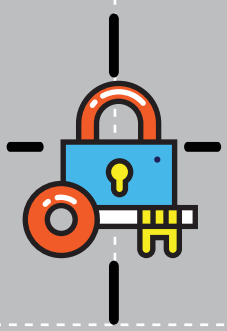
3.

Information démographique identifiable (Demographically Identifiable Information ou DII)

4.

Vulnérabilités spéciales

5.



Contrôleur des données

6.

SECTION 2 Principes et définitions clefs

Responsabilité en matière de données – Le devoir de garantir le respect des droits des personnes en matière de consentement, confidentialité, sécurité et propriété concernant les processus de collecte, d'analyse, de conservation, de présentation et de réutilisation des données, tout en respectant les valeurs de transparence et d'ouverture.[iv]

Collecte et traitement des données justes et respectueux de la loi – C'est le principe général qui gouverne l'ensemble du cycle de traitement des données, de la collecte à leur élimination. Il implique le respect des droits de l'homme et de ne causer aucun préjudice : les personnes ne doivent pas être exposées à une violation de leurs droits, subir des préjudices ou un traitement sans dignité ou discriminatoire, suite à la collecte et au traitement des données personnelles. Dans la mesure où cela s'applique, la collecte et le traitement des données doivent être menés en conformité avec les lois locales qui régissent la protection des données et les régulations en vigueur.

Information personnelle identifiable (Personally Identifiable Information ou PII) ou donnée personnelle – Une donnée personnelle est toute information relative à un individu qui l'identifie (identifiant direct) ou qui peut être utilisée pour l'identifier (identifiant indirect).[v] Un numéro de téléphone seul[vi] peut sembler inoffensif car il ne permet pas d'identifier immédiatement une personne, il peut cependant facilement être utilisé pour trouver des informations personnelles sur quelqu'un.

Information démographique identifiable (Demographically Identifiable Information ou DII) – Il s'agit d'une donnée agrégée qui inclut des informations personnelles et qui fait souvent référence à des sous-groupes de la population. En plus d'informations sur le déplacement d'une personne ou de son statut de réfugié, le PAM conserve des listes de noms de personnes, qui peuvent être utilisées pour identifier l'appartenance religieuse ou ethnique des personnes.

Cela peut permettre d'identifier des lieux de concentration de personnes d'une religion ou d'une ethnie spécifique – quelque chose à prendre sérieusement en compte dans un contexte de conflit.

Les données proxy sur le genre, l'âge et la santé (par ex., le logement et le type de toilettes) sont aussi souvent collectées. Même si elles peuvent ne pas être considérées comme des données personnelles, cela peut tout de même entraîner des risques.[vii]

Vulnérabilités spéciales – Il s'agit des caractéristiques socio-économiques qui peuvent conduire à l'exclusion, à des préjudices et ou des informations biaisées. Par exemple :

- Age: handicaps, infirmité ou normes sociales particulières qui peuvent être liés à l'âge et empêcher la participation à une enquête et/ou la compréhension complète d'une enquête.
- Genre: dynamiques de pouvoir au sein d'un ménage ou d'une communauté, rôles attribués socialement et influence excessive des maris, pères, membres de la famille et leaders communautaires sur les femmes et les jeunes filles qui peuvent conduire à des préjudices, une discrimination ou des réponses auto-censurées et ou des réponses incorrectes. Le même risque existe pour les hommes et les jeunes garçons dans des sociétés matriarcales.
- Autres facteurs de diversité: la capacité linguistique, l'analphabétisme, des incapacités, l'orientation sexuelle, l'affiliation politique, l'appartenance ethnique et les croyances religieuses et culturelles peuvent affecter négativement la libre participation des personnes à une enquête.

Contrôleur des données – Lorsque le PAM met en œuvre des enquêtes, en interne ou à travers une agence ou un prestataire de services externe, le PAM est le contrôleur des données. L'organisation est le gardien principal des données personnelles et détermine les objectifs et la manière dont les données personnelles sont traitées. Le statut du PAM de contrôleur des données implique des obligations qui sont décrites dans ce guide. La position de contrôleur des données est aussi décrite dans le règlement européen sur la protection générale des données (European General Data Protection Regulation ou GDPR) à venir, qui s'il n'est pas applicable à toutes les opérations du PAM, peut fournir des orientations pour résoudre des problèmes particuliers en matière de responsabilité concernant des données.[viii]

