

MANUEL SUR LA PROTECTION DES DONNÉES DANS L'ACTION HUMANITAIRE

DEUXIÈME ÉDITION



BRUSSELS
PRIVACY
HUB



CICR

MANUEL SUR LA PROTECTION DES DONNÉES DANS L'ACTION HUMANITAIRE

CHRISTOPHER KUNER ET MASSIMO MARELLI

DEUXIÈME ÉDITION

SOMMAIRE

REMERCIEMENTS	10
AVANT-PROPOS	11
GLOSSAIRE DES TERMES ET ABRÉVIATIONS	13
1 ^{re} PARTIE – CONSIDÉRATIONS D'ORDRE GÉNÉRAL	
CHAPITRE 1: INTRODUCTION	21
1.1 Contexte	22
1.2 Objectif	23
1.3 Structure et approche	27
1.4 À qui s'adresse ce manuel?	27
CHAPITRE 2: PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES	29
2.1 Introduction	30
2.2 Notions élémentaires de la protection des données	33
2.3 Ensembles de données agrégées, pseudonymisées et anonymisées	36
2.4 Droit applicable et organisations internationales	37
2.5 Principes applicables au traitement des données	38
2.5.1 Principes de licéité, de loyauté et de transparence du traitement	38
2.5.2 Principe de limitation des finalités	39
2.5.3 Principe de proportionnalité	39
2.5.4 Principe de minimisation des données	41
2.5.5 Principe de qualité des données	42
2.6 Situations particulières en matière de traitement des données	42
2.6.1 Finalités de santé	42
2.6.2 Activités administratives	44
2.6.3 Traitement ultérieur	44
2.7 Conservation des données	46
2.8 Sécurité des données et du traitement	47
2.8.1 Introduction	47
2.8.2 Sécurité physique	49
2.8.3 Sécurité informatique	49
2.8.4 Devoir de discrétion et conduite du personnel	51
2.8.5 Plan d'urgence	51
2.8.6 Méthodes de destruction	52
2.8.7 Autres mesures	53
2.9 Le principe de responsabilité	53
2.10 Information	54
2.10.1 Données recueillies auprès de la personne concernée	54
2.10.2 Notices d'information	55
2.10.3 Données non recueillies auprès de la personne concernée	56

2.11	Droits des personnes concernées	57
2.11.1	Introduction	57
2.11.2	Droit d'accès	57
2.11.3	Droit de rectification	59
2.11.4	Droit de suppression	60
2.11.5	Droit d'opposition	60
2.12	Partage de données et transfert international de données	61

CHAPITRE 3 : FONDEMENTS JURIDIQUES DU TRAITEMENT

DES DONNÉES PERSONNELLES.....63

3.1	Introduction	64
3.2	Consentement	65
3.2.1	Consentement univoque	66
3.2.2	Moment	66
3.2.3	Validité	66
3.2.4	Vulnérabilité	67
3.2.5	Enfants	68
3.2.6	Consentement éclairé	69
3.2.7	Consentement documenté	69
3.2.8	Refus ou retrait du consentement	69
3.3	Intérêt vital	70
3.4	Motifs importants d'intérêt public	71
3.5	Intérêt légitime	72
3.6	Exécution d'un contrat	74
3.7	Respect d'une obligation légale	74

CHAPITRE 4 : TRANSFERT INTERNATIONAL DE DONNÉES.....77

4.1	Introduction	78
4.2	Règles fondamentales applicables au transfert international de données	80
4.3	Fondement juridique applicable au transfert international de données	80
4.3.1	Introduction	80
4.3.2	Fondements juridiques du transfert international de données	81
4.4	Atténuation des risques pour l'individu	81
4.4.1	Garanties appropriées/clauses contractuelles	82
4.4.2	Responsabilité	84
4.5	Relation entre le responsable du traitement et le sous-traitant	85
4.6	Divulgaration des données personnelles aux autorités	85

CHAPITRE 5 : ANALYSES D'IMPACT RELATIVES À LA PROTECTION

DES DONNÉES.....89

5.1	Introduction	90
5.2	Déroulement de l'analyse d'impact relative à la protection des données	92
5.2.1	Une analyse d'impact relative à la protection des données est-elle nécessaire?	92

5.2.2	L'équipe chargée de l'analyse d'impact relative à la protection des données	92
5.2.3	Description du traitement des données personnelles	93
5.2.4	Consultation des parties prenantes	93
5.2.5	Identification des risques	94
5.2.6	Évaluation des risques	94
5.2.7	Choix des solutions	94
5.2.8	Recommandations.	94
5.2.9	Application des recommandations convenues	94
5.2.10	Contrôle ou audit de l'analyse d'impact relative à la protection des données par un expert	95
5.2.11	Actualisation de l'analyse d'impact relative à la protection des données en cas de modification du projet	95

2^e PARTIE – SITUATIONS ET TECHNOLOGIES SPÉCIFIQUES EN MATIÈRE DE TRAITEMENT

CHAPITRE 6 : ANALYSE DE DONNÉES ET BIG DATA 97

6.1	Introduction	98
6.2	Application des principes fondamentaux de la protection des données	104
6.2.1	Limitation de(s) la finalité(s) et traitement ultérieur	105
6.2.2	Fondements juridiques du traitement des données personnelles	106
6.2.3	Traitement équitable et licite	109
6.2.4	Minimisation des données	110
6.2.5	Sécurité des données	112
6.3	Droits des personnes concernées	112
6.4	Partage de données	113
6.5	Transfert international de données	114
6.6	Relation entre le responsable du traitement et le sous-traitant.	115
6.7	Analyses d'impact relatives à la protection des données	116

CHAPITRE 7 : DRONES/UAV ET TÉLÉDÉTECTION 119

7.1	Introduction	120
7.2	Application des principes fondamentaux de la protection des données	124
7.2.1	Fondements juridiques du traitement des données personnelles	124
7.2.2	Transparence/Information	127
7.2.3	Limitation de(s) la finalité(s) et traitement ultérieur	128
7.2.4	Minimisation des données	128
7.2.5	Conservation des données	129
7.2.6	Sécurité des données	129
7.3	Droits des personnes concernées	130
7.4	Partage de données	131
7.5	Transfert international de données	133
7.6	Relation entre le responsable du traitement et le sous-traitant.	133
7.7	Analyses d'impact relatives à la protection des données	134

CHAPITRE 8 : BIOMÉTRIE	137
8.1 Introduction	138
8.2 Application des principes fondamentaux de la protection des données	140
8.2.1 Fondements juridiques du traitement des données personnelles	142
8.2.2 Traitement équitable et licite	145
8.2.3 Limitation de(s) la finalité(s) et traitement ultérieur	146
8.2.4 Minimisation des données	147
8.2.5 Conservation des données	148
8.2.6 Sécurité des données	148
8.3 Droits des personnes concernées	149
8.4 Partage de données	149
8.5 Transfert international de données	150
8.6 Relation entre le responsable du traitement et le sous-traitant	150
8.7 Analyses d'impact relatives à la protection des données	151
CHAPITRE 9 : PROGRAMMES DE TRANSFERTS MONÉTAIRES	153
9.1 Introduction	154
9.2 Application des principes fondamentaux de la protection des données	158
9.3 Principes fondamentaux de la protection des données	160
9.3.1 Fondements juridiques du traitement des données personnelles	160
9.3.2 Limitation de(s) la finalité(s) et traitement ultérieur	162
9.3.3 Minimisation des données	164
9.3.4 Conservation des données	165
9.3.5 Sécurité des données	165
9.4 Droits des personnes concernées	166
9.5 Partage de données	167
9.6 Transfert international de données	168
9.7 Relation entre le responsable du traitement et le sous-traitant	169
9.8 Analyses d'impact relatives à la protection des données	169
CHAPITRE 10 : SERVICES CLOUD	173
10.1 Introduction	174
10.2 Responsabilité dans le cloud	176
10.3 Application des principes fondamentaux de la protection des données	177
10.3.1 Fondements juridiques du traitement des données personnelles	178
10.3.2 Traitement équitable et licite	179
10.3.3 Limitation de(s) la finalité(s) et traitement ultérieur	179
10.3.4 Transparence	180
10.3.5 Conservation des données	181
10.4 Sécurité des données	182
10.4.1 Protection des données en transit	186
10.4.2 Protection des actifs	186

10.4.2.1	Localisation physique	186
10.4.2.2	Sécurité des centres de données	186
10.4.2.3	Sécurité des données stockées (données au repos)	187
10.4.2.4	Purge des données	187
10.4.2.5	Élimination des équipements	187
10.4.2.6	Disponibilité	187
10.4.3	Ségrégation des utilisateurs	188
10.4.4	Gouvernance	188
10.4.5	Sécurité opérationnelle	188
10.4.6	Personnel	189
10.4.7	Développement	189
10.4.8	Chaîne d'approvisionnement	189
10.4.9	Gestion des utilisateurs	189
10.4.10	Identité et authentification	190
10.4.11	Interfaces externes	190
10.4.12	Administration des services	190
10.4.13	Audits	190
10.4.14	Utilisation des services	190
10.5	Droits des personnes concernées	191
10.6	Transfert international de données	191
10.7	Relation entre le responsable du traitement et le sous-traitant	191
10.8	Analyses d'impact relatives à la protection des données	192
10.9	Privilèges et immunités dans le cloud	192
10.9.1	Mesures juridiques	192
10.9.2	Mesures organisationnelles	193
10.9.3	Mesures techniques	193

CHAPITRE 11: APPLICATIONS MOBILES DE MESSAGERIE 195

11.1	Introduction	196
11.1.1	Les applications mobiles de messagerie dans l'aide humanitaire	198
11.2	Application des principes fondamentaux de la protection des données	200
11.2.1	Traitement des données personnelles via les applications mobiles de messagerie	200
11.2.1.1	Menaces potentielles	201
11.2.2	Quels types de données les applications mobiles de messagerie collectent-elles ou conservent-elles?	202
11.2.3	Comment d'autres parties peuvent-elles accéder à des données partagées sur des applications mobiles de messagerie?	205
11.2.4	Fonctionnalités des applications mobiles de messagerie liées au respect de la vie privée et à la sécurité	208
11.2.4.1	Anonymat autorisé/pas d'exigence d'authentification de l'identité	208
11.2.4.2	Pas de conservation du contenu des messages	208
11.2.4.3	Chiffrement de bout en bout	208
11.2.4.4	Propriété des données	208

11.2.4.5	Non-conservation ou conservation minimale des métadonnées	209
11.2.4.6	Code de l'application mobile de messagerie en open source ..	209
11.2.4.7	L'entreprise examine soigneusement les demandes de divulgation émanant des forces de l'ordre	209
11.2.4.8	Partage limité de données personnelles avec des tiers	210
11.2.4.9	Restriction de l'accès via le système d'exploitation, le logiciel ou les correctifs de sécurité spécifiques de l'appareil	210
11.2.5	Traitement de données personnelles recueillies par des applications mobiles de messagerie	210
11.3	Fondements juridiques du traitement des données personnelles ..	211
11.4	Conservation des données	212
11.5	Droits de rectification et de suppression	213
11.6	Minimisation des données	213
11.7	Limitation de(s) la finalité(s) et traitement ultérieur	214
11.8	Gestion, analyse et vérification des données	215
11.9	Protection des données dès la conception	216
11.10	Transfert international de données	217

CHAPITRE 12 : IDENTITÉ NUMÉRIQUE 219

12.1	Introduction	220
12.1.1	Authentification, identification et vérification : qui êtes-vous et comment pouvez-vous le prouver?	222
12.1.2	Identité numérique	223
12.1.3	Conception et gouvernance du système	224
12.1.4	Identité numérique dans le secteur humanitaire : scénarios possibles	226
12.1.5	Identité numérique en tant qu'identité fondamentale	227
12.2	Analyses d'impact relatives à la protection des données	229
12.3	Protection des données dès la conception et par défaut	230
12.4	Relation entre le responsable du traitement et le sous-traitant. ...	231
12.5	Droits des personnes concernées	231
12.5.1	Droit d'accès	232
12.5.2	Droits de rectification et de suppression	233
12.6	Application des principes fondamentaux de la protection des données	234
12.6.1	Fondements juridiques du traitement des données personnelles	234
12.6.2	Limitation de(s) la finalité(s) et traitement ultérieur	234
12.6.3	Proportionnalité	235
12.6.4	Minimisation des données	236
12.6.5	Sécurité des données	236
12.6.6	Conservation de données	237
12.7	Transfert international de données	237

CHAPITRE 13 : MÉDIAS SOCIAUX 239

13.1	Introduction	240
13.1.1	Médias sociaux dans le secteur humanitaire	240

13.1.2	Médias sociaux et données	242
13.1.2.1	Quelles données sont générées sur les médias sociaux et de quelle manière ?	242
13.1.2.2	Quelles sont les données susceptibles d'être partagées avec des tiers ?	244
13.1.2.3	Quelles données les organismes chargés de l'application des lois et les autorités publiques peuvent-ils obtenir ?	246
13.2	Analyses d'impact relatives à la protection des données	247
13.3	Considérations éthiques et autres défis	249
13.4	Relation entre le responsable du traitement et le sous-traitant	250
13.5	Principes fondamentaux de la protection des données	252
13.5.1	Fondements juridiques du traitement de données personnelles	252
13.5.2	Information	252
13.5.3	Conservation des données	254
13.5.4	Sécurité des données	255
13.6	Transfert international de données	255

