7. Utilisation responsable des technologies de collecte et de gestion des données

Le concept de « données responsables » holistique, impliquant de porter une attention particulière à la gestion des données à chaque étape du cycle de projet.

Les praticiennes et praticiens du développement et de l'action humanitaire qui collectent et diffusent des données de projet sont confrontés à des changements technologiques et politiques sur le terrain. Il est important de renforcer les connaissances et les pratiques en matière de données responsables afin d'identifier et réduire de manière efficace les risques pour les organisations et les personnes participant aux projets, et de concevoir des plans de collecte, d'utilisation et de diffusion des données relatives au projet qui les mitigent.

La pratique guidée par le principe de « ne pas nuire » dans les projets doit être élargie pour inclure les aspects physiques, numériques et psychosociaux liés à la sécurité des données.

Il est maintenant plus facile de recueillir et archiver des quantités massives de données. Bien que les méthodes et outils de collecte de données numériques sont conçus pour augmenter l'efficacité et l'exactitude des données, les bailleurs de fonds exigent également davantage de collecte et d'analyse de données pour les projets financés. Cela a conduit à une situation où des quantités importantes de données sont recueillies, produites et mises à disposition par les organisations. Cependant, les organisations et le personnel peuvent ne pas être parfaitement au courant de la façon de protéger les données de manière responsable.

Au stade de la conception du projet, on réfléchit rarement aux informations qui doivent être stockées, aux métadonnées qui sont automatiquement recueillies, et aux acteurs qui auront accès à ces données. Les organisations doivent clarifier dès le départ quelles données seront communiquées, auprès de qui elles seront recueillies et avec qui elles seront partagées, et dans quelles circonstances et conditions. Elles doivent aussi donner des informations détaillées sur l'entretien responsable, la conservation ou la destruction des données.

Cycle de vie des données

Le cycle de vie des données décrit ce qui arrive aux données à travers un cycle de projet, depuis la collecte et le stockage des données, jusqu'à l'analyse, à la communication et au partage des données. Les principes et les pratiques de gestion responsable des données doivent être intégrés à chaque étape.

Consentement éclairé

Les éléments standards devraient inclure :

- des explications faciles à comprendre sur le but de la collecte de données
- pourquoi les répondant-e-s ont été invités à participer
- le caractère volontaire de la participation
- le temps nécessaire pour participer et la forme que prendra la participation
- les avantages et les risques liés à la participation à la collecte de données
- les types de données qui seront recueillis
- la façon dont les données seront stockées et analysées
- avec qui elles seront partagées
- les utilisations prévues de ces données
- le niveau de confidentialité et d'anonymat des données des répondant-e-s
- la possibilité de retirer son consentement en tout temps
- les coordonnées d'une des personnes qui mènent l'étude, au cas où les répondant-e-s auraient d'autres questions ou préoccupations.

La **confidentialité** signifie que même si les membres de l'équipe de projet (ou les membres du personnel désignés) connaissent l'identité de certain-e-s répondant-e-s, ils s'engagent à respecter certains principes pour garder confidentiel tout ce qu'ils apprendront au sein de l'équipe de projet. Cet engagement de confidentialité peut être volontaire ou légalement requis, selon les circonstances et le contexte de l'objectif de la collecte de données. La confidentialité peut être représentée par une échelle qui part d'un point où toutes les données recueillies sont publiques, jusqu'à un autre où toutes les données (et les résultats de ces données) sont entièrement confidentielles et ne peuvent être partagées au-delà des personnes désignées.

La confidentialité est une nécessité si nous voulons nous assurer que les répondant-e-s puissent donner des réponses complètement honnêtes, notamment en ce qui concerne les relations de pouvoir.

L'**anonymat** correspond à la mesure dans laquelle les répondant-e-s peuvent être associés aux réponses que nous avons enregistrées. Cela signifie que des mesures spécifiques ont été prises afin de s'assurer que les réponses (données) ne permettent pas d'identifier les répondant-e-s. L'anonymat peut être atteint en éliminant de la collecte de données ou d'un ensemble de données toutes les réponses ou variables qui pourraient permettre d'associer certaines réponses ou données à des répondant-e-s individuels spécifiques. L'anonymat peut aussi être représenté comme une échelle qui part d'un point où les réponses/données peuvent facilement permettre de retracer les répondant-e-s individuels (p. ex. contient les noms) jusqu'à un autre point où les réponses/données sont totalement anonymes et ne peuvent pas être associées à des répondant-e-s spécifiques.