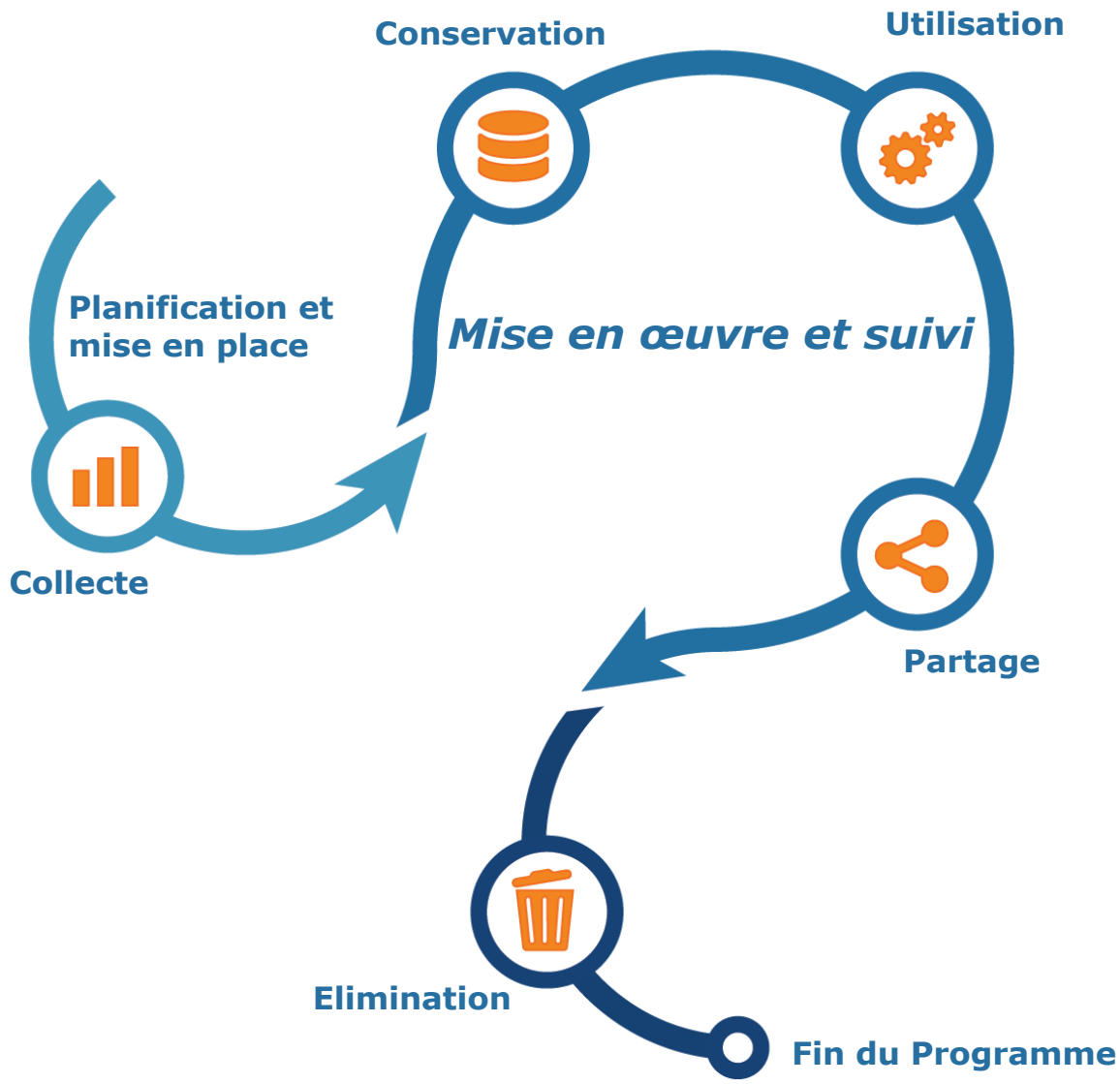
Chaîne de responsabilités en matière de données

3

A chaque étape du cycle de vie des données humanitaires, il existe des risques quant à la sécurité des données qui peuvent porter préjudice aux personnes, communautés et même au PAM et à ses partenaires. Le tableau ci-dessous fait la liste des risques les plus probables et des préjudices qui peuvent se concrétiser avant, pendant et après la collecte des données.

Etape	Risque	Préjudice potentiel
Avant la collecte des données	• La conception de l'enquête est vague et des données PII ou DII non nécessaires sont collectées • La collecte est en porte-à-faux avec les dispositions légales et réglementaires • Le PAM passe un contrat avec un (des) prestataires de services tiers non professionnel(s) service provider(s)	• Conflit avec des individus, communautés ou autorités; perte de confiance et de crédibilité • Poursuites judiciaires • Mauvaise qualité des services par les prestataires tiers, préjudice à la réputation du PAM
Données collectées	• Le consentement n'est pas requis avant la collecte de données • Les listes avec des informations personnelles (noms et numéros) sont divulguées • Excès – trop d'informations sont collectées avec les numéros de téléphone, permettant d'identifier les personnes selon leurs réponses • Les personnes en contexte de conflit peuvent s'exposer elles-mêmes à des risques en répondant à un appel (par ex., interdiction de téléphoner dans certains conflits) • Les appels ou les messages écrits sont suivis et lus/écoutés par les parties en conflit	• Mauvaise compréhension de l'objectif de l'enquête (par ex., les opérateurs du PAM sont perçus comme des espions) • Les personnes sont ciblées pour une fraude téléphonique (par ex., des parties tierces se font passer pour le PAM) • Les personnes pourraient croire qu'elles vont perdre leur aide si elles ne participent pas. • Violence basée sur le genre (par ex., enquêteur masculin appelle une femme mariée ou l'inverse)
Données analysées	• Des concentrations géographiques de groupes minoritaires ethniques, religieux ou autres sont identifiées • Les données sont mal agrégées	• Un acteur militaire analyse et utilise les données pour chercher les personnes ou les communautés à attaquer • Documentation ou catégorisation erronée d'individus ou de communautés entraînant une discrimination ou l'exclusion
Données conservées, partagées ou utilisées	• Les données personnelles ne sont pas conservées dans un lieu en sécurité et protégées par un mot de passe et/ou peuvent être victime de violations ou d'attaques malveillantes • Les enregistrements de données font l'objet d'une fuite en raison d'une négligence ou d'un vol • Les enregistrements de données ne sont pas éliminés à la fin du projet	• Les PII ou DII font l'objet d'une fuite, et sont utilisées contre un groupe ciblé ou exploitées de différentes manières.

La chaîne de responsabilité et sa place dans le cycle du programme peuvent être illustrées comme suit:



Veuillez noter que la chaîne de responsabilités en matière de données a la solidité de son élément le plus faible et est tributaire de la capacité de l'organisation à gérer les cas de risques tout au long du cycle de vie dans le cadre des plans de préparation concernant les données.[ix] Des actions appropriées peuvent atténuer de nombreux risques parmi ceux identifiés ci-dessus et les sections suivantes contiennent un guide par étape sur la mise en place de protections.