CHAPITRE 14 : BLOCKCHAIN 257

14.1	Introduction	258
14.1.1	Qu'est-ce qu'une blockchain ?	258
14.1.2	Types de blockchain	261
14.1.3	La blockchain en pratique	263
14.1.4	Utilisations dans le secteur humanitaire	264
14.2	Analyses d'impact relatives à la protection des données	267
14.3	Protection des données dès la conception et par défaut	268
14.4	Relation entre le responsable du traitement et le sous-traitant	270
14.5	Principes fondamentaux de la protection des données	272
14.5.1	Minimisation des données	272
14.5.2	Conservation de données	273
14.5.3	Proportionnalité	273
14.5.4	Sécurité des données	273
14.6	Droits des personnes concernées	275
14.6.1	Droit d'accès	275
14.6.2	Droit de rectification	275
14.6.3	Droit de suppression	276
14.6.4	Restrictions des droits des personnes concernées	277
14.7	Transfert international de données	278
	Pièces jointes : Cadre décisionnel pour l'utilisation de la blockchain dans l'action humanitaire	279

CHAPITRE 15 : CONNECTIVITÉ COMME FORME D'AIDE 283

15.1	Introduction	284
15.1.1	Présentation de la connectivité comme offre d'assistance	285
15.1.2	Contexte opérationnel	286
15.1.3	Multiples parties prenantes et partenariats	286
15.2	Analyses d'impact relatives à la protection des données	289
15.3	Relation entre le responsable du traitement et le sous-traitant	290

15.4	Principes fondamentaux de la protection des données	291
15.4.1	Fondements juridiques du traitement des données personnelles	291
15.4.2	Sécurité des données	292
15.4.3	Conservation de données	293
15.4.4	Informations	294
15.5	Transfert international de données	294

CHAPITRE 16 : INTELLIGENCE ARTIFICIELLE ET APPRENTISSAGE

AUTOMATIQUE 297

16.1	Introduction	298
16.1.1	Que sont l'intelligence artificielle et l'apprentissage automatique?	298
16.1.2	Comment fonctionnent l'intelligence artificielle et l'apprentissage automatique?	299
16.1.3	Intelligence artificielle dans le secteur humanitaire	301
16.1.4	Défis et risques liés à l'utilisation de l'intelligence artificielle	303
16.2	Analyse d'impact relative à la protection des données	304
16.3	Application des principes fondamentaux de la protection des données	305
16.3.1	Limitation de la finalité et traitement ultérieur	305
16.3.2	Traitement équitable et licite	306
16.3.2.1	Licéité	306
16.3.2.2	Loyauté et biais	308
16.3.2.3	Transparence	310
16.3.3	Minimisation des données	311
16.3.4	Conservation des données	312
16.3.5	Sécurité des données	313
16.4	Droits des personnes concernées	314
16.4.1	Droit à l'information	314
16.4.2	Droit de suppression	315
16.4.3	Droits relatifs à la prise de décisions automatisée	315
16.5	Relation entre le responsable du traitement et le sous-traitant	317
16.5.1	Respect des obligations	317
16.5.2	Responsabilité	317
16.6	Transfert international de données	318
16.7	Protection des données dès la conception et par défaut	318
16.8	Problèmes et considérations éthiques	320

ANNEXE I: MODÈLE DE RAPPORT D'AIPD 325

ANNEXE II: PARTICIPANTS AUX ATELIERS 331

REMERCIEMENTS

Le présent manuel est une publication conjointe du Brussels Privacy Hub, un centre de recherche de l'Université libre de Bruxelles (Vrije Universiteit Brussel, VUB), en Belgique, et du Bureau de la Protection des données du Comité international de la Croix-Rouge (CICR), à Genève (Suisse), par Christopher Kuner (VUB) et Massimo Marelli (CICR).

Conseil consultatif:

- Christopher Kuner, Júlia Zomignani Barboza et Lina Jasmontaite (VUB);
- Massimo Marelli, Vincent Graf Narbel, Sarah Dwidar, Luca Bettoni, Pierre Apraxine et Romain Bircher (CICR);
- Catherine Lennman, Préposé fédéral à la protection des données et à la transparence (Suisse);
- Claire-Agnes Marnier, Olivier Matter et Petra Candellier, Contrôleur européen de la protection des données;
- Alexander Beck, Haut Commissariat des Nations Unies pour les réfugiés (HCR);
- Christina Vasala Kokkinaki, Organisation internationale pour les migrations (OIM);
- Lucie Laplante et James De France, Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge;
- Stuart Campo, Bureau de la coordination des affaires humanitaires des Nations Unies (OCHA);
- Nathaniel Raymond, Yale University;
- Alexandrine Pirlot de Corbion, Ed Geraghty et Gus Hosein, Privacy International;
- Marine Revel, Association francophone des autorités de protection des données personnelles;
- Carmela Troncoso, École polytechnique fédérale de Lausanne;
- Mary Nunn, Médecins Sans Frontières;
- Awa Ndiaye et Anna Thiam, Commission de protection des données personnelles (Sénégal).

Les auteurs remercient ICT Legal Consulting, qui leur a donné l'autorisation d'utiliser les documents sur la sécurité dans le cloud (<https://www.ictlegalconsulting.com/?lang=en>), et Trilateral Research (<http://trilateralresearch.com/>), qui les a autorisés à utiliser les documents sur les analyses d'impact relatives à la protection des données.

Lorsqu'un chapitre du manuel fait appel à d'autres contributions, celles-ci sont mentionnées en note de bas de page dans le chapitre concerné.

AVANT-PROPOS

Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l'Europe et membre de la Commission de protection des données, organe de contrôle indépendant du CICR

Je suis heureux de présenter le *Manuel sur la protection des données dans l'action humanitaire*, issu d'une collaboration très fructueuse entre le Comité international de la Croix-Rouge (CICR) et le Brussels Privacy Hub (BPH).

La protection des données personnelles revêt une importance fondamentale pour les organisations humanitaires car elle fait partie intégrante de la protection de la vie, de l'intégrité et de la dignité des bénéficiaires.

En 2015, la 37^e Conférence internationale des commissaires à la protection des données et à la vie privée a adopté la Résolution sur la protection des données personnelles et l'action humanitaire internationale, qui visait notamment à répondre à la demande de coopération des acteurs humanitaires afin d'établir des lignes directrices sur la protection des données. Un groupe de travail a été constitué et a participé au projet sur la protection des données dans l'action humanitaire géré conjointement par le BPH et le CICR, dont l'objectif était d'étudier les liens entre les lois relatives à la protection des données et l'action humanitaire afin d'appréhender l'impact des nouvelles technologies sur la protection des données dans le secteur humanitaire et d'établir des lignes directrices appropriées.

Ce projet a réuni des organisations humanitaires, des autorités chargées de la protection des données et des spécialistes des technologies dans le cadre d'une série d'ateliers couvrant tout un ensemble de questions, telles l'analyse des données, les drones, la biométrie, les programmes de transferts monétaires, les services de cloud computing et les applications mobiles de messagerie, qui revêtent tous une importance croissante dans le secteur humanitaire.

Ce manuel est un des produits de ce projet; il sera utile pour sensibiliser les organisations humanitaires à la protection des données personnelles et les aider à respecter les normes en la matière. Il répond aussi à la nécessité de disposer de lignes directrices précises pour l'interprétation des principes de protection des données applicables à l'action humanitaire, en particulier lorsque de nouvelles technologies sont en jeu. Je suis convaincu qu'il se révélera tout aussi précieux aux acteurs humanitaires qu'aux autorités chargées de la protection des données et aux entreprises privées. Il montre clairement que la législation en matière de protection des données n'interdit pas de recueillir et de partager des données personnelles,

mais qu'elle instaure en fait un cadre dans lequel les données personnelles peuvent être utilisées en toute confiance, sachant que le droit des individus à la protection de la vie privée est respecté.

Jean-Philippe Walter est l'ancien préposé fédéral suppléant à la protection des données et à la transparence au sein de l'autorité suisse de protection des données. Il préside l'Association francophone des autorités de protection des données personnelles et il est le coordinateur du groupe de travail sur la Résolution sur la protection des données personnelles et l'action humanitaire internationale adoptée par la Conférence internationale des commissaires à la protection des données et à la vie privée (désormais nommée Global Privacy Assembly).

GLOSSAIRE DES TERMES ET ABRÉVIATIONS

Action humanitaire: toute activité entreprise sur une base impartiale en vue d'exécuter des opérations d'assistance, de secours et de protection dans une situation d'urgence humanitaire. Elle peut comprendre l'assistance humanitaire, l'aide humanitaire et la protection.

Analyse de données (data analytics): pratique consistant à combiner de très grands volumes d'informations provenant de sources diverses (big data) et à les analyser au moyen d'algorithmes complexes pour éclairer les décisions.

Analyse d'impact relative à la protection des données ou AIPD: analyse consistant à détecter, évaluer et gérer les risques qui découlent d'un projet, d'une politique, d'un programme ou d'une autre initiative ayant pour finalité le traitement de données personnelles.

Anonymisation: opération faisant appel à des techniques garantissant que les ensembles de données contenant des données personnelles sont rendus totalement et irréversiblement anonymes, de sorte qu'il est impossible de les rattacher à une personne physique identifiée ou identifiable ou que la personne concernée n'est plus identifiable.

Apprentissage automatique: forme spécifique d'intelligence artificielle pouvant être définie comme l'étude d'algorithmes qui améliorent les performances lors de l'exécution d'une tâche spécifique, sous forme de données lisibles par machine.

Biométrie ou reconnaissance biométrique: reconnaissance automatique des personnes sur la base de leurs caractéristiques biologiques et comportementales.

Blockchain: « par nature, base de données décentralisée en ajout seulement qui est gérée par un algorithme de consensus et stockée sur plusieurs nœuds (informatiques)¹ ».

BPD: bureau de la protection des données d'une organisation humanitaire.

Consentement: manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée donne son accord au traitement de données personnelles qui la concernent.

Contrat de niveau de service: contrat entre un prestataire de services et un client par lequel le premier s'engage notamment sur la fiabilité des services Internet et de télécommunications à fournir.

¹ M. Finck, « Blockchains and Data Protection in the European Union », *European Data Protection Law Review*, vol. 4, n° 1, 2018, p. 17 : <https://doi.org/10.21552/edpl/2018/1/6>.

Donnée personnelle: toute information relative à une personne physique identifiée ou identifiable.

Données relatives à la santé ou données de santé: données personnelles sur la santé physique ou mentale d'un individu qui donnent des informations sur son état de santé.

Donnée sensible: donnée personnelle qui, si elle est divulguée, peut entraîner une discrimination ou une répression à l'encontre de la personne physique concernée. En général, sont considérées comme sensibles les données relatives à l'état de santé, à la race ou à l'origine ethnique, ou bien aux affiliations religieuses ou politiques, ou à des groupes armés, ou encore les données génétiques ou biométriques. Toutes les données sensibles requièrent une protection renforcée même si les différents types de données qui entrent dans cette catégorie (par exemple, différents types de données biométriques) n'ont pas nécessairement le même niveau de sensibilité. Étant donné les situations particulières dans lesquelles les organisations humanitaires sont appelées à travailler et la possibilité que certaines données puissent engendrer des discriminations, on ne peut espérer établir une liste définitive des données sensibles dans l'action humanitaire. La sensibilité des données et les garanties appropriées (mesures de sécurité techniques et organisationnelles, par exemple) doivent être considérées au cas par cas.

Drone: petit engin aérien ou non, fonctionnant de manière autonome ou piloté à distance. On les appelle aussi UAV (de l'anglais *Unmanned Aerial Vehicles*), véhicules aériens sans pilote, aérodynes sans équipage, télépilotes ou programmés.

DS: Directeur de la sécurité.

DSI: Directeur de la sécurité informatique.

DT: Directeur technique.

EIISI: Équipe d'intervention en cas d'incident de sécurité informatique.

EIIU: Équipe d'intervention informatique d'urgence.

IaaS (Infrastructure as a Service): infrastructure en tant que service.

Identification des clients (Know Your Customer, KYC): procédure permettant aux entreprises de contrôler l'identité de leurs clients afin de respecter la réglementation et la législation sur le blanchiment d'argent et la corruption².

Identité numérique: désigne « un ensemble d'attributs d'identité collectés et stockés sous forme électronique qui décrit de manière unique une personne dans un contexte donné et qui est utilisé lors de transactions électroniques³ ».

² PwC, *Know Your Customer: Quick Reference Guide* : <http://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html>.

³ GSMA, Groupe de la Banque mondiale et Secure Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, 2016, p. 11 : <https://www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation/>.

Intelligence artificielle: «ensemble de sciences, théories et techniques dont le but est de reproduire par une machine des capacités cognitives d'un être humain⁴». Dans sa forme actuelle, son objectif est de permettre aux concepteurs de technologies de «confier à une machine des tâches complexes auparavant déléguées à un humain⁵».

Organisation humanitaire: organisation qui apporte de l'aide afin d'alléger les souffrances humaines ou qui protège la vie et la santé et respecte la dignité humaine dans une situation d'urgence humanitaire, conformément à son mandat ou à sa mission.

Organisation internationale: organisation et ses entités subordonnées régies par le droit international public, ou tout autre organe créé au moyen ou sur la base d'un accord entre deux pays ou plus.

PaaS (*Platform as a Service*): plateforme en tant que service

Personne concernée: personne physique (c'est-à-dire un individu) susceptible d'être identifiée, directement ou indirectement, notamment par référence à des données personnelles.

Personne portée disparue: personne dont on est sans nouvelles et pour laquelle une opération de recherche a été lancée.

Programmes de transferts monétaires: aide sous forme de bons et d'espèces, interventions monétaires et aide en espèces. Il s'agit de termes du secteur humanitaire qui désignent une aide humanitaire apportée sous forme de bons ou d'espèces.