L'anonymat est souhaitable dans la collecte des données parce qu'elle peut limiter les dégâts causés par une éventuelle fuite de données non autorisée. Notez que même si les noms ne sont pas divulgués, il faut considérer d'autres moyens par lesquels les répondant-e-s pourraient être identifiés. Par exemple, l'âge, le sexe et le nom de la communauté pourraient être suffisants pour identifier une personne dans une petite communauté.

La **protection des données** se réfère à l'existence physique des données (sur quel support - papier ou électronique, et où les données sont stockées), la capacité de stocker et d'accéder aux données au cours d'une période requise pour les utiliser, la façon dont l'accès aux données est géré, et les exigences légales de conserver certaines données pendant une période déterminée. Conseils :
- Planifier ce qui se passera après le projet et lorsque les données seront définitivement supprimées.
- Examiner la possibilité de sauvegarder les données à l'extérieur du site.

La **sécurité des données** fait référence à la menace d'origine humaine par rapport aux données (p. ex. accès non autorisé aux données ; intention de vous empêcher d'accéder à vos données). Conseils :
- Utiliser des technologies et des applications avec chiffrement.
- Utiliser un outil de gestion des mots de passe.
- Assurer la sécurité des ordinateurs de votre organisation et de vos ordinateurs personnels.
- Lire attentivement les modalités des services que vous utilisez.

Utilisation responsable des technologies de collecte et de gestion des données

LISTE DE CONTRÔLE

www.salanga.org

Questions clés pour l'utilisation responsable des technologies de collecte et de gestion des données

1 COLLECTE CIBLÉE

Quelles données allez-vous recueillir et comment ?

- ☐ Nous avons une vision claire de la raison pour laquelle nous voulons entreprendre la recherche et la façon dont les données seront utilisées
- ☐ Seule l'information qui est nécessaire dans le cadre du projet est recueillie
- ☐ Un consentement éclairé a été donné par chaque répondant-e avant la collecte des données
- ☐ Une grande priorité est accordée à l'anonymisation des données
- ☐ Il est culturellement approprié d'utiliser les technologies sélectionnées avec le groupe de répondant-e-s

2 IMPLICATION RESPECTUEUSE

Auprès de qui allez-vous recueillir des données ?

- ☐ L'utilisation des technologies de collecte de données ne causera aucun préjudice aux groupes vulnérables
- ☐ Les manières dont les répondant-e-s sont potentiellement vulnérables sont décrites

3 STOCKAGE DES DONNÉES

Où allez-vous stocker les données ?

- ☐ Les risques et avantages des différents types de stockage ont été considérés
  (physique ; serveurs hors site ; stockage dans le nuage)
- ☐ Les pratiques de gestion responsable des données sont prises en considération dans l'ensemble du cycle de vie des données
- ☐ Des règles sont établies pour le traitement des données à long terme
  (combien de temps les données seront conservées ; l'information est cryptée…)

4 ACCÈS AUX DONNÉES

Qui aura accès aux données ?

- ☐ Les rôles sont définis pour préciser qui aura accès à quels types de données
- ☐ Des conditions d'utilisation sont élaborées pour les données partagées avec des tiers
- ☐ Des niveaux d'autorisation différents liés aux données sont attribués aux différentes catégories de personnes
- ☐ Toutes les personnes qui ont accès aux données ont une bonne compréhension de la sécurité des données
- ☐ Des règles sont en place pour s'assurer que les données ne se retrouvent pas entre de mauvaises mains

Ce document a été adapté du document « Responsible Development Data – Practitioner's Guide (V1) » [https://responsibledata.io/]

SPUR CHANGE Capacity-Building & Knowledge Sharing for Small and Medium Organizations (SMO) | inter-council network | Global Affairs Canada | Affaires mondiales Canada | salanga