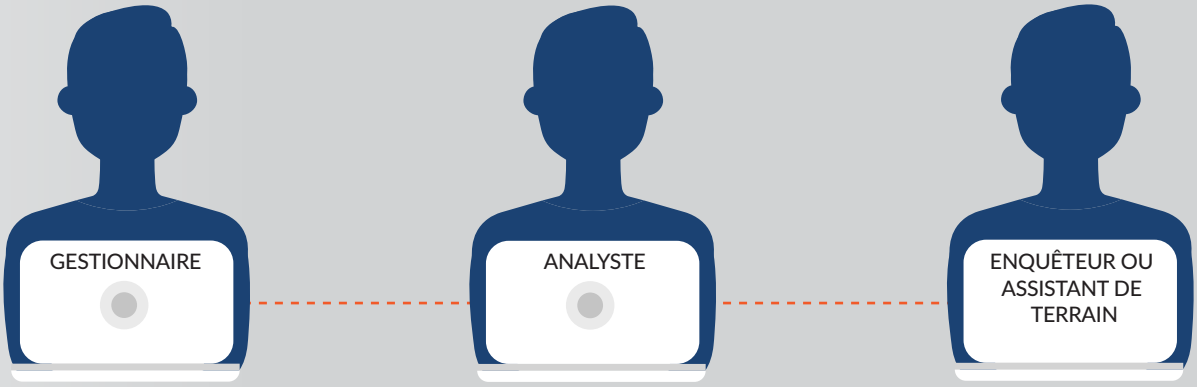
SECTION 3 Chaîne de responsabilités en matière de données

Lucia Casarin, WFP

Encadré 1

Préparation, responsabilités et rôles pour promouvoir une utilisation

Une utilisation responsable effective des données dépend de la capacité de jugement des individus ou groupes qui en ont la responsabilité ou ont pour fonction de superviser la mise en œuvre et le respect de la politique. Pour cette raison, toute politique en matière de données doit clairement déterminer et décrire les responsabilités et les rôles de chacun. Le PAM a noté que certaines politiques centralisent cette fonction, alors que d'autres ont une approche plus décentralisée. Le sentiment général est qu'une approche décentralisée ou distribuée est plus efficace, permettant à un groupe plus large de participer à la prise de décision, mais la structure finale et la délimitation des devoirs doivent être basées sur les besoins spécifiques de l'organisation et les retours de la communauté des utilisateurs et autres parties prenantes. Voici les principales responsabilités et rôles d'un gestionnaire de données du PAM, d'un analyste et d'un opérateur/assistant de terrain :



ne doit jamais demander les PII et doit décider quand l'analyse des DII est appropriée. Il doit approuver les rapports d'analyse. Il surveille constamment quelles sont les données autorisées, par qui, et dans quel but tout au long du projet. Il est responsable de la gestion des risques de l'analyse des DII. Il doit mener des audits aléatoires de la sécurité des données (par ex., retirer les registres de PII et les vérifier).

il ne doit ni avoir accès au PII, ni les demander à un fournisseur tiers et ne doit pas chercher à ré-identifier les données anonymes. Il ne doit pas partager les analyses basées sur les DII à moins que le gestionnaire n'ait donné son autorisation.

il a besoin d'accéder au PII pour appeler les personnes. Il ne doit jamais partager les PII. Il doit respecter les Procédures Opérationnelles Standard pour la sécurité des données à tout moment.

SECTION 3 Chaîne de responsabilités en matière de données

3.1 Avant la collecte des données

Consulter la législation domestique en vigueur – La législation locale peut présenter des défis pour la collecte d'informations sensibles, en particulier pour les partenaires locaux du PAM. Par exemple, les lois domestiques applicables peuvent contenir des dispositions qui peuvent obliger les partenaires locaux du PAM à dévoiler les données personnelles en leur possession au gouvernement. Dans ces circonstances, le PAM doit seulement collecter les données s'il est d'accord pour partager les données avec le gouvernement.

Garantir que la collecte des données ait un objectif spécifié – En raison des sensibilités et des risques associés à la collecte, la conservation et au partage des données, il ne faut jamais collecter des données personnelles et démographiques sans discernement. L'objectif de la collecte et du traitement des données doit être clair et sans ambigüité et doit être défini avant la collecte des données.

Minimisation des données: collecter des données sur la base des besoins d'information seulement – La collecte des données doit être limitée au minimum nécessaire pour atteindre les objectifs afin d'éviter des intrusions non nécessaires et potentiellement préjudiciables pour la vie privée des personnes. En particulier, la collecte d'informations sur l'appartenance ethnique, les opinions politiques, les croyances religieuses et les orientations/choix sexuels ou de santé doit être strictement évitée à moins qu'elle ne soit absolument nécessaire pour atteindre l'objectif de l'enquête. Ces informations ne sont généralement pas collectées dans les enquêtes sur la sécurité alimentaire su PAM.

Conduire une évaluation de l'impact sur la confidentialité – Avant de mener une collecte de données dans un pays, le PAM doit conduire une évaluation de l'impact sur la confidentialité (Privacy Impact Assessment ou PIA)[x]: c'est une analyse systématique de tous les facteurs (dont ceux légaux, opérationnels et environnementaux) qui peuvent conduire à des risques de violation des droits ou d'abus. Le PIA met au point des stratégies pour atténuer ces risques et peut être mené par un officier VAM du PAM en partenariat avec le gouvernement et d'autres parties prenantes clefs. Le PIA doit identifier tous les groupes qui sont particulièrement vulnérables en raison du contexte dans lequel les données sont collectées. Cela va permettre au PAM de maintenir des standards élevés de protection pour ces données qui peuvent permettre d'identifier un individu comme faisant partie d'un groupe vulnérable. Sinon, le PAM peut décider de ne pas collecter d'informations personnelles ou démographiques du tout. Le PIA doit prendre en compte les vulnérabilités particulières mentionnées à la section 2.

Comprendre et prendre en compte le contexte local – si possible, prenez conseils auprès de spécialistes de la protection avant de commencer une enquête (cela peut faire partie du PIA). Les meilleures pratiques incluent :

Impliquez-vous avec les communautés au sujet des principaux risques associés à la collecte de données proposée. Cela peut être fait en interviewant des membres de la communauté et à travers une revue de la littérature sur l'environnement en matière de téléphonie mobile (par ex., propriété de téléphones portables, taux d'utilisation, normes sociales et de genre) dans le pays.

- Travailler avec une organisation communautaire (community-based organization ou CBO) ou une ONG dans la communauté qui peut sensibiliser les personnes sur l'activité. Il est essential de s'impliquer avec la communauté avant de collecter les données. S'il existe des risques en matière de protection, le PAM doit informer/sensibiliser les personnes au sujet des risques établis. Cela est généralement fait avec l'aide d'une CBO locale, comme cela fut le cas pour mVAM dans l'est de la RDC. Au Niger, mVAM a créé un partenariat avec l'ONG internationale ACTED pour atteindre ce but.
- Explorer les possibilités avec les groupes qui se sont auto-organisés, où les répondants mettent eux-mêmes en place des comités de gestion.