Pseudonymisation: traitement de données personnelles différent de l'anonymisation, à l'issue duquel les données ne peuvent plus être attribuées à une personne précise sans informations complémentaires, sous réserve que ces informations complémentaires soient conservées à part et fassent l'objet de mesures techniques et organisationnelles garantissant que les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable.

Responsable du traitement: personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles.

SaaS (*Software as a Service*): logiciel en tant que service.

Services cloud: désignent le plus souvent «un modèle permettant d'accéder partout, aisément et à la demande, par le réseau, à des ressources informatiques configurables mutualisées (réseaux, serveurs, stockage, applications et services par exemple) qui peuvent être rapidement mobilisées et libérées avec un minimum d'effort de gestion ou d'intervention d'un prestataire de services⁶».

4 Conseil de l'Europe (CdE), Glossaire, entrée Intelligence artificielle : <https://www.coe.int/fr/web/artificial-intelligence/glossary>.

5 Ibid.

6 US NIST SP 800-145, *The NIST Definition of Cloud Computing*, septembre 2011 : <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

Sous-traitant : personne physique ou morale qui traite des données personnelles pour le compte du responsable du traitement.

Sous-traitant ultérieur : personne physique ou morale chargée par un sous-traitant de traiter des données personnelles pour son compte.

Tiers : personne physique ou morale, autorité publique, service public ou organisme autre que la personne concernée, le responsable du traitement et le sous-traitant.

TLS (Transport Layer Security) : protocole cryptographique garantissant le respect de la vie privée et l'intégrité des données entre un client et un serveur via une connexion Internet.

Traitement : opération ou ensemble d'opérations portant sur des données personnelles ou des ensembles de données personnelles effectuées ou non à l'aide de procédés automatisés, comme la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, l'alignement, la combinaison ou la suppression.

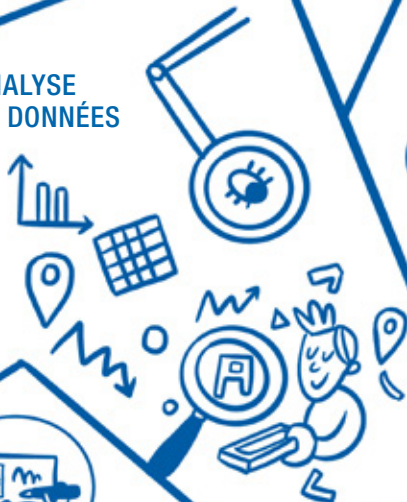
Traitement ultérieur : traitement des données personnelles allant au-delà des finalités initialement spécifiées au moment de la collecte des données.

Transfert international de données : tout acte consistant à transférer ou à rendre accessible des données personnelles hors du pays ou de l'organisation internationale au sein desquels elles ont été initialement recueillies ou traitées, y compris à une autre entité de la même organisation humanitaire ou à un tiers, par voie électronique, par Internet ou par d'autres moyens.

Urgence humanitaire : événement ou série d'événements (résultant notamment de conflits armés ou de catastrophes naturelles) constituant une menace critique pour la santé, la sécurité ou le bien-être d'une communauté ou d'un autre groupe important de personnes, habituellement sur une zone étendue.

Violation des données : modification non autorisée, copie, destruction illicite, perte accidentelle, divulgation abusive, transfert indu ou altération des données personnelles.

ANALYSE
DE DONNÉES



SERVICES CLOUD

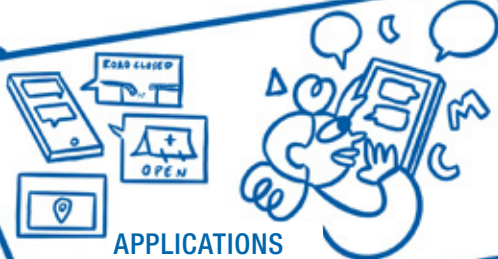


PROGRAMMES
DE TRANSFERTS
MONÉTAIRES

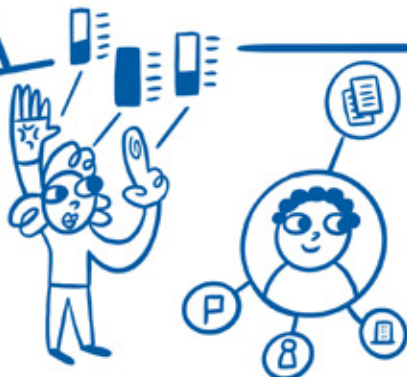
IDENTITÉ
NUMÉRIQUE



APPLICATIONS
MOBILES
DE MESSAGERIE



BIOMÉTRIE

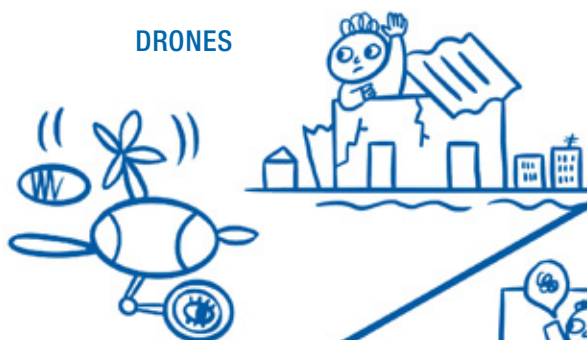


CICR



BRUSSELS
PRIVACY
HUB

DRONES



CONNECTIVITÉ
COMME FORME
D'AIDE

MÉDIAS SOCIAUX



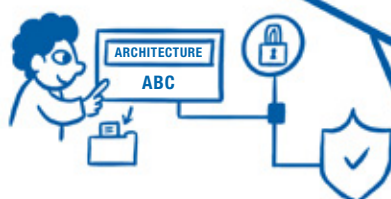
TROUVÉ !



FOURNITURES
DU CICR
DISPONIBLES



BLOCKCHAIN



INTELLIGENCE
ARTIFICIELLE

CHAPITRE 1

INTRODUCTION

1.1 CONTEXTE

La protection des données personnelles des individus fait partie intégrante de la protection de leur vie, de leur intégrité et de leur dignité. C'est pourquoi elle revêt une importance fondamentale pour les organisations humanitaires.

Les suggestions données dans ce manuel quant aux modalités d'application des principes de protection des données par les organisations humanitaires s'appuient sur des lignes directrices, des procédures de travail et des pratiques qui ont été établies dans le domaine de l'action humanitaire dans les environnements les plus instables et dans l'intérêt des victimes les plus vulnérables de conflits armés, d'autres situations de violence, de catastrophes naturelles, de pandémies et d'autres urgences humanitaires (ensemble les « urgences humanitaires »). Une partie de ces lignes directrices, de ces procédures et de ces pratiques est antérieure à l'émergence et au développement des législations sur la protection des données, mais toutes reposent sur le principe de la dignité humaine et sur la notion de protection qui sous-tendent le droit de la protection des données. Ces lignes directrices ont été notamment exposées dans l'ouvrage intitulé *Standards professionnels pour les activités de protection*⁷.



K. Ashawi/Reuters

Un homme en vélomoteur longe des bâtiments détruits par la guerre à Al-Bab (Syrie), mars 2017.

⁷ CICR, *Standards professionnels pour les activités de protection menées par les organisations humanitaires et de défense des droits de l'homme lors de conflits armés et d'autres situations de violence*, 3^e éd., Genève, 2018 : <https://www.icrc.org/fr/publication/0999-standards-professionnels-pour-les-activites-de-protection-menees-par-les>. Toutes les références Internet ont été consultées en mars 2020.

Depuis quelques années, le développement de nouvelles technologies facilitant et accélérant le traitement de volumes croissants de données personnelles dans un monde interconnecté suscite des préoccupations quant à de possibles intrusions dans la sphère privée des individus. Partout dans le monde, des efforts de réglementation ont été entrepris pour y répondre.

Ce manuel est publié dans le cadre du projet sur la protection des données dans l'action humanitaire, qui a été mis sur pied conjointement par le Brussels Privacy Hub – un centre de recherche de l'Université libre de Bruxelles (VUB), en Belgique – et le Bureau de la protection des données du CICR, à Genève (Suisse). Son contenu a été élaboré dans le cadre d'une série d'ateliers organisés en 2015 et 2016 à Bruxelles et à Genève avec des représentants d'organisations humanitaires (y compris des praticiens de l'action humanitaire), des autorités de protection des données, des universitaires, des organisations non gouvernementales (ONG), des chercheurs et d'autres spécialistes, qui se sont réunis pour examiner des questions d'intérêt commun concernant la protection des données dans l'action humanitaire, en particulier dans le contexte des nouvelles technologies. La liste des participants à ces ateliers figure à l'annexe II.

1.2 OBJECTIF

Ce manuel se propose d'approfondir les discussions amorcées au titre de la Résolution sur la protection des données personnelles et l'action humanitaire internationale, adoptée par la Conférence internationale des commissaires à la protection des données et à la vie privée (ICDPPC)⁸ en 2015, à Amsterdam. Il n'a pas vocation à se substituer aux normes légales applicables ni aux règles, politiques et procédures en matière de protection des données qu'une organisation peut avoir adoptées, mais plutôt à sensibiliser les organisations humanitaires aux normes de protection des données personnelles et à les aider à veiller à leur respect dans le cadre de leurs activités humanitaires, en donnant des indications précises sur l'interprétation des principes de protection des données dans le contexte de l'action humanitaire, en particulier lorsque de nouvelles technologies sont en jeu.

Ce manuel est conçu pour faciliter l'intégration des principes et droits relatifs à la protection des données dans les situations d'urgence humanitaire. Cependant, il ne remplace pas la législation nationale sur la protection des données applicable à une organisation humanitaire qui ne bénéficie pas des privilèges et immunités généralement accordés à une organisation internationale et ne donne pas de conseils sur son application.

⁸ ICDPPC, Résolution sur la protection des données personnelles et l'action humanitaire internationale, Amsterdam (Pays-Bas), 2015 : https://www.cai.gouv.qc.ca/documents/R%C3%A9solution-sur-la-protection-des-donn%C3%A9es-personnelles-et-l'action-humanitaire-internationale_fr.pdf.

Le respect des normes en matière de protection des données personnelles n'en suppose pas moins la prise en compte de la portée et de la finalité spécifiques des activités humanitaires, qui consistent à pourvoir aux besoins élémentaires et urgents d'individus vulnérables. La protection des données et l'action humanitaire doivent être envisagées comme des champs compatibles et complémentaires qui se confortent mutuellement. La protection des données ne doit donc pas être considérée comme une entrave au travail des organisations humanitaires ; tout au contraire, elle doit être au service de leur action. De même, il ne faut jamais interpréter les principes de protection des données de manière à ce qu'ils fassent obstacle à des activités humanitaires essentielles, mais toujours de manière à ce qu'ils servent l'objectif ultime de l'action humanitaire, à savoir préserver la vie, l'intégrité et la dignité des victimes d'urgences humanitaires.

Les recommandations et lignes directrices présentées dans ce manuel se fondent sur certains des instruments internationaux les plus importants en matière de protection des données, notamment :

- la Résolution de l'Assemblée générale des Nations Unies 45/95 du 14 décembre 1990⁹ portant adoption des Principes directeurs pour la réglementation des fichiers personnels informatisés¹⁰, dans laquelle figure la clause humanitaire appelant à exercer une attention particulière et à faire preuve de flexibilité dans l'application des principes de protection des données dans le secteur humanitaire ;
- les Principes des Nations Unies en matière de protection des données personnelles et de la vie privée (en anglais), adoptés par le Comité de haut niveau sur la gestion (HLCM) lors de sa 36^e séance le 11 octobre 2018¹¹ ;
- les Normes internationales pour la protection de la vie privée et des données à caractère personnel (Résolution de Madrid) (en anglais) adoptées par l'ICDPPC à Madrid en 2009¹² ;
- le Cadre de l'OCDE pour la protection de la vie privée (en anglais) (2013)¹³ ;
- la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)¹⁴

9 Résolution de l'Assemblée générale des Nations Unies 45/95 du 14 décembre 1990, A/RES/45/95.

10 Assemblée générale des Nations Unies, Guidelines for the Regulation of Computerized Personal Data Files : <http://www.refworld.org/docid/3ddcafaac.html>.

11 HLCM, Personal Data Protection and Privacy Principles, 18 décembre 2018 : https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf.

12 ICDPPC, International Standards on the Protection of Personal Data and Privacy : http://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf?mc_phishing_protection_id=28047-br1tehqu81eaoar3q10.

13 The OECD Privacy Framework : <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

14 CdE, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ouverte à la signature le 28 janvier 1981, entrée en vigueur le 1^{er} octobre 1985, STE n° 108 : <https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108>.

et son Protocole STCE n° 223 d'amendement à la Convention (désormais dénommée Convention 108+)¹⁵.

D'autres normes importantes ont également été prises en compte, notamment :

- les évolutions réglementaires récentes, dans la mesure où elles reflètent de nouvelles évolutions des notions et des principes de protection des données intervenues à la lumière de leur application au fil des ans et des difficultés engendrées par les nouvelles technologies (dont la mise à jour de la Convention 108, ainsi que le Règlement général européen sur la protection des données 2016/679 [RGPD])¹⁶ ;
- la Résolution sur la protection des données et les catastrophes naturelles majeures¹⁷ adoptée par l'ICDPPC à Mexico en 2011 (en anglais) ;
- la Résolution sur la protection de la vie privée et l'action humanitaire internationale adoptée par l'ICDPPC à Amsterdam en 2015¹⁸ ;
- les *Règles du CICR en matière de protection des données personnelles* (2015)¹⁹ ;
- les *Standards professionnels pour les activités de protection du CICR* (2018)²⁰ ;
- la *Politique relative à la protection des données des personnes relevant de la compétence du HCR* (2015)²¹ ;
- le *Manuel de l'OIM sur la protection des données* (en anglais) (2010)²².

15 CdE, Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ouvert à la signature le 10 octobre 2018, STCE n° 223 : <https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/09000016808ac919>.

16 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), [2016] JO L119/1 : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR>.

17 ICDPPC, Resolution on Data Protection and Major Natural Disasters : http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-Major-Natural-Disasters.pdf?mc_phishing_protection_id=28047-br1tehqud81eaoar3q10.

18 ICDPPC, Résolution sur la protection des données personnelles et l'action humanitaire internationale, Amsterdam (Pays-Bas), 2015 : https://www.cai.gouv.qc.ca/documents/R%C3%A9solution-sur-la-protection-des-donn%C3%A9es-personnelles-et-l'action-humanitaire-internationale_fr.pdf.

19 CICR, *Règles du CICR en matière de protection des données personnelles* : <https://www.icrc.org/fr/publication/4261-icrc-rules-on-personal-data-protection?language=fr>.

20 CICR, *Standards professionnels pour les activités de protection menées par les organisations humanitaires et de défense des droits de l'homme lors de conflits armés et d'autres situations de violence*, 3^e éd., Genève, 2018 : <https://www.icrc.org/fr/publication/0999-standards-professionnels-pour-les-activites-de-protection-menees-par-les>.

21 HCR, *Politique relative à la protection des données des personnes relevant de la compétence du HCR* (mai 2015) : <https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=5bf7c99c4>.

22 OIM, *IOM Data Protection Manual* (2010) : <https://publications.iom.int/books/iom-data-protection-manual>.

Ce manuel recommande des normes minimales pour le traitement des données personnelles. Les organisations humanitaires peuvent prévoir des exigences plus fortes en matière de protection des données si elles le jugent opportun ou si elles sont soumises à des lois plus strictes à l'échelle nationale ou régionale.

Il convient d'emblée de souligner quelques considérations :

- Alors que le droit à la protection de la vie privée est un droit humain reconnu depuis longtemps à l'échelle mondiale²³, le droit à la protection des données personnelles est un droit relativement récent, étroitement lié au droit au respect de la vie privée, qui établit les conditions applicables au traitement de données concernant une personne physique identifiée ou identifiable. Plus de 100 lois et normes propres à la protection des données ont été adoptées ces dernières années à l'échelle nationale et régionale²⁴, et le droit fondamental à la protection des données est de plus en plus largement reconnu dans le monde. En conséquence, l'instauration de règles de protection des données personnelles doit être une priorité pour toutes les organisations humanitaires, même lorsque ce n'est pas une obligation légale au regard des privilèges et immunités dont bénéficient certaines d'entre elles, puisque le principal objectif de leurs activités est d'œuvrer à la sécurité et à la dignité des personnes physiques.
- Certaines organisations humanitaires sont des organisations internationales qui bénéficient de privilèges et d'immunités et ne sont pas soumises à la législation nationale. Néanmoins, le respect de la vie privée et des règles de protection des données est, dans bien des cas, une condition préalable pour qu'elles puissent recevoir des données personnelles émanant d'autres entités.
- Les situations d'urgence exceptionnelle dans lesquelles interviennent les organisations humanitaires engendrent des problématiques particulières quant à la protection des données. Il faut donc être particulièrement attentif et flexible dans l'application des principes de protection des données dans le secteur humanitaire. Cette nécessité se reflète également dans de nombreux instruments et normes internationaux cités plus haut, qui prévoient des règles plus strictes pour le traitement des données sensibles²⁵.
- L'absence d'approche uniforme dans le droit de la protection des données à l'égard des données personnelles des personnes décédées implique que les organisations humanitaires doivent adopter leurs propres politiques en la matière (par exemple, en appliquant dans le cas de personnes décédées les règles applicables aux données personnelles des personnes physiques, dans la mesure où cela s'avère opportun). Pour les organisations qui ne bénéficient pas de l'immunité de juridiction, cette question peut être régie par le droit applicable.

²³ Voir article 12 de la Déclaration universelle des droits de l'homme et article 17 du Pacte international relatif aux droits civils et politiques.

²⁴ Voir Conférence des Nations Unies sur le commerce et le développement (CNUCED), *Data Protection regulations and international data flows: Implications for trade and development* (2016) : <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468>.

²⁵ Voir [section 2.2: Notions élémentaires de la protection des données](#).

- Ce manuel est consacré à la protection des données personnelles et à l'application de ce domaine du droit à l'action humanitaire. Cependant, dans les conflits armés et autres situations de violence, de nombreuses menaces sont plus collectives qu'individuelles – un village, une communauté, un groupe particulier d'hommes et de femmes peuvent être exposés aux mêmes menaces ; une bonne gestion des données personnelles peut alors se révéler insuffisante. Dans certains cas, le traitement de données non personnelles peut engendrer des menaces spécifiques au niveau collectif. À cet égard, plusieurs initiatives prises dans le secteur humanitaire se sont intéressées aux implications du traitement des données pour les communautés plus généralement et font référence, par exemple, aux informations démographiques identifiables²⁶ ou aux informations communautaires identifiables²⁷.
- Dans les situations d'urgence humanitaire, les organisations humanitaires traitent les données personnelles de différentes catégories de personnes physiques, comme les bénéficiaires et les intervenants impliqués dans leurs activités, ainsi que le personnel et les fournisseurs de biens et services, ou même les donateurs. Bien que ce manuel soit plus particulièrement consacré au traitement des données personnelles des bénéficiaires, des considérations analogues s'appliquent à la gestion des données personnelles d'autres catégories de personnes.

1.3 STRUCTURE ET APPROCHE

La première partie de ce manuel s'applique à tous les types de traitement de données personnelles. La deuxième partie aborde plus particulièrement certaines technologies et situations de traitement des données, et analyse plus précisément les questions qui se posent dans ces contextes en matière de protection des données. Les scénarios de traitement décrits dans la deuxième partie doivent toujours être lus en gardant la première partie à l'esprit. Les définitions des termes employés tout au long du manuel se trouvent dans le glossaire figurant au début de l'ouvrage.

1.4 À QUI S'ADRESSE CE MANUEL ?

Ce manuel s'adresse au personnel des organisations humanitaires intervenant dans le traitement de données personnelles dans le cadre des opérations humanitaires menées par leur organisation, en particulier aux personnes chargées d'appliquer les règles de protection des données et de fournir des conseils en la matière. Il peut également s'avérer utile aux autres parties engagées dans l'action humanitaire ou la protection des données, comme les autorités de protection des données, les entreprises privées ou d'autres acteurs concernés par ces activités.

²⁶ Voir *The Signal Code – A Human Rights Approach to Information During Crisis* : <https://signalcode.org/>.

²⁷ Voir Humanitarian Data Exchange Initiative : <https://data.humdata.org/faq>.

CHAPITRE 2

PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

2.1 INTRODUCTION

Les organisations humanitaires recueillent et traitent les données personnelles d'individus affectés par des urgences humanitaires dans le but de mener des activités humanitaires. Travaillant principalement dans le cadre d'urgences humanitaires, elles interviennent dans des situations où l'état de droit n'est pas toujours pleinement respecté. Dans ces situations, l'accès à la justice et le respect du cadre international des droits humains peuvent être limités, voire inexistants. En outre, la législation en matière de protection des données personnelles peut être embryonnaire ou inexistante, ou ne pas être entièrement applicable.

Le droit d'une personne à la protection de ses données personnelles n'est pas un droit absolu ; il doit être considéré au regard de l'objectif général de protection de la dignité humaine, et mis en balance avec d'autres libertés et droits fondamentaux, conformément au principe de proportionnalité²⁸.

Étant donné que les organisations humanitaires exercent leurs activités principalement lors d'urgences humanitaires, elles œuvrent dans des situations où il est souvent nécessaire de protéger les données personnelles des bénéficiaires et de



Walungu, province du Sud-Kivu (République démocratique du Congo). Le CICR fournit de la nourriture à 1 750 familles déplacées et résidentes, décembre 2016.

28 Le principe de proportionnalité dans ce contexte ne doit pas être confondu avec le principe de proportionnalité en droit international humanitaire. Le principe de proportionnalité envisagé ici exige que les organisations humanitaires prennent les mesures les moins intrusives possible lorsqu'elles limitent le droit à la protection des données et le droit d'accès aux données personnelles pour accomplir leur mandat et intervenir dans des situations d'urgence.

leur personnel afin de préserver leur sécurité, leur vie et leur travail. La protection des données personnelles et l'action humanitaire sont donc complémentaires et se confortent mutuellement. Cependant, il peut aussi arriver qu'il faille trouver un compromis entre différents droits et libertés (par exemple entre la liberté d'expression et d'information et le droit à la protection des données, ou entre le droit à la liberté et à la sécurité d'une personne et le droit à la protection des données). Le cadre des droits humains vise à garantir le respect de l'ensemble de ces droits et des libertés fondamentales en mettant en balance, au cas par cas, les différents droits et libertés. Cette approche requiert souvent une interprétation téléologique des droits²⁹, c'est-à-dire une interprétation qui donne la priorité à leurs finalités.

EXEMPLE :

Le droit de la protection des données exige que des informations de base soient fournies aux personnes concernant le traitement de leurs données personnelles. Cependant, dans une situation d'urgence humanitaire, ce droit doit être mis en balance avec d'autres droits, en particulier les droits de l'ensemble des personnes affectées. Il ne serait donc pas nécessaire d'informer toutes les personnes des conditions de la collecte des données avant de leur fournir une aide si cela devait gravement entraver, retarder ou empêcher la distribution de cette aide. Les organisations humanitaires concernées pourraient donner ces informations selon une approche moins ciblée et individualisée, par exemple à l'aide d'affiches publiques, ou de manière individuelle à un stade ultérieur.

Certaines organisations humanitaires dont le mandat est ancré dans le droit international doivent suivre des procédures de travail particulières pour être en mesure d'accomplir ce mandat. En vertu du droit international, ces mandats peuvent justifier des dérogations aux principes et aux droits reconnus en matière de traitement des données personnelles.

Il peut être nécessaire, par exemple, de mettre en balance d'un côté les droits relatifs à la protection des données et, de l'autre, l'objectif d'assurer la responsabilité historique et humanitaire des parties prenantes dans les urgences humanitaires. Dans ces situations, il peut en effet arriver que les organisations humanitaires soient les seules entités externes présentes et qu'elles représentent la seule possibilité pour les générations futures d'avoir un compte rendu extérieur des faits

²⁹ Conformément aux Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés par la Résolution 45/95 de l'Assemblée générale des Nations Unies du 14 décembre 1990.

et de donner une voix aux victimes³⁰. Les données des organisations humanitaires peuvent également être nécessaires pour aider les victimes de conflits armés et d'autres situations de violence, ou leurs descendants, par exemple afin d'attester de leur identité et de leur statut juridique, de soumettre une demande de réparation, etc. La conservation des données par les organisations humanitaires peut revêtir une importance fondamentale, et ce d'autant plus que dans les situations d'urgence humanitaire il peut y avoir peu ou pas d'autres traces documentaires.

La confidentialité peut elle aussi jouer un rôle fondamental pour certaines organisations humanitaires, car elle peut être une condition préalable indispensable pour assurer la viabilité de l'action humanitaire dans des contextes instables ainsi que pour garantir l'acceptation par les parties à un conflit et les acteurs engagés dans d'autres situations de violence, la proximité à l'égard des personnes dans le besoin et la sécurité de leur personnel. Elle peut, par exemple, avoir un impact sur la mesure dans laquelle les personnes concernées peuvent exercer leurs droits d'accès aux données les concernant³¹.

La liste ci-dessous récapitule les principaux points expliqués en détail dans ce manuel, qu'il convient de considérer dans le cadre de la protection des données eu égard aux finalités du traitement des données :

- Des données personnelles sont-elles traitées ?
- Les données traitées permettent-elles d'identifier des personnes physiques ?
- Les informations doivent-elles être protégées même si elles ne sont pas considérées comme des données personnelles ?
- La législation locale sur la protection des données et le respect de la vie privée (si elle est applicable) a-t-elle été respectée ?
- Quelle est la finalité de la collecte et du traitement des données ? Le processus de traitement est-il strictement limité à cette finalité ? La finalité justifie-t-elle l'ingérence dans la vie privée de la personne concernée ?
- Quelle est la base juridique du traitement des données ? Comment les principes de loyauté et de licéité de ce traitement seront-ils assurés ?
- Le traitement des données personnelles est-il proportionné ? La même finalité pourrait-elle être atteinte de manière moins intrusive ?
- Qui sont les responsables du traitement des données et les sous-traitants ? Quelles relations existe-t-il entre eux ?

30 Voir « Les archives du CICR relatives aux prisonniers de la Première Guerre mondiale inscrites au Registre de la Mémoire du monde de l'UNESCO », 15 novembre 2007 : <https://www.icrc.org/fre/resources/documents/feature/ww1-feature-151107.htm>.