Encadré 2

Comités de gestion et collecte de données par téléphone portable

Dans le projet pilote mVAM dans le camp 3 de Mugunga dans l'est de la RDC, les participants à l'enquête se sont organisés eux-mêmes lors de la mise en place de l'activité. Ils ont constitué un comité des résidents du camp, composé d'hommes et de femmes. Les membres du comité ont fait le lien avec le bureau de terrain du PAM à Goma pour communiquer toutes les questions ou problèmes sur la collecte de données qui se sont posés lors de l'enquête. Au début, les personnes du camp avaient beaucoup de questions sur l'objectif de l'enquête et comment/quand elles recevraient les crédit de téléphone, compensation pour leur participation à l'enquête. Les personnes voulaient savoir pourquoi le PAM collecte des données et voulaient être informées des modalités de cette activité. Ils avaient aussi besoin de conseils sur l'utilisation de base des téléphones que le PAM a fournit au début du projet. Le PAM a commencé à recevoir des appels des membres de la communauté qui voulaient en savoir plus sur ses distributions alimentaires.

Alors que l'activité continuait, les questions ont changé. Les résidents de Mugunga 3 qui se préparaient à rentrer chez eux, ont voulu savoir s'ils pouvaient garder leur téléphone quand ils partent du camps et continuer à participer à l'enquête. Les personnes ont aussi demandé s'il n'y avait pas de restrictions sur l'utilisation du crédit d'appel téléphonique que les personnes qui ont répondu à l'enquête ont ensuite reçu.

Le comité a aidé les plus âgés à utiliser les appareils téléphoniques fournis par le PAM et à retrouver les répondants qui ont manqué un passage de l'enquête, ce qui a permis d'avoir des taux mensuels de réponses élevés. Le comité a aussi été en contact avec les enquêteurs du PAM et les leaders locaux qui s'occupent de la gestion du camps.

Choisir le bon prestataire de services – La décision de mettre en œuvre des enquêtes soi-même (gestion en interne) ou de les sous-traiter a des implications différentes en terme de risque.

- **Interne** – Quand le PAM met en œuvre une enquête lui-même, le personnel du PAM collecte les numéros de téléphone des bénéficiaires et gère les listes de contacts (liste de noms et numéros de téléphone). C'est au PAM d'obtenir le consentement des répondants, de gérer les numéros de téléphone en toute sécurité et de collecter les données de manière responsable. Le PAM a la responsabilité de garantir que son personnel respecte les bonnes pratiques en matière de gestion des données et de leur confidentialité. Le PAM est considéré être le seul contrôleur des données dans les cas où le PAM a la responsabilité intégrale de la protection des données personnelles des répondants.
- **Sous-traitance** – Le PAM sous-traite parfois les enquêtes par téléphone à des centres d'appels commerciaux ou des prestataires de services pour les enquêtes par SMS ou IVR (système de réponse vocale interactif). Le prestataire de services tiers a une liste de numéros de téléphone (obtenus de différentes façons, dont des campagnes présentes ou à travers des opérateurs de téléphonie mobile) ou le PAM fournit les numéros de téléphone. Dans le premier cas, le PAM n'est pas responsable de l'utilisation et de la gestion des numéros. Dans le second cas, le rôle du PAM est de vérifier et de superviser le prestataire de services tiers. Notez que le PAM reste le contrôleur des données même quand il délègue l'utilisation des détails des téléphone portables à un prestataire tiers et l'organisation est pleinement responsable de la protection des données personnelles de personnes tout au long du cycle de vie des données.

3.2 Lors de la collecte des données

Chercher à obtenir un consentement informé de la part des participants – C'est la pierre angulaire du système entier de protection des données et fait référence aux principes de légalité et d'équité: aucune donnée personnelle ne doit être collectée sans le consentement informé de la personne. Pour permettre aux gens de donner leur consentement informé, le PAM (ou le prestataire de services qui travaille pour le PAM) doit garantir que les personnes ont reçu les informations suivantes :

- L'identité et le mandat du PAM et du prestataire de services
- Les types de données personnelles qui seront collectées
- L'objectif de l'utilisation des données personnelles
- Acteurs avec lesquels les données devraient être partagées (par ex., opérateurs des réseaux mobiles ou autres acteurs humanitaires)
- Comment accéder, mettre à jour, modifier, corriger ou effacer les données quand c'est faisable et pertinent
- Le droit du bénéficiaire de refuser de fournir des informations et les implications de retirer son consentement, dont l'effet que cela peut avoir sur le type d'assistance qui peut être apportée, si cela est possible.

La sécurité des communications avec des appareils portables n'est pas forcément assurée et ces communications peuvent être piratées par des parties tierces avec des compétences et des ressources appropriées. Pour cette raison, le PAM devrait être attentif à ne pas inclure des PII sensibles dans les enquêtes. Les questionnaires ne doivent pas mentionner des lieux spécifiques, des informations portant sur l'appartenance ethnique ou religieuse ou les noms des participants. Des outils sûrs doivent être utilisés pour les messages et les enquêtes (des exemples sont fournis à la Section 4).

Encadré 3

Lignes directrices pour identifier et sélectionner les prestataires de services tiers.

- Lors de la sélection, les prestataires de services doivent être examinés de près et approuvés. Le PAM doit être très attentif aux compagnies qui se portent candidates et évaluer leur conformité aux meilleures pratiques en matière de sécurité et de confidentialité des données.
- Pour une liste de prestataires approuvés, consultez les Accords de Long Terme existants (Long Term Agreements ou LTAs)[xi] sur les services de collecte de données à distance incluant les entretiens téléphoniques assistés par ordinateur (CATI), IVR (système de réponse vocale interactif), SMS et les enquêtes en ligne.
- Les prestataires doivent remplir au minimum les exigences suivantes:

  – Les numéros de téléphone doivent être obtenus de manière légale.

  – Les données (sous forme physique ou digitale) sont conservées dans un lieu sûr.