31 *Ibid.*

- Les données sont-elles exactes et à jour?
- Est-ce que l'on veillera à recueillir et traiter la plus petite quantité de données possible?
- Pendant combien de temps les données personnelles seront-elles conservées? Comment veillera-t-on à ce que les données soient uniquement conservées le temps nécessaire pour atteindre la finalité du traitement?
- Des mesures de sécurité adéquates ont-elles été prises pour protéger les données?
- A-t-on clairement indiqué aux personnes concernées qui assumait la responsabilité du traitement des données personnelles?
- Les personnes concernées ont-elles été informées de la manière dont leurs données personnelles sont traitées et avec qui elles seront partagées?
- Des procédures sont-elles prévues pour garantir que les personnes concernées peuvent faire valoir leurs droits en ce qui concerne le traitement de leurs données personnelles?
- Sera-t-il nécessaire de partager des données avec des tiers? Dans quelles circonstances les données personnelles seront-elles communiquées ou rendues accessibles à des tiers? Comment les personnes concernées en seront-elles informées?
- Les données personnelles seront-elles rendues accessibles dans un autre pays que celui dans lequel elles ont été initialement collectées ou traitées? Sur quelle base juridique?
- Des analyses d'impact relatives à la protection des données ont-elles été réalisées pour déterminer, évaluer et gérer les risques pour les données personnelles découlant d'un projet, d'une politique, d'un programme ou d'une autre initiative?

2.2 NOTIONS ÉLÉMENTAIRES DE LA PROTECTION DES DONNÉES³²

Le droit de la protection des données et les pratiques en la matière limitent le **traitement** des **données personnelles** des **personnes concernées** afin de protéger leurs droits.

Le **traitement** doit s'interpréter comme toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données personnelles ou des ensembles de données personnelles, comme la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation

³² Les termes définis ci-dessous figurent également dans le glossaire figurant au début de ce manuel.

ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement, la combinaison ou la suppression.

Donnée personnelle : toute information relative à une personne physique identifiée ou identifiable. Une personne concernée est une personne physique (c'est-à-dire un individu) qui peut être identifiée, directement ou indirectement, notamment par référence à ses données personnelles.

Certaines lois relatives à la protection des données incluent la catégorie des **données sensibles** dans la notion de données personnelles. Pour les besoins de ce manuel, les données sensibles sont des données personnelles qui, si elles sont divulguées, peuvent entraîner une discrimination ou une répression à l'encontre de la personne physique concernée. En général, sont considérées comme sensibles les données relatives à l'état de santé, à la race ou à l'origine ethnique, ou bien aux affiliations religieuses ou politiques, ou à des groupes armés, ou encore les données génétiques ou biométriques. Toutes les données sensibles requièrent une protection renforcée même si les différents types de données qui entrent dans cette catégorie (par exemple, différents types de données biométriques) n'ont pas nécessairement le même niveau de sensibilité. Étant donné les environnements particuliers dans lesquels travaillent les organisations humanitaires et la possibilité que certaines données puissent engendrer des discriminations, on ne peut espérer établir une liste définitive des données sensibles pour l'action humanitaire. En effet, une simple liste de noms, par exemple, peut être très sensible dans certaines situations si elle expose les personnes qui y figurent ou leur famille à un risque de persécution. De même, dans d'autres situations, il peut être nécessaire d'inclure dans les données recueillies pour faire face aux urgences humanitaires des données qui seraient en principe interdites dans un contexte ordinaire de protection des données, mais qui peuvent être relativement anodines dans la culture locale et dans la situation considérée. Il faut donc examiner au cas par cas la sensibilité des données et les garanties appropriées afin de protéger les données sensibles (mesures de sécurité techniques et organisationnelles, par exemple).

Il est important de garder à l'esprit que dans une situation d'urgence humanitaire, le traitement des données peut causer de graves préjudices, même lorsque les données ne peuvent pas être considérées comme des données personnelles. Les organisations internationales doivent donc être prêtes à appliquer les protections décrites dans ce manuel à d'autres catégories de données lorsque l'absence de protection pourrait engendrer des risques pour les individus.

EXEMPLE :

Une organisation humanitaire révèle par inadvertance le nombre de personnes se trouvant dans un groupe qui fuit une situation de violence armée et publie des images aériennes à ce sujet. L'un des acteurs armés ayant forcé ces gens à fuir se sert ensuite de ces informations pour localiser la population déplacée et exerce des représailles. Ces informations (le nombre de personnes recensées dans un groupe et les images aériennes – sous réserve de la résolution et d'autres facteurs pouvant permettre d'identifier les individus) ne sont pas en elles-mêmes des données personnelles, mais elles peuvent être extrêmement sensibles dans certaines circonstances. L'organisation humanitaire n'aurait pas dû révéler ces informations, mais, au contraire, les protéger.

Il importe également de comprendre la distinction entre **responsable du traitement** et **sous-traitant**. Le responsable du traitement est la personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles, alors que le sous-traitant est la personne physique ou morale qui traite des données personnelles pour le compte du responsable du traitement. Enfin, un tiers est une personne physique ou morale, une autorité publique, un service public ou un organisme autre que la personne concernée, le responsable du traitement ou le sous-traitant.

EXEMPLE :

Une organisation humanitaire internationale recueille des informations sur l'identité des personnes dans le cadre d'une urgence humanitaire afin de leur apporter de l'aide. Pour ce faire, elle fait appel aux services d'une ONG locale qui a besoin d'utiliser les informations d'identification initialement collectées par l'organisation humanitaire. Les deux organisations signent un contrat régissant l'utilisation des données, en vertu duquel l'organisation humanitaire internationale a le pouvoir de donner à l'ONG des instructions sur la façon dont celle-ci utilise les données et l'ONG s'engage à respecter les mesures de protection des données requises par l'organisation humanitaire. L'ONG charge en outre une société de conseil informatique de la maintenance courante de son système informatique sur lequel les données sont enregistrées.

Dans ce cas précis, l'organisation humanitaire internationale, l'ONG et la société de conseil informatique traitent les données personnelles de personnes physiques, qui sont les personnes concernées. L'organisation humanitaire internationale est le responsable du traitement et l'ONG est le sous-traitant, tandis que la société de conseil informatique est un sous-traitant ultérieur.

2.3 ENSEMBLES DE DONNÉES AGRÉGÉES, PSEUDONYMISÉES ET ANONYMISÉES

Comme indiqué plus haut, ce manuel n'aborde pas le traitement de données ne concernant pas des individus, telles que les données agrégées ou statistiques, ni le traitement de données ayant été rendues anonymes de quelque autre manière que ce soit pour que la personne concernée ne soit plus identifiable.

Lorsque des données agrégées sont dérivées de données personnelles et pourraient, dans certaines circonstances, engendrer des risques pour les personnes concernées, il est important de veiller à ce que leur traitement, leur partage ou leur publication ne puisse pas conduire à la réidentification de ces personnes³³.

Bien qu'il ne soit pas obligatoire d'obtenir le consentement explicite des personnes concernées pour utiliser leurs données personnelles dans des ensembles de données agrégées ou dans des statistiques, les organisations humanitaires doivent veiller à ce que le traitement des données ait un autre fondement légitime³⁴ et n'expose pas les individus ou les groupes à des préjudices ni ne fragilise leur protection de quelque autre manière que ce soit.

L'anonymisation des données personnelles peut permettre de répondre aux besoins de protection et d'assistance des individus vulnérables sans porter atteinte à leur vie privée. Le terme « anonymisation » recouvre les techniques permettant de convertir des données personnelles en données anonymes. Lorsqu'on anonymise des données, il est indispensable de s'assurer que les ensembles de données qui contiennent des données personnelles sont rendus totalement et irréversiblement anonymes. Les procédures d'anonymisation ne sont pas chose aisée, en particulier lorsqu'on a affaire à de grands ensembles de données contenant un large éventail de données personnelles, qui peuvent engendrer un risque plus important de réidentification³⁵.

La « pseudonymisation », qui se distingue de l'anonymisation, est le traitement des données personnelles à l'issue duquel celles-ci ne peuvent plus être attribuées à une personne précise sans informations complémentaires, sous réserve que ces informations complémentaires soient conservées à part et fassent l'objet de

33 Voir UK Government Statistical Service, *Privacy and data confidentiality methods: a Data and Analysis Method Review (DAMR)*. National Statistician's guidance: confidentiality of official statistics. This guidance has been superseded by Privacy and data confidentiality methods: a National Statistician's Quality Review (NSQR) : <https://gss.civilservice.gov.uk/policy-store/privacy-and-data-confidentiality-methods-a-national-statisticians-quality-review-nsqr/>.

34 Voir chapitre 3 : *Fondements juridiques du traitement des données personnelles*.

35 Voir Bureau du Commissaire à l'information du Royaume-Uni, *Anonymisation: managing data protection risk – Code of practice* : <https://ico.org.uk/media/1061/anonymisation-code.pdf> ; voir aussi Groupe de travail « Article 29 » sur la protection des données de l'Union européenne, *Avis 05/2014 sur les Techniques d'anonymisation* : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf.

mesures techniques et organisationnelles garantissant que les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable. Cette opération peut nécessiter de remplacer les données d'état civil³⁶ présentes dans un ensemble de données par un numéro. Partager des numéros d'enregistrement/identification au lieu de noms est une bonne pratique, mais cela ne constitue pas une anonymisation.

Avant de partager ou de publier des données anonymisées, il importe de s'assurer que l'ensemble de données ne comprend aucune donnée personnelle et qu'il est impossible de réidentifier les personnes. Le terme « réidentification » décrit le processus consistant à reconvertir des données qui auraient été anonymisées en données personnelles par des « recoupements » ou des techniques similaires³⁷. Si le risque de réidentification semble raisonnablement probable, on doit considérer les informations comme des données personnelles, soumises à tous les principes et orientations exposés dans ce manuel. Il peut être très difficile d'évaluer le risque de réidentification avec une certitude absolue.

Avant de partager ou de publier des données agrégées, il est important de s'assurer que les ensembles de données ne révèlent pas la localisation réelle de groupes peu nombreux ou à risques, par exemple par une mise en correspondance des données, telles que le pays d'origine, la religion ou les vulnérabilités particulières, avec les coordonnées géographiques des personnes concernées.

2.4 DROIT APPLICABLE ET ORGANISATIONS INTERNATIONALES

L'action humanitaire fait intervenir de nombreux acteurs, comme les organisations humanitaires, les autorités locales et les entreprises privées. En ce qui concerne les organisations humanitaires, certaines sont des ONG soumises à la juridiction du pays dans lequel elles travaillent, tandis que d'autres sont des organisations internationales bénéficiant de privilèges et d'immunités grâce auxquels elles peuvent accomplir en toute indépendance le mandat qui leur est confié par la communauté des États en vertu du droit international.

En ce qui concerne les ONG, les règles qui déterminent le droit applicable en matière de protection des données dépendent de plusieurs éléments factuels. Ce manuel n'aborde pas les considérations relatives au droit applicable ; toute question sur ce point doit être adressée au service juridique de l'ONG ou à son bureau de la protection des données³⁸.

³⁶ <https://en.wiktionary.org/wiki/anagraphic>.

³⁷ NB : « identifié » ne signifie pas nécessairement « nommé » ; la possibilité d'établir un lien fiable entre certaines données et une personne connue peut être suffisante.

³⁸ Voir [section 1.2 : Objectif](#).

Outre les lois auxquelles l'ONG peut être soumise, le traitement des données personnelles est régi par ses politiques ou règles internes en matière de protection des données, par ses engagements contractuels éventuels et par toute autre règle applicable en la matière. Les lignes directrices données dans ce manuel doivent toujours être appliquées sans préjudice de ces règles et obligations. Ces lignes directrices se fondent sur les meilleures pratiques et normes reconnues, et il est recommandé aux organisations internationales d'en tenir compte lorsqu'elles conçoivent ou interprètent leurs règles et politiques de protection des données pour l'action humanitaire.

Les organisations internationales bénéficient de privilèges et d'immunités garantissant qu'elles peuvent accomplir en toute indépendance le mandat qui leur est confié par la communauté internationale en vertu du droit international, et elles ne sont pas placées sous la juridiction des pays dans lesquelles elles travaillent. Elles peuvent donc traiter des données personnelles conformément à leurs propres règles, sous la surveillance et le contrôle de leurs systèmes de conformité internes ; à cet égard, elles constituent leur propre « juridiction ». Cette caractéristique des organisations internationales a des implications particulières, en particulier pour le transfert international des données, qui sera abordé en plus amples détails au [chapitre 4 : Transfert international de données](#).

2.5 PRINCIPES APPLICABLES AU TRAITEMENT DES DONNÉES

Le traitement des données personnelles entrepris par les organisations humanitaires doit respecter les principes énoncés ci-après.

2.5.1 PRINCIPES DE LICÉITÉ, DE LOYAUTÉ ET DE TRANSPARENCE DU TRAITEMENT

Le traitement des données personnelles doit être équitable et licite. Pour être licite, le traitement doit avoir une base juridique, comme il est expliqué plus précisément au [chapitre 3 : Fondements juridiques du traitement des données personnelles](#). Pour être équitable, le traitement doit être transparent.

Le traitement de données personnelles doit toujours être transparent pour les personnes concernées. Le principe de transparence exige de donner au moins un minimum d'informations sur le traitement aux personnes concernées au moment de la collecte, mais sous réserve des conditions logistiques et de sécurité, ainsi que de l'urgence éventuelle du traitement. Les informations et communications relatives au traitement des données personnelles doivent être faciles d'accès et aisément compréhensibles, ce qui suppose de prévoir des traductions, si nécessaire, et d'employer un langage clair et simple. Des informations plus précises sur les

notices d'information à fournir avant ou pendant la collecte des informations sont présentées à la [section 2.10.2: Notices d'information](#).

2.5.2 PRINCIPE DE LIMITATION DES FINALITÉS

Au moment de la collecte des données, l'organisation humanitaire doit déterminer et énoncer les finalités spécifiques du traitement des données, qui doivent être explicites et légitimes. À titre d'exemple, les finalités suivantes peuvent être pertinentes en contexte humanitaire :

- apporter une assistance humanitaire ou fournir des services aux populations touchées afin de pérenniser les moyens d'existence ;
- rétablir les liens familiaux entre des personnes séparées en raison d'urgences humanitaires ;
- protéger les personnes touchées et faire respecter le droit international des droits humains/droit international humanitaire, y compris en documentant chacune des violations qui ont été commises ;
- fournir une assistance médicale ;
- assurer l'inclusion dans les systèmes nationaux (par exemple pour les réfugiés) ;
- fournir des documents ou un statut juridique/une identité, par exemple aux personnes déplacées ou apatrides ;
- protéger l'eau et l'habitat.

Pour une transparence maximale, les organisations humanitaires doivent veiller à étudier et déterminer, dans toute la mesure du possible, toutes les finalités qui, en situation humanitaire, sont et pourraient être envisagées lors de tout traitement ultérieur éventuel, et ce, dès le début de la collecte des données.

2.5.3 PRINCIPE DE PROPORTIONNALITÉ

Le principe de proportionnalité est au cœur du droit de la protection des données. Il est applicable tout au long du cycle de traitement des données et peut être invoqué à différents stades des opérations de traitement. Cela suppose de veiller à ce qu'une action ou mesure liée au traitement des données personnelles soit bien adaptée à l'objectif poursuivi. On pourra notamment se poser les questions suivantes : La base légitime sélectionnée est-elle proportionnée à l'objectif poursuivi ? Les mesures techniques et organisationnelles sont-elles proportionnées aux risques associés au traitement ?

Les données traitées par les organisations humanitaires doivent être adéquates, pertinentes et non excessives pour les finalités de la collecte et du traitement. Cela exige, en particulier, de veiller à ne collecter et à ne traiter ultérieurement que les données nécessaires pour atteindre les finalités (définies à l'avance) et à limiter au minimum requis la durée pendant laquelle ces données sont conservées avant d'être anonymisées ou supprimées³⁹.

³⁹ Voir [section 2.7: Conservation des données](#).

Le principe de proportionnalité est particulièrement important pour les évaluations transversales des besoins réalisées par les organisations humanitaires, soit en interne, soit à l'échelle interorganisationnelle. Lorsqu'elles conduisent ces évaluations, les organisations humanitaires risquent de recueillir des quantités de données excessives par rapport aux finalités, notamment lorsqu'elles réalisent des enquêtes comportant plusieurs centaines de champs à remplir, qui seront ou non utilisés ultérieurement. Dans ces situations, il est important de pouvoir faire la distinction entre ce qu'il est « intéressant de savoir » et ce qu'il est « nécessaire de savoir » pour aider les bénéficiaires. Les organisations humanitaires doivent aussi évaluer leurs besoins de données par rapport au préjudice que pourraient subir les personnes auprès desquelles les données sont collectées, ainsi que par rapport au risque de susciter une certaine lassitude et des attentes démesurées auprès des personnes qu'elles cherchent à aider.

Cependant, il n'est pas toujours possible de limiter la quantité de données recueillies. Par exemple, lorsque survient une nouvelle urgence humanitaire, l'ampleur des besoins humanitaires n'est pas toujours connue au moment de la collecte des données. L'application de ce principe peut donc être restreinte dans des circonstances exceptionnelles et pour une durée limitée si la protection de la personne concernée ou des droits et des libertés d'autrui l'exige.

Il est possible également qu'en raison de l'urgence, la finalité au moment de la collecte soit très générale. Dans ce cas, une collecte de données de grande ampleur pourrait s'avérer nécessaire. L'étendue de cette collecte pourrait ensuite être revue à la baisse en fonction des circonstances. Pour déterminer si une interprétation flexible de la proportionnalité est acceptable face à une nouvelle urgence humanitaire, les facteurs suivants doivent être pris en compte :

- l'urgence de l'intervention ;
- la proportionnalité entre la quantité de données personnelles collectées et les objectifs de l'action humanitaire ;
- les difficultés (liées à des contraintes logistiques ou de sécurité) que l'on pourrait rencontrer s'il fallait revenir vers la personne concernée afin de recueillir de nouvelles données si l'on envisageait d'autres finalités ;
- les objectifs de l'action de l'organisation humanitaire ;
- la nature et la portée des données personnelles qui peuvent s'avérer nécessaires pour atteindre les finalités spécifiées ;
- les attentes des personnes concernées ;
- la sensibilité des données personnelles en question.

EXEMPLE :

Une organisation humanitaire recueille des données personnelles afin d'apporter une assistance humanitaire à un groupe de personnes vulnérables dans une région frappée par une catastrophe. Au début de l'action humanitaire, il n'a pas été possible de déterminer les besoins précis des personnes touchées ni l'assistance et les programmes dont elles auraient besoin immédiatement ou ultérieurement (la destruction des installations d'assainissement pourrait engendrer des risques d'épidémie par exemple). De ce fait, l'organisation humanitaire entreprend un important projet de collecte de données afin d'évaluer pleinement les besoins des personnes touchées et de concevoir des programmes d'intervention. Une fois l'urgence passée, il s'avère que bien qu'une action humanitaire ait été nécessaire, l'assainissement a été rétabli à temps pour éviter une épidémie. En conséquence, il est possible que l'organisation humanitaire doive supprimer les données initialement collectées.

Dans tous les cas, il faut réexaminer périodiquement la nécessité de conserver les données recueillies, conformément au principe de minimisation des données.

2.5.4 PRINCIPE DE MINIMISATION DES DONNÉES

Le principe de minimisation des données est étroitement lié au principe de proportionnalité. La minimisation des données vise à garantir qu'on ne traite que la quantité minimale de données personnelles nécessaire pour atteindre l'objectif et les finalités pour lesquels les données ont été collectées. Elle exige de limiter le traitement des données personnelles au minimum requis, qu'il s'agisse de la quantité de données ou de l'étendue de la collecte. Les données personnelles doivent être supprimées lorsqu'elles ne sont plus nécessaires aux finalités de la collecte initiale ou à un traitement ultérieur compatible. Elles doivent être également supprimées lorsque les personnes concernées ont retiré leur consentement au traitement ou s'opposent légitimement à celui-ci. Cependant, même dans ces circonstances, les données personnelles peuvent être conservées si elles sont nécessaires à des fins historiques, statistiques ou scientifiques légitimes, ou si l'organisation humanitaire est légalement tenue de conserver ces données, et ce, en tenant compte des risques associés et en mettant en œuvre les garanties adéquates.

Pour déterminer si les données ne sont plus nécessaires aux finalités pour lesquelles elles ont été recueillies ou à un traitement ultérieur compatible, les organisations humanitaires doivent examiner les aspects suivants :

- La finalité spécifiée a-t-elle été atteinte ?
- Dans la négative, toutes les données sont-elles encore nécessaires pour l'atteindre ? La probabilité d'atteindre la finalité spécifiée est-elle si faible que la conservation des données ne se justifie plus ?

- Des inexactitudes ont-elles affecté la qualité des données personnelles?
- Des mises à jour et des changements significatifs ont-ils rendu inutiles les données personnelles enregistrées initialement?
- Les données sont-elles nécessaires pour des finalités historiques, statistiques ou scientifiques légitimes? Est-il proportionné de les conserver compte tenu des risques associés? Des garanties appropriées pour la protection des données sont-elles en place en vue de cette conservation ultérieure?
- La situation de la personne concernée a-t-elle changé et ces nouveaux facteurs rendent-ils les données initialement enregistrées obsolètes et non pertinentes?

2.5.5 PRINCIPE DE QUALITÉ DES DONNÉES

Les données personnelles doivent être aussi exactes et à jour que possible. Toutes les mesures raisonnables doivent être prises pour rectifier ou supprimer dans les meilleurs délais les données personnelles inexactes compte tenu des finalités du traitement. L'organisation humanitaire doit systématiquement réexaminer les informations collectées afin de vérifier qu'elles sont fiables, exactes et à jour, conformément aux lignes directrices et procédures opérationnelles.

Lorsque l'on considère la fréquence de cet examen, il convient de tenir compte i) des contraintes logistiques et sécuritaires, ii) des finalités du traitement et iii) des conséquences possibles de données inexactes. Toutes les mesures raisonnables doivent être prises pour limiter le risque de prendre une décision susceptible de nuire à un individu, comme exclure une personne d'un programme humanitaire sur la base de données potentiellement inexactes.

2.6 SITUATIONS PARTICULIÈRES EN MATIÈRE DE TRAITEMENT DES DONNÉES

Les paragraphes qui suivent donnent des exemples de situations courantes en matière de traitement des données qui requièrent des explications particulières.

2.6.1 FINALITÉS DE SANTÉ

Une mauvaise gestion (y compris la divulgation) de données de santé pourrait causer un important préjudice aux personnes concernées. Les données de santé doivent donc être considérées comme des données particulièrement sensibles et des garanties spécifiques doivent être prises lors de leur traitement, comme pour les données sensibles. De plus, les données de santé sont de plus en plus ciblées par les cyberattaques. Les prestataires de soins de santé humanitaires doivent traiter les données conformément au Code international d'éthique médicale de l'Association

médicale mondiale (AMM)⁴⁰, qui prévoit des obligations professionnelles particulières en matière de confidentialité.

Les organisations humanitaires peuvent traiter des données de santé pour les finalités suivantes :

- la médecine préventive ou du travail, le diagnostic médical, les soins ou le traitement ;
- la gestion de services de soins de santé ;
- des raisons d'intérêt vital, notamment la fourniture d'une assistance médicale essentielle pour sauver la vie de la personne concernée ;
- la santé publique, par exemple protéger contre de graves menaces pour la santé ou garantir des niveaux élevés de qualité et de sécurité, notamment en ce qui concerne les médicaments ou les appareils médicaux ;
- des finalités de recherche historique, statistique ou scientifique, comme les registres de patients établis pour améliorer le diagnostic et distinguer les différents types de maladies similaires et préparer des études pour les thérapies, sous réserve de conditions et de garanties.

Les données de santé doivent être conservées séparément des autres données personnelles et elles ne doivent être accessibles qu'au personnel ou aux prestataires de soins de santé expressément délégués par les prestataires de soins de santé humanitaires pour gérer les données de santé selon les garanties de confidentialité formulées dans les contrats (de travail, de conseil ou autres) et uniquement aux fins de gestion des données prédéfinies. Ces données peuvent également être accessibles au personnel dans le cadre de recherches selon les garanties de confidentialité et de protection des données énoncées dans les contrats (de travail, de conseil ou autres) et uniquement aux fins de recherche prédéfinies.

Les organisations humanitaires exerçant des activités de protection ou d'assistance peuvent également traiter des données de santé, par exemple lorsque c'est nécessaire pour localiser des personnes disparues (lorsque des données de santé peuvent être requises pour les identifier ou les retrouver) ou pour plaider pour un traitement adéquat des individus privés de liberté ou encore pour établir des programmes de développement des moyens d'existence ciblant les besoins de catégories de bénéficiaires particulièrement vulnérables (comme les personnes souffrant de malnutrition ou de maladies particulières)⁴¹.

40 AMM, *Code international d'éthique médicale de l'AMM* : <https://www.wma.net/fr/policies-post/code-international-dethique-medicale-de-lamm/>.

41 Voir [section 2.6.3: Traitement ultérieur](#).



J. Zocherman/CICR

État de Jonglei (Soudan du Sud). Un blessé de guerre évacué par une équipe médicale.

2.6.2 ACTIVITÉS ADMINISTRATIVES

Les organisations humanitaires traitent généralement des données personnelles pour des finalités liées à l'emploi, à la gestion des carrières, aux évaluations, au marketing direct et à d'autres besoins administratifs. Dans certains cas, elles peuvent aussi avoir des activités de traitement sensibles comme le suivi par GPS de leurs véhicules pour la gestion des flottes et de la sécurité. Certaines circonstances opérationnelles peuvent rendre le traitement des données personnelles des employés particulièrement sensible en raison, par exemple, du contexte géopolitique dans lequel une aide humanitaire est apportée. Dans ce cas, il sera nécessaire de fournir, dans la mesure du possible, des garanties supplémentaires pour le traitement des données.

2.6.3 TRAITEMENT ULTÉRIEUR

Les organisations humanitaires peuvent traiter des données personnelles pour d'autres finalités que celles qui ont été initialement spécifiées au moment de la collecte lorsque ce traitement ultérieur est compatible avec les finalités initiales de la collecte et, en particulier, lorsqu'il est nécessaire à des fins historiques, statistiques ou scientifiques.

Pour déterminer si une finalité du traitement ultérieur est compatible avec les finalités de la collecte initiale, les aspects suivants doivent être pris en compte :

- le lien entre la ou les finalités initiales et celle(s) du traitement ultérieur ;
- les circonstances dans lesquelles les données ont été collectées, y compris les attentes raisonnables des personnes concernées quant à leur utilisation future ;

- la nature des données personnelles ;
- les conséquences du traitement ultérieur envisagé pour les personnes concernées ;
- les garanties appropriées ;
- la mesure dans laquelle ces garanties protégeraient la confidentialité des données personnelles et l'anonymat des personnes concernées.

La situation dans laquelle les données ont été recueillies, y compris les attentes raisonnables des personnes concernées quant à leur utilisation future, est un facteur particulièrement important, sachant que lorsque les personnes concernées fournissent des données pour une finalité particulière, elles comprennent généralement qu'un ensemble d'activités humanitaires associées peut aussi entrer en jeu et peuvent en fait penser que toutes les mesures possibles de protection et d'assistance seront mises en place. Ceci est particulièrement important dans les situations humanitaires parce qu'une conception trop étroite de la compatibilité pourrait priver les personnes concernées des bénéfices de l'action humanitaire.