  – Des procédures opérationnelles standard sont en place pour les opérateurs de centre d'appels et les personnes responsable des informations; ils doivent être tenus de respecter les standards les plus élevés et les meilleures pratiques pour assurer la sécurité des données.

- Tout nouveau contrat avec un prestataire de services doit inclure des clauses de confidentialité claires. Il doit aussi spécifier combien de temps les PII and DII seront conservées une fois qu'elles auront été utilisées dans un but spécifique et doit détailler comment le prestataire va partager les données avec le PAM (c.-à-d. par des emails cryptés, dans des enveloppes fermées et signées, etc.).

Encadré 4

Défis associés au consentement

Le consentement n'est une simple case à cocher. Un consentement pleinement informé inclut une divulgation complète des risques et des conséquences négatives potentielles de la participation. Pour une organisation humanitaire comme le PAM qui intervient dans des contexte d'urgence volatile et complexe, ce n'est pas toujours faisable ou même possible. Cependant, en principe, une certaine forme de consentement qu'il soit simple ou obtenu par un intermédiaire doit être obtenue même dans des contextes risqués et particulièrement quand le PAM collecte des données sur les groupes économiquement défavorisés et marginalisés et des communautés qui ont des besoins de protection importants comme les personnes déplacées et les réfugiés.

L'importance croissante des données issues du monde participatif (crowdsourcing) à travers l'utilisation d'application de messageries et d'agents conversationnels (chatbots) pose un autre défi à l'obtention du consentement. Le PAM qui teste ces nouveaux instruments et applications doit faire le compte-rendu de son apprentissage et partager les meilleures pratiques afin d'établir les stratégies et les standards à suivre pour répondre aux défis de la responsabilité en matière de données à notre époque.

Pour plus d'informations, voir le Manuel Responsible Data Forum handbook et les lignes directrices du Comité International de la Croix Rouge (International Committee of the Red Cross).

Etre particulièrement attentif dans les situations de conflit – Dans les situations de conflit, il est important d'éviter les modalités qui laissent une grande empreinte digitale qui peut exposer le PAM ou les personnes à des risques. Cela inclut les SMS et la composition digitale aléatoire (random digit dialling ou RDD).[xii] Il est particulièrement important d'être prudent avec les SMS car les messages restent dans les téléphones que des forces de sécurité ou d'autres groupes peuvent fouiller – à moins que la personne qui a répondu n'efface le message. Les appels vocaux sont plus appropriés dans des situations de conflit car ils ne laissent pas la même trace sur le téléphone d'une personne répondant à l'enquête. Il faut par ailleurs prendre en compte les facteurs suivants :

- C'est une bonne pratique d'organiser les appels dans la soirée ou à un moment que préfère la personne à interviewer, quand les personnes sont dans le privé chez eux.
- Il existe des interdictions strictes d'appels dans certaines zones de conflit. Mener une collecte de données par téléphone dans ce contexte signifie mettre les gens en danger. Une évaluation adéquate de la situation avec une perspective juridique et politique est importante pour éviter ce type d'erreur. Souvenez-vous que quelque fois les risques de collecte de données dans des contextes de conflit sont simplement trop élevés.
- Quand les risques sont plus importants que les bénéfices, pensez à des approches alternatives (par ex., la détection à distance, le suivi des réseaux sociaux).
- Chercher à obtenir une autorisation sécuritaire pour votre projet en partageant le concept de votre collecte de données avec l'officier chargé de la sécurité du PAM.

3.3 Après la collecte de données

Garantir l'intégrité des données – Pour analyser votre responsabilité en matière de données, la première étape est de vérifier et de valider les données. Du point de vue d'un analyste, cela est généralement fait lors du processus de nettoyage des données, mais il existe d'autres facteurs structurels qui sont critiques pour l'intégrité comme les restrictions d'accès, l'interopérabilité entre les différentes plateformes, les changements d'enregistrement des données, et les mécanismes de backup en cas de défaillances. Les systèmes de gestion de l'information doivent être mis en place de manière à ce que l'information soit disponible pour les bonnes personnes au bon moment, en respectant le principe de garantie de la confidentialité dès la conception (privacy by design). Gérer les biais des données est aussi une étape importante pour assurer l'intégrité des données, particulièrement quand les résultats ont des implications pour l'allocation des ressources de l'aide, notamment quand certaines communautés ont la priorité sur d'autres ou quand des groupes vulnérables sont exclus. En raison des taux de propriété de téléphone portable et de connexion disproportionnés, l'existence de biais est inhérente aux enquêtes par téléphone portable. La littérature existante a montré que les résultats sont généralement biaisés dans la direction des populations les plus riches, plus jeunes, plus éduquées et masculines des zones urbaines. Le PAM prend en compte les biais lors de l'analyse des données avec une stratification postérieure, une repondération et une triangulation.[xiii]

Conserver les données dans un environnement sûr – Le PAM doit chercher à offrir des standards élevés de sécurité des données et est responsable vis-à-vis des répondants suite à la collecte des données.

SECTION 3 Chaîne de responsabilités en matière de données

Une fois que les données ont été collectées, il devient une cible potentielle pour des acteurs malveillants qui cherchent à porter atteinte à sa réputation ou à obtenir des informations sur des cibles potentielles pour des attaques ou dans d'autres buts. Les données doivent être conservées dans un lieu sûr, qu'il soit physique ou digital.[xiv] Inévitablement, les données seront conservées sur plusieurs plateformes, pendant toute leur durée de vie et plusieurs instruments sont utilisés pour la collecte des données (appareil portable, IVR, web, papier), la conservation (appareil portable, ordinateur portable, base de données centralisée et papier) et le nettoyage et l'analyse des données (documents Excel, SQL, visualisation des données et autres plateforme de compte-rendu). Un plan de sécurité des données doit être mis en place pour chaque plateforme utilisée.