Par conséquent, les finalités strictement liées à l'action humanitaire, et qui n'engendrent pas de risques non prévus dans l'étude des finalités initiales, seront probablement compatibles les unes avec les autres et, si cette compatibilité est confirmée, une organisation humanitaire pourra légitimement traiter des données personnelles au-delà des finalités spécifiques de la collecte initiale, pour autant qu'elle le fasse dans le cadre de l'action humanitaire. En principe, le traitement ultérieur devrait être permis s'il est nécessaire et proportionné pour protéger la sécurité publique et la vie, l'intégrité, la santé, la dignité ou la sécurité des personnes touchées dans le cadre de l'action humanitaire. Ces caractéristiques de nécessité et de proportionnalité doivent être évaluées au cas par cas. Elles ne sauraient être présumées.

Même lorsque la finalité du traitement ultérieur est exclusivement liée à l'action humanitaire, le traitement pour une nouvelle finalité ne sera pas considéré compatible si les risques pour la personne concernée sont supérieurs aux avantages du traitement ultérieur ou si celui-ci engendre de nouveaux risques. Cette analyse dépend des circonstances. On pourra, par exemple, tirer cette conclusion si le traitement risque d'être contraire aux intérêts de la personne à laquelle les informations ont trait ou à ceux de sa famille, notamment lorsqu'il risque de porter atteinte à leur vie, à leur intégrité, à leur dignité, à leur sécurité psychologique ou physique, à leur liberté ou à leur réputation. Les conséquences peuvent être les suivantes :

- harcèlement ou persécution de la part des autorités ou de tiers ;
- poursuites judiciaires ;
- problèmes sociaux ;
- graves souffrances psychologiques.

Un traitement ultérieur peut être considéré incompatible, par exemple, lorsque les données personnelles sont recueillies avec les informations nécessaires pour faciliter la recherche d'une personne portée disparue. Le traitement ultérieur de ces informations pour demander aux autorités compétentes d'enquêter sur les violations possibles du droit applicable (par exemple dans le contexte d'activités de protection de la population civile) peut être incompatible du fait des conséquences néfastes qu'il pourrait avoir pour les personnes concernées et des difficultés probables à fournir des garanties appropriées.

Si la finalité du traitement ultérieur envisagée n'est pas compatible avec celle de la collecte initiale, on ne doit pas procéder au traitement ultérieur des données, sauf s'il est jugé approprié en vertu d'une autre base juridique. Dans ce cas, des mesures supplémentaires peuvent être requises selon le fondement applicable⁴².

Le traitement ultérieur des données personnelles ne doit pas non plus être considéré compatible s'il est contraire à des obligations légales ou professionnelles, à d'autres obligations de secret et de confidentialité ou au principe « ne pas nuire ».

Il est possible d'agréger et d'anonymiser les données pour réduire leur sensibilité et permettre ainsi leur utilisation à des fins accessoires.

EXEMPLE :

Les données recueillies pour distribuer de la nourriture et offrir des abris au cours d'une opération humanitaire peuvent être également utilisées pour organiser la fourniture de services médicaux aux personnes déplacées. Toutefois, le traitement des données recueillies (si elles ne sont pas agrégées ni anonymisées) pour planifier les besoins budgétaires de l'organisation humanitaire pour l'année à venir ne peut être considéré comme un traitement ultérieur compatible.

2.7 CONSERVATION DES DONNÉES

Une durée de conservation doit être définie pour chaque catégorie de données (trois mois, un an, etc.). S'il n'est pas possible, à la date de la collecte, de déterminer combien de temps les données doivent être conservées, une durée de conservation initiale doit être fixée. Au terme de celle-ci, on procédera à une évaluation afin de déterminer si les données doivent être supprimées ou si elles sont encore nécessaires aux fins pour lesquelles elles ont été initialement collectées (ou à des fins légitimes ultérieures). Dans l'affirmative, la durée de conservation initiale pourra être prolongée pour une durée limitée.

⁴² Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

Lorsque des données ont été supprimées, toutes les copies de ces données doivent également être supprimées. Si l'organisation humanitaire a partagé des données avec des tiers, elle doit prendre des mesures raisonnables pour s'assurer que ces derniers suppriment eux aussi les données en question. Cette obligation de suppression est à prendre en compte dans les réflexions initiales sur la possibilité de partager des données avec des tiers et doit être stipulée dans tout contrat de partage de données⁴³.

2.8 SÉCURITÉ DES DONNÉES ET DU TRAITEMENT

2.8.1 INTRODUCTION

La sécurité des données est une composante essentielle d'un système efficace de protection des données. Les données personnelles devraient être traitées de manière à garantir une sécurité appropriée, par exemple, afin de prévenir tout accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que toute utilisation non autorisée de ces données et de cet équipement, à plus forte raison dans les environnements instables dans lesquels les organisations humanitaires sont souvent appelées à intervenir.

Toute personne agissant sous l'autorité du responsable du traitement qui a accès à des données personnelles doit exclusivement les traiter conformément aux politiques applicables exposées dans ce manuel.

Pour préserver la sécurité, le responsable du traitement doit évaluer les risques propres au traitement et prendre des mesures pour les atténuer. Ces mesures doivent garantir un niveau de sécurité approprié (compte tenu des technologies disponibles, des conditions logistiques et sécuritaires et des coûts de mise en œuvre) à la nature des données personnelles à protéger et aux risques associés. Elles portent sur les aspects suivants :

- la formation du personnel et des partenaires ;
- la gestion des droits d'accès aux bases de données contenant des données personnelles ;
- la sécurité physique des bases de données (réglementation de l'accès, dégâts causés par l'eau et la température, etc.) ;
- la sécurité informatique (protection par mot de passe, transfert sécurisé des données, chiffrement, sauvegardes régulières, etc.) ;
- les clauses de discrétion ;
- les contrats de partage de données avec des partenaires et des tiers ;
- les méthodes de destruction des données personnelles ;

43 Voir [section 2.12 : Partage de données et transfert international de données](#), et [chapitre 4 : Transfert international de données](#).

- les procédures opérationnelles standards relatives à la gestion et la conservation des données ;
- toute autre mesure appropriée.

Ces mesures visent à garantir la sécurité des données personnelles, tant sur le plan technique qu'organisationnel, et leur protection par des dispositions raisonnables et appropriées contre les utilisations abusives, les modifications non autorisées, les copies, l'altération, la destruction illicite, la perte accidentelle, la divulgation abusive ou les transferts indus (ci-après désignés conjointement « violation des données »). Les mesures de sécurité des données doivent être adaptées, entre autres, aux caractéristiques suivantes :

- type d'opération ;
- niveau de risques évalués en matière de protection des données ;
- nature et sensibilité des données personnelles en question ;
- forme ou format de stockage, de transfert et de partage des données ;
- environnement/localisation des données personnelles ;
- conditions logistiques et sécuritaires.

Les mesures de sécurité des données doivent être régulièrement revues et actualisées afin de garantir un niveau de protection approprié au degré de sensibilité des données personnelles et, le cas échéant, au développement de nouvelles technologies permettant une sécurité renforcée.

Le responsable du traitement est tenu d'assumer les tâches suivantes :

- mise en place d'un système de gestion de la sécurité de l'information ; comprend l'établissement et l'actualisation régulière d'une politique de sécurité des données fondée sur les normes internationalement reconnues et sur une évaluation des risques. Cette politique doit être constituée, par exemple, de règles de sécurité informatique, de lignes directrices relatives à la sécurité physique, à la sécurité des courriers électroniques, à l'usage du matériel informatique et à la classification des informations (publiques, internes, confidentielles ou strictement confidentielles), d'un plan d'urgence et d'instructions pour la destruction des documents.
- développement de l'infrastructure de communication et des bases de données afin de préserver la confidentialité, l'intégrité et la disponibilité des données conformément à la politique de sécurité ;
- mise en place de toutes les mesures appropriées pour préserver la sécurité des données traitées dans le système informatique du responsable du traitement ;
- octroi et administration des droits d'accès aux bases de données contenant des données personnelles sur la base du « besoin de savoir » ;
- sécurité des installations permettant au personnel autorisé d'accéder au système ;
- veiller, avant de consentir un droit d'accès aux données à un membre du personnel, à ce que celui-ci puisse respecter pleinement les règles de sécurité (formation adaptée, engagement de discrétion, obligation de confidentialité en vertu du contrat de travail, à signer avant d'autoriser l'accès à une base de données) ;

- tenue d'un registre des membres du personnel ayant accès à chaque base de données ; des mises à jour peuvent être nécessaires, notamment lorsque le personnel se voit attribuer de nouvelles responsabilités qui n'exigent plus qu'il ait accès aux bases de données ;
- tenue, si possible, d'un journal historique et conduite éventuelle d'audits du personnel ayant accès à une base de données, et ce, aussi longtemps que les données traitées par ledit personnel figurent dans la base de données.

Les membres du personnel doivent traiter les données dans les limites des droits qui leur sont octroyés. Ceux qui disposent de droits d'accès supérieurs ou sont responsables de l'administration des droits d'accès peuvent être astreints à d'autres obligations contractuelles de confidentialité et de non-divulgaration.

2.8.2 SÉCURITÉ PHYSIQUE

Le responsable du traitement est tenu d'assumer les tâches suivantes :

- fixer les règles de sécurité définissant les contrôles procéduraux, techniques et administratifs qui garantissent des niveaux de confidentialité appropriés ainsi que l'intégrité physique et la disponibilité des bases de données (physiques ou informatiques) compte tenu des risques diagnostiqués ;
- veiller à ce que le personnel connaisse et respecte ces règles de sécurité ;
- instaurer des mécanismes de contrôle appropriés pour préserver la sécurité des données ;
- veiller à ce que des normes appropriées en matière de sécurité électrique et de sécurité incendie soient appliquées aux installations de stockage ;
- veiller à ce que les volumes de stockage soient maintenus au strict minimum.

2.8.3 SÉCURITÉ INFORMATIQUE

Le responsable du traitement doit :

- énoncer les règles de sécurité définissant les contrôles procéduraux, techniques et administratifs qui garantissent des niveaux appropriés de confidentialité, d'intégrité et de disponibilité des systèmes d'information utilisés, sur la base de l'évaluation des risques ;
- instaurer des mécanismes de contrôle appropriés afin de garantir le maintien de la sécurité des données ;
- instaurer si nécessaire des règles de sécurité spécifiques pour une partie de l'infrastructure de communication informatique, une base de données ou un service précis, par exemple, dans le cadre du traitement de données personnelles particulièrement sensibles ou essentielles.

Toutes les correspondances internes et externes par courrier électronique contenant des données personnelles doivent être traitées sur la base du « besoin de savoir ». Les destinataires de courriers électroniques doivent être sélectionnés avec soin afin d'éviter toute diffusion inutile des données personnelles aux personnes qui n'ont

pas besoin de ces informations dans le cadre de leur rôle. Les comptes de messagerie privés ne doivent pas être utilisés pour transférer des données personnelles.

L'accès à distance aux serveurs et l'utilisation d'ordinateurs à domicile doivent respecter les règles énoncées dans la politique de sécurité informatique du responsable du traitement. Sauf nécessité absolue liée à des raisons opérationnelles, il faut éviter d'utiliser des points d'accès à Internet et des connexions wifi non sécurisées pour extraire, partager, transmettre ou transférer des données personnelles.

Les membres du personnel qui manipulent des données personnelles doivent prendre les précautions voulues lorsqu'ils se connectent à distance aux serveurs du responsable du traitement. Les mots de passe doivent toujours être protégés et changés régulièrement. Ils ne doivent pas être saisis automatiquement au moyen d'un trousseau d'accès⁴⁴. Les membres du personnel doivent veiller à se déconnecter convenablement des systèmes informatiques et à fermer les navigateurs.

Une attention particulière doit être portée à la sécurité des ordinateurs portables, des smartphones et autres appareils multimédias portables, surtout lorsque l'on travaille dans un environnement difficile. Les appareils multimédias portables doivent être conservés en tout temps en lieu sûr.

Les appareils portables ou amovibles ne doivent pas être utilisés pour conserver des fichiers contenant des données personnelles sensibles. Lorsqu'il est impossible de faire autrement, les données personnelles doivent être transférées dès que possible vers des systèmes informatiques et applications de bases de données appropriés. Si des supports de mémoire flash tels que des clés USB ou des cartes mémoire sont utilisés pour stocker temporairement des données personnelles, ils doivent être conservés en lieu sûr, et les données électroniques doivent être chiffrées. Les informations enregistrées sur l'appareil portable ou amovible doivent être effacées dès qu'elles ont été enregistrées correctement s'il n'est plus nécessaire de les conserver sur ce support.

Toutes les données électroniques doivent être couvertes par des mécanismes de récupération et des procédures de sauvegarde efficaces, et le responsable informatique doit veiller à ce que des sauvegardes soient effectuées régulièrement. La fréquence des sauvegardes doit être adaptée à la sensibilité des données personnelles et aux ressources techniques. Les enregistrements électroniques doivent être automatisés afin de faciliter la récupération des données lorsque les sauvegardes sont difficiles à réaliser, notamment en raison de coupures de courant régulières, de défaillances système ou de catastrophes.

⁴⁴ Un trousseau ou gestionnaire de mots de passe est une application ou une fonction matérielle qui permet d'enregistrer et d'organiser plusieurs mots de passe sous un mot de passe maître.

Lorsque des données électroniques et des applications de base de données ne sont plus nécessaires, le responsable du traitement doit se rapprocher du responsable informatique en vue de leur suppression permanente.

2.8.4 DEVOIR DE DISCRÉTION ET CONDUITE DU PERSONNEL

Le devoir de discrétion est un élément clé de la sécurité des données personnelles. Il implique :

- la signature, par tous les membres du personnel et consultants extérieurs, d'accords ou de clauses de discrétion et de confidentialité dans le cadre de leur contrat de travail ou de conseil. Cette exigence va de pair avec l'obligation pour le personnel de ne traiter des données que conformément aux instructions du responsable du traitement ;
- la signature de clauses de confidentialité contractuelles par tous les sous-traitants externes. Cette exigence va de pair avec l'obligation pour le sous-traitant de ne traiter des données que conformément aux instructions du responsable du traitement ;
- la stricte application des directives relatives à la classification des informations en fonction de leur degré de confidentialité ;
- le traitement et l'enregistrement corrects, dans le fichier de la personne concernée, des demandes qu'elle a formulées, et ce, de manière sécurisée et confidentielle afin qu'aucune demande ne soit partagée avec des tiers ;
- l'atténuation des risques de fuite, en permettant uniquement aux membres du personnel autorisés d'effectuer la collecte et la gestion des données émanant de sources confidentielles, et en s'assurant que ces personnes ont accès aux documents conformément aux directives applicables à la classification des informations.

Les membres du personnel doivent attribuer un degré de confidentialité aux données qu'ils traitent sur la base des directives applicables à la classification des informations et respecter la confidentialité des données qu'ils consultent, transmettent ou utilisent pour les besoins du traitement externe. Il est possible de revoir à tout moment le degré de confidentialité qui a initialement été attribué aux données, s'il y a lieu.

2.8.5 PLAN D'URGENCE

Le responsable du traitement est chargé d'établir et de mettre en œuvre un plan pour la protection, l'évacuation ou la destruction sécurisée des données en cas d'urgence.

2.8.6 MÉTHODES DE DESTRUCTION

Lorsqu'il est établi que la conservation des données personnelles n'est plus nécessaire, toutes les données et sauvegardes doivent être rendues anonymes ou détruites en toute sécurité. La méthode de destruction à privilégier dépend notamment des facteurs suivants :

- nature et sensibilité des données personnelles ;
- format et support d'enregistrement ;
- volume des enregistrements papier et électronique.

Préalablement à la destruction, le responsable du traitement doit évaluer la sensibilité des données personnelles à éliminer afin de s'assurer que les méthodes de destruction utilisées sont appropriées. Sur ce point, les trois paragraphes suivants reposent sur des informations extraites du Manuel de l'OIM sur la protection des données⁴⁵.

Les documents papier doivent être détruits par des méthodes telles que le déchiquetage ou l'incinération, de manière à empêcher toute utilisation ou reconstitution future. S'il est décidé que les documents papier doivent être convertis en enregistrements numériques, toute trace des documents papier doit être détruite après leur conversion fidèle au format électronique, sauf si la législation nationale applicable exige de conserver des documents papier ou si une copie papier doit être conservée à des fins d'archivage. La destruction d'importants volumes de documents papier peut être confiée à des entreprises spécialisées. Dans ces circonstances, le responsable du traitement doit veiller à ce que les intervenants, et ce, tout au long de la chaîne de responsabilité, s'engagent à respecter la confidentialité des données personnelles et à ce que la production des registres et des certificats de destruction fasse partie des obligations contractuelles incombant aux sous-traitants, et que ces derniers les respectent.

La destruction des données électroniques doit être confiée au personnel des services informatiques compétent car les fonctionnalités d'effacement des systèmes informatiques n'assurent pas nécessairement une suppression complète des données. Sur instruction, le personnel informatique compétent doit veiller à supprimer toute trace de données personnelles des systèmes informatiques et autres logiciels. Les disques et applications de bases de données doivent être purgés et tous les médias réinscriptibles, comme les CD, les DVD, les microfiches, les bandes vidéo et audio qui sont utilisés pour enregistrer des données personnelles, doivent être effacés avant d'être réutilisés. Les mesures physiques de destruction des données électroniques comme le recyclage, la pulvérisation ou l'incinération doivent être strictement surveillées.

⁴⁵ OIM, *IOM Data Protection Manual*, 2010, p. 83-84 : <https://publications.iom.int/books/iom-data-protection-manual>.

Le responsable du traitement doit veiller à ce que tous les contrats de service, protocoles d'accord, conventions et contrats écrits de transfert ou de traitement prévoient une durée de conservation avant la destruction des données personnelles une fois la finalité spécifiée atteinte. Les tiers doivent restituer les données personnelles au responsable du traitement et certifier que toutes les copies en ont été détruites, y compris celles qui ont été communiquées à leurs mandataires et sous-traitants. Il est nécessaire de tenir des registres de destruction indiquant la date et la méthode de destruction ainsi que la nature des documents détruits, et de les joindre aux rapports de projet ou d'évaluation.

2.8.7 AUTRES MESURES

La sécurité des données exige en outre des mesures organisationnelles internes appropriées, notamment la diffusion régulière à tous les employés des règles en matière de sécurité des données et des obligations qui leur incombent en vertu de la législation sur la protection des données ou des règles internes pour les organisations bénéficiant de privilèges et d'immunités, en particulier en matière de confidentialité.

Chaque responsable du traitement doit attribuer la fonction de responsable de la sécurité des données à un ou plusieurs membres de son personnel (éventuellement Administration ou Informatique) pour exécuter les opérations de sécurité. Le responsable de la sécurité doit notamment :

- veiller au respect des procédures et des règles de sécurité applicables ;
- mettre à jour ces procédures, le cas échéant ;
- animer des formations sur la sécurité des données à l'intention du personnel.

2.9 LE PRINCIPE DE RESPONSABILITÉ

Le principe de responsabilité repose sur l'obligation qui incombe aux responsables du traitement de respecter les principes ci-dessus et de démontrer que des mesures adéquates et proportionnées ont été prises au sein de leur organisation respective pour lesdits principes soient effectivement respectés.

Ces mesures, toutes fortement recommandées pour permettre aux organisations humanitaires de respecter les exigences de protection des données, peuvent être les suivantes :

- élaboration de politiques de traitement des données personnelles (y compris de politiques relatives à la sécurité du traitement) ;
- tenue de registres internes des activités de traitement de données ;
- création d'un organe indépendant chargé de superviser l'application des règles en matière de protection des données, comme le bureau de la protection des données, et nomination d'un responsable de la protection des données ;

- organisation de formations à la protection des données à l'intention de l'ensemble du personnel ;
- AIPD⁴⁶ ;
- enregistrement auprès des autorités compétentes (autorités de protection des données comprises) si la loi l'exige et si ce n'est pas incompatible avec le principe « ne pas nuire ».

2.10 INFORMATION

Conformément au principe de transparence, les personnes concernées doivent recevoir des informations relatives au traitement de leurs données personnelles. En principe, ces informations doivent être fournies avant que leurs données personnelles soient traitées, mais il est possible de déroger à cette règle s'il faut apporter une aide d'urgence.

Les personnes concernées doivent être informées oralement ou par écrit, de manière aussi transparente que la situation le permet et, si possible, directement. Si c'est impossible, l'organisation humanitaire doit envisager de diffuser les informations par d'autres moyens, par exemple, en ligne, par le biais de prospectus ou d'affiches qui se présentent sous un format et sont placées dans des lieux faciles d'accès (espaces publics, marchés, lieux de culte et bureaux des organisations), par communication radio ou en discutant avec des représentants de la communauté. Dans la mesure du possible, les personnes concernées doivent être tenues informées des modalités et des finalités du traitement de leurs données personnelles réalisé pour leur compte et des résultats qui s'ensuivent.

Les informations données peuvent varier, selon que les données sont recueillies directement auprès de la personne concernée ou non.

2.10.1 DONNÉES RECUEILLIES AUPRÈS DE LA PERSONNE CONCERNÉE

Les données personnelles peuvent être recueillies directement auprès de la personne concernée en vertu des fondements juridiques suivants⁴⁷ :

- l'intérêt vital de la personne concernée ou d'une autre personne ;
- l'intérêt public ;
- le consentement individuel ;
- l'intérêt légitime de l'organisation humanitaire ;
- une obligation légale ou contractuelle.

⁴⁶ Voir [chapitre 5 : Analyses d'impact relatives à la protection des données](#).

⁴⁷ Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

Les circonstances déterminent les informations à fournir aux personnes concernées dans chacun de ces cas. La priorité à cet égard est de fournir suffisamment d'informations aux personnes concernées pour leur permettre d'exercer effectivement leurs droits à la protection des données⁴⁸.

2.10.2 NOTICES D'INFORMATION

Dans les cas particuliers où le consentement peut constituer une base juridique⁴⁹, la personne doit pouvoir apprécier pleinement les risques et les avantages du traitement des données; dans le cas contraire, le consentement risque de ne pas être considéré comme valable.

Des informations précises doivent être données lorsqu'il est fait recours au consentement ou que les personnes concernées exercent leur droit d'opposition au traitement ou leurs droits d'accès, de rectification et de suppression des données. Il convient de souligner que la personne concernée peut s'opposer au traitement ou retirer son consentement à tout moment. Lorsque le consentement de la personne concernée constitue une base juridique, il est nécessaire de lui fournir les informations suivantes :

- l'identité et les coordonnées du responsable du traitement;
- la finalité précise du traitement de ses données personnelles et une explication des risques et des avantages potentiels;
- la possibilité de traiter ses données personnelles pour d'autres finalités que celles qui ont été initialement spécifiées à la date de la collecte si elles sont compatibles avec l'une des finalités mentionnées plus haut, avec indication de ces autres finalités compatibles;
- la possibilité de retirer son consentement à tout moment;
- les circonstances dans lesquelles il pourrait être impossible de traiter ses données personnelles de manière confidentielle;
- les droits d'accès, d'opposition, de rectification et de suppression auxquels elle peut prétendre, la manière d'exercer ses droits et les limites éventuelles à cet égard;
- le ou les pays tiers ou organisations internationales auxquels le responsable du traitement pourra avoir besoin de transférer les données pour atteindre la finalité de la collecte initiale et du traitement ultérieur;
- la durée pendant laquelle les données personnelles seront conservées ou au moins les critères permettant de déterminer cette durée, ainsi que les mesures prises pour s'assurer que les données sont exactes et à jour;
- les autres organisations, telles que les autorités du pays de collecte des données, avec lesquelles ses données personnelles peuvent être échangées;

⁴⁸ Voir [section 2.11: Droits des personnes concernées](#).

⁴⁹ Voir [section 3.2: Consentement](#).

- des informations sur la logique sous-jacente, si des décisions sont prises sur la base d'un traitement automatisé;
- les mesures de sécurité prises par le responsable du traitement en ce qui concerne le traitement des données.

En vertu des autres fondements juridiques du traitement, le responsable du traitement doit effectuer une analyse des risques, et des informations plus élémentaires sont suffisantes. Lorsque le consentement de la personne concernée ne constitue pas une base juridique, il est recommandé de lui fournir au moins les informations suivantes :

- l'identité et les coordonnées du responsable du traitement ;
- la finalité précise du traitement de ses données personnelles ;
- la ou les personnes à contacter pour toute question concernant le traitement de ses données personnelles ;
- les parties avec lesquelles les données seront échangées, en particulier si elles peuvent être échangées avec les autorités (les forces de l'ordre, par exemple) ou des entités présentes sur un autre territoire ou dans un autre État.

D'autres informations doivent être fournies, si nécessaire, à la demande de la personne concernée ou pour lui permettre de donner son consentement et d'exercer ses droits d'accès, d'opposition, de rectification et de suppression des données⁵⁰.

À titre exceptionnel, lorsque, en raison de contraintes logistiques et sécuritaires, notamment de difficultés d'accès au terrain, il n'est pas possible de fournir ces informations immédiatement ou sur le lieu où se trouvent les individus, ou que les données n'ont pas été collectées directement auprès des personnes concernées, les informations doivent être mises à disposition dès que possible dans un format facile d'accès et aisément compréhensible⁵¹. Les organisations humanitaires doivent aussi s'abstenir de recueillir de nombreuses données auprès des bénéficiaires jusqu'à ce que ces informations puissent être fournies de manière adéquate, sauf si elles sont absolument nécessaires pour des finalités humanitaires.

2.10.3 DONNÉES NON RECUEILLIES AUPRÈS DE LA PERSONNE CONCERNÉE

Lorsque les données personnelles n'ont pas été recueillies auprès de la personne concernée, les informations indiquées à la section 2.10.2 ci-dessus, en fonction de la base juridique utilisée pour collecter les données, doivent être données à la personne concernée dans un délai raisonnable après l'obtention de ces données compte tenu des circonstances précises de leur traitement ou, s'il est envisagé de les divulguer à un autre destinataire, au plus tard lorsqu'elles sont divulguées pour la première fois, sous réserve de contraintes logistiques et sécuritaires. Cette

⁵⁰ Voir [section 2.10 : Information](#), et [section 3.2 : Consentement](#).

⁵¹ Voir [section 2.10 : Information](#).

exigence ne s'applique pas si la personne concernée possède déjà les informations nécessaires ou si la transmission de données est impossible ou demanderait un effort disproportionné, auquel cas il convient de tenir compte des mesures énoncées ci-dessus, à la section 2.10 : Information.

EXEMPLE :

Des informations peuvent être fournies après avoir obtenu les données, par exemple, lorsqu'une intervention de protection concernant de multiples victimes est documentée et que les informations sont recueillies auprès de