Eliminer les données une fois que l'objectif est atteint – Avec la quantité très importante de données générées par le PAM à travers l'utilisation d'outils conventionnels et nouveaux, il faut faire une distinction entre les données ouvertes et disponibles comme bien public et les données qui doivent être éliminées quand l'objectif spécifique du projet a été atteint. Dans le premier cas, le PAM a mis en place un système de meilleures pratiques avec une banque de données ouvertes facilité par API (Application Programming Interface), où les rapports sur la sécurité alimentaire sont librement disponibles en ligne avec les données agrégées qui ont été rendues anonymes. Dans le second cas, il est critique que la conception de l'enquête comprenne un calendrier pour les données avec une date « d'expiration claire » afin qu'à la fin du projet, les données soient éliminées de manière responsable.[xv]

Agir rapidement en cas de violation des données – Même si les contrôles requis et les systèmes de vérification sont en place, une violation peut se produire à un point particulier de la chaîne de responsabilité. Des violations de la confidentialité et la divulgation de données, qu'elles soient intentionnelles ou non, peuvent avoir des répercussions éthiques et opérationnelles importantes. La perte, le vol et la mauvaise utilisation de données peut causer des préjudices aux personnes que le PAM cherche à aider ainsi qu'à son propre personnel. Une fois qu'une violation de la confidentialité a lieu, il n'est pas possible de retourner en arrière, et elle peut affecter de manière négative les bénéficiaires pour le reste de leur vie. Tous les incidents ou les vols doivent faire immédiatement l'objet d'un compte-rendu à l'équipe dirigeante et aux officiers chargés de la sécurité du PAM. Le PAM doit aussi établir un plan de contingence au cas où les outils ou les données sont confisquées ou perdues (par ex., capacité d'effacer les données à distance et garder des mécanismes de sauvegarde). De plus, un système de gestion des cas de violation des données doit être mis en place pour enregistrer, gérer et faire le suivi des rapports d'incidents.

Garder la redevabilité à l'esprit – les répondants doivent être capables de contacter le PAM et/ou les prestataires d'accès pour accéder, vérifier, corriger, mettre à jour et effacer leurs données personnelles à tout moment. Certains des mécanismes simples proposés par la politique sur la confidentialité des données du PAM incluent : a) donner les coordonnées des points focaux du bureau de pays et des sous-bureaux du PAM; b) mettre un place un bureau sur le site du projet pour recueillir des commentaires; et c) utiliser les mécanismes existants pour recueillir les plaintes et les retours dont des lignes directes (hotlines) gratuites, des boîtes pour récolter des suggestions, et des groupes basés sur les communautés.

Résumé

Avant la collecte des données

1. Consulter la législation domestique en vigueur
2. Garantir que la collecte des données ait un objectif spécifié
3. Minimisation des données: collecter des données sur la base des besoins d'information seulement
4. Conduire une évaluation de l'impact sur la confidentialité
5. Comprendre et prendre en compte le contexte local
6. Choisir le bon prestataire de services

Lors de la collecte des données

1. Chercher à obtenir un consentement informé de la part des participants
2. Etre particulièrement attentif dans les situations de conflit

Après la collecte de données

1. Garantir l'intégrité des données
2. Conserver les données dans un environnement sûr
3. Eliminer les données une fois que l'objectif est atteint
4. Agir rapidement en cas de violation des données
5. Garder la redevabilité à l'esprit

Outils et méthodes que les officiers du PAM sur le terrain peuvent utiliser pour atténuer les risques

4

1. Garder les listes de participants confidentielles et ne pas partager les numéros de téléphone

2. Utiliser les méthodes de transfert cryptées

3. Utiliser un système de stockage des données sûr

4. Garantir que les prestataires tierce partie respectent leurs obligations

5. Prendre des précautions additionnelles lors du partage ou du compte-rendu sur la géo- localisation

6. Suivi, évaluation and réitération

7. Travailler avec le gouvernement

8. Approches alternatives

SECTION 4 Outils et méthodes que les officiers du PAM sur le terrain peuvent utiliser pour atténuer les risques

Garder les listes de participants confidentielles et ne pas partager les numéros de téléphone – les bases de données du PAM doivent être conservées sous clefs (lorsque le support est le papier) ou dans des documents cryptés dont l'accès est protégé par un mot de passe. Quand les numéros de téléphone sont conservés, ils doivent être convertis en un identifiant (ID) anonyme – un code alphanumérique généré de manière aléatoire qui rend impossible de retrouver le numéro initial – avant que les données ne soient partagées. Quand le PAM travaille avec une tierce partie, le fournisseur doit avoir pour instruction de ne pas partager les numéros de téléphone ou les noms des répondants avec le PAM. **Utiliser les méthodes de transfert cryptées** – L'email n'est pas un outil sûr de transfert de données. Si vous avez besoin de transférer des listes de numéros de téléphone, il faut utiliser le système de partage de documents 'WFP Box' plutôt que le système d'emails Outlook. Si pour n'importe quelle raison, vous utilisez une méthode alternative, assurez-vous que votre circulation de messages ou d'emails soit cryptée en utilisant un outil sûr (par ex., Signal Whisper ou d'autres outils de cryptage ou de conservation en ligne). **Utiliser un système de stockage des données sûr** – le PAM a mis à jour les logiciels Pollit et Verboice pour permettre le stockage local des numéros de téléphone. Cela rend nos systèmes moins vulnérables à un piratage que si les données sont stockées sur une plateforme publique. C'est la confidentialité dès la conception (privacy by design). Une autre bonne pratique est l'authentification à deux facteurs (two-factor authentication ou 2FA), qui est un processus sécuritaire qui prévoit l'authentification des utilisateurs par deux méthodes, une qui est généralement un mot de passe et l'autre une vérification email/appel/message (un exemple es la vérification Google en deux étapes)[xvii].

De nombreuses organisations ont commencé à utiliser 2FA pour protéger les données sensibles et confirmer l'identité des personnes qui essayent d'accéder au système.

Garantir que les prestataires tierce partie respectent leurs obligations – un prestataire tierce partie doit garder les numéros de téléphone et il ne doit pas lui être demandé de les partager avec le bureau. Une disposition demandant que le prestataire élimine ces informations des données qui sont éventuellement envoyées au PAM peut être ajoutée à l'accord qui régit la collaboration entre le PAM et des prestataires tierce partie, particulièrement dans des contextes sensibles. Son respect doit être vérifié par le PAM à travers des audits aléatoires ainsi que des vérifications par une partie externe.

Prendre des précautions additionnelles lors du partage ou du compte-rendu sur la géo-localisation – L'exactitude de la localisation GPS (par ex., tours de téléphonie mobile) doit être détériorée en fournissant seulement les coordonnés avec deux décimales. Lors du partage de données de géo-localisation, assurez-vous d'utiliser des méthodes de transferts cryptées intégrales (end-to-end encryption transfer methods). Dans des contextes de conflit, soyez prudent quant à la fourniture d'informations de géo-localisation. Les informations sur l'endroit où se trouvent les répondants font partie des données les plus sensibles dans ce type de contexte.[xviii] Le PAM travaille souvent avec des informateurs clefs dans des zones assiégées ou des zones difficiles à atteindre. Lors du compte-rendu des résultats, ne mentionnez pas la localisation précise de l'informateur car cette information peut lui faire courir des risques.

SECTION 4 Tools and methods that WFP Field Officers can use to mitigate risk

Suivi, évaluation and réitération – Faire le compte-rendu des atteintes à la sécurité et partager les leçons apprises est fondamental pour faire prendre conscience et diffuser les bonnes pratiques en matière de sécurité. Dans le cas d'une atteinte aux données, le PAM doit prendre des mesures adéquates pour contenir le problème et le réparer, comme par exemple en informant l'équipe dirigeante (directeur du bureau de pays or le directeur approprié), en faisant le compte-rendu de l'incident et en réparant la violation des données dans le cadre d'un processus de compte-rendu global après action impliquant tous les acteurs pertinents. Note qu'une violation des données est une cause de rupture de contrat avec un prestataire tierce partie.

Travailler avec le gouvernement – Le PAM travaille de manière rapprochée avec les autorités locales. Nous suggérons que seules les données anonymes soient partagées avec les partenaires du gouvernement avec lesquels le PAM collabore et seulement si les répondants ont donné leur consentement quand ils ont décidé de participer.

Approches alternatives – Souvenez-vous, nous n'avons pas besoin de tout savoir ! Dans les environnements les plus sensibles, les informations qui permettraient d'identifier un individu ou un groupe ne doivent pas être collectées. Des approches alternatives impliquent d'utiliser les applications de discussions cryptées[xix] qui offrent une meilleure sécurité que le SMS. La plupart des centres d'appels commerciaux utilisent un logiciel qui empêche un opérateur de voir le numéro qui est composé.

Lucia Casarin, WFP

Conclusion:
le PAM en faveur de données ouvertes et gérées de manière responsable

5

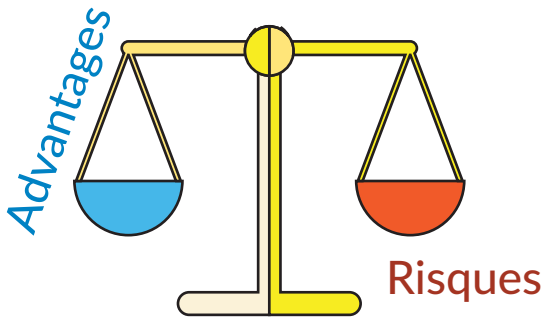
Les enquêtes par téléphone portable peuvent être très bénéfiques pour les opérations du PAM, particulièrement dans les zones difficile d'accès. Cependant, ce potentiel peut seulement être exploité de manière éthique et durable en respectant un processus solide de responsabilité en matière de données. Si le processus décrit dans ce document est mis en œuvre de manière permanente dans les projets d'enquête par téléphone portable du PAM, en utilisant les outils et méthodes présentés dans la section 4, et s'il est mis à jour régulièrement pour prendre en compte les derniers développements dans le domaine de la responsabilité en matière de données, il va permettre d'assurer une balance optimale entre les avantages de l'utilisation des données digitales et les risques potentiels associées à cette utilisation.

Il n'existe pas de raccourcis dans le domaine de la responsabilité en matière de données et la responsabilité est celle de tous les acteurs du cycle de vie des données humanitaires. La responsabilité en matière de données est un processus qui requiert de réévaluer les risques régulièrement pour prendre en compte les changements de contexte ou d'utilisation des données. Les documents comme celui-ci doivent aussi être revus régulièrement pour prendre en compte les derniers développements dans un domaine qui évolue rapidement.

Ce guide de terrain doit donc être considéré comme un document en évolution. Si vous notez des erreurs ou si vous trouvez que les pratiques suggérées dans ce document ne fonctionnent pas bien dans une situation particulière, n'hésitez pas à nous contacter à l'adresse fournie ci-dessous.

Les enquêtes par téléphone portable peuvent être très bénéfiques pour les opérations du PAM

...en respectant un processus solide de responsabilité en matière de données!



Une balance optimale entre les avantages de l'utilisation des données digitales et les risques potentiels associées à cette utilisation.

Annexe

Lectures recommandées

Electronic Cash Transfer Learning Action Network (eLAN). Data Management and Protection Starter Kit

Gordon, Grant, 2016. Monitoring Conflict to Reduce Violence: Evidence from a Satellite Intervention in Darfur

GSMA, 2014.Guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak

Harvard Humanitarian Initiative, 2016. Data Preparedness: Connecting Data, decision-making and humanitarian response

Harvard Humanitarian Initiative, 2017. The Signal Code: A Human Rights Approach to Information During Crisis

International Committee for the Red Cross. Humanitarian Futures for Messaging Apps

International Organization for Migration, 2010. Data Protection Manual

McDonald, Sean, 2016. Ebola: A Big Data Disaster – Privacy, Property and the Law of Disaster Experimentation

OCHA, Leiden University and NYU GovLab, 2016. Mapping Responsible Data Approaches

Oxfam, 2015.Responsible Program Data Policy

Responsible Data Forum, 2016.The Handbook of the Modern Development Specialist

UN Global Pulse, 2016.Privacy Advisory Group Meeting Report 2015-2016

UN OCHA, 2016. Think Brief - Building Data Responsibility into Humanitarian Action

WFP, 2016. Guide to Personal Data Protection and Privacy

[i] Il y a eu plus de 6 000 violations de données depuis 2005.

[ii] Voir, par exemple, "Yahoo hack: 1bn accounts compromised by biggest data breach in history".

[iii]Le Groupe international pour la Responsabilité en matière de données (*The International Data Responsibility Group* ou IDRG) est un réseau mondial d'experts et d'organisations qui travaillent sur les principes et standards qui encadrent la révolution dans le domaine des données dans le contexte de l'action humanitaire, du développement durable, de la justice et de la paix. Ces membres cherchent à construire un socle de connaissances qui font autorité et permettent l'expérimentation responsable en matière de diffusion, traitement et utilisation de données et la minimisation des risques. L'IDRG est conçue comme une plateforme en réseau avec un secrétariat qui assure la coordination basé à La Haye. Les partenaires affiliés et ceux dans le domaine de la recherche se rencontrent chaque année lors d'une conférence annuelle internationale sur la responsabilité en matière de responsabilité.

[iv] Source: définition de travail du Forum sur la responsabilité en matière de données, Septembre 2014.

[v] C'est inspiré du règlement européen sur la protection générale des données General Data Protection GDPR article 4 sous 1: «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

[vi] Un numéro de téléphone, s'il est triangulé avec d'autres informations qui ne sont pas strictement personnelles (par ex., identité du fournisseur, couverture géographique du fournisseur et lieu de naissance de l'utilisateur) peut permettre à des pirates malveillants de retrouver l'identité de la personne indirectement. Les numéros de portable doivent être considérés comme une information personnelle et traités en conformité avec les standards du PAM en matière de protection des données personnelles. Le PAM enregistre d'habitude les noms et numéros des personnes dans des listes que les opérateurs utilisent pour faire les appels. Les listes identifient si les personnes qui répondent vivent dans un camp pour personnes déplacées ou réfugiés et contiennent parfois le nom du camps et sa localisation. Le PAM ne collecte pas les adresses physiques des personnes, les listes vont mentionner un lieu de résidence (par ex., un camp, un quartier, un village). Les listes vont aussi probablement mentionner si la personne est un réfugié, un déplacé interne ou quelqu'un qui est rentré chez lui (c.-à-d. quelqu'un qui habitait auparavant dans un camp). Cela peut être utilisé pour identifier les individus par déduction – en combinant un certain nombre d'informations qui permettent dire que le répondant ne peut que être la personne X. Une autre menace est qu'une fois que l'acteur malveillant a accès à une personne à travers son numéro de téléphone, il pourrait contacter cette personne pour lui extorquer plus d'informations ou de l'argent ou du crédit téléphonique en se présentant comme un opérateur, ou à travers d'autres moyens d'ingénierie sociale.

[vii] Taylor, Linnet, Luciano Floridi, et Bart van der Sloot, 2017. "Group Privacy".

[viii] Voir le portail GDPR portal.

[ix] Pour plus d'informations sur la préparation en matière de données, voir Harvard Humanitarian Initiative report.

[x] Pour plus d'informations sur le PIA, voir le Kit de départ en matière de gestion et de protection des données du Réseau d'Action et d'Apprentissage pour les transferts électroniques de cash (Electronic Cash Transfer Learning Action Network's ou eLAN) disponible à http://elan.cashlearning.org/

[xi] LTAs sont disponibles dans la base de données gérée par la division des achats au siège (database managed by HQ Procurement). Pour plus d'informations, contacter

HQ.Procurement@wfp.org

[xii] La composition digitale aléatoire est une technique d'échantillonnage pour les enquêtes par téléphone selon laquelle les participants à l'enquête sont sélectionnés par la composition au hasard des numéros de téléphone. Utilisée par les centres d'appels ou par des prestataires tierce partie qui n'ont pas de liste de numéros de téléphone, cette technique a pour avantage d'inclure des numéros qui ne sont pas sur des listes et qui auraient été omis si les numéros avaient été tirés d'un annuaire.

[xiii] Des documents additionnels qui apportent des détails sur comment le biais a été pris en compte sont disponibles sur les pages pays du site mVAM.

[xiv] Comme minimum, les spécifications suivantes sont recommandées:

- **SERVEUR:**
  - Processor: Inter(R) Xeon(R) CPU – 4 (or 6) Processors
  - Mémoire: 16 (or 32) GB RAM
- **BASE DE DONNEES:**
  - Microsoft SQL Server
  - MongoDB

[xv] Il n'existe pas une norme unique établie sur le temps de conservation des données, car cela dépend du pays et du contexte. Des orientations sur la détention de données personnelles sont disponibles aux pages 82-83 du *Guide du PAM sur la protection et la confidentialité des données personnelles*. "Le PAM ne doit pas conserver des données personnelles plus longtemps qu'il n'est nécessaire pour atteindre l'objectif légitime spécifique pour lequel elles ont été collectées…. Une extension est permise quant elle est dans l'intérêt des bénéficiaires…les données rendues anonymes ou moins sensibles peuvent être conservées plus longtemps si c'est utile ».

[xvi]Les lignes directrices mVAM pour rendre anonyme des données sont disponibles en cliquant ici

[xvii] Pour une liste des sites ou des services dans le domaine du 2FA, visitez ce site.

[xviii] Pour plus d'informations sur ce sujet (même si pas spécifiquement lié à des contextes de conflits), voir 'Building Data Responsibility Into Humanitarian Action' du NYU GovLab, du Centre sur l'Innovation de l'Université de Leiden et OCHA, p. 3: "(...) le type d'informations le plus critique produit par l'écosystème est l'information sur les moments et le lieux des activités spécifiques des populations affectées, c.-à-d. « les métadata spatiotemporelles.»

[xix] Une liste d'applications sûres de messagerie est disponible ici

Kusum Hachhethu, WFP

Contact

Si vous avez des commentaires, questions ou suggestions sur ce guide de terrain, merci de contacter les collèges suivants qui ont participé à la rédaction de ce document:

Jos Berens, *Chargé de projet sur la responsabilité en matière de données*, Centre pour l'Innovation de l'Université de Leiden (j.b.berens@fgga.leidenuniv.nl)

Jean-Martin Bauer, *Analyste senior de la sécurité alimentaire*, PAM (jean-martin.bauer@wfp.org)

Angie Lee, *Analyste de la sécurité alimentaire*, PAM (angie.lee@wfp.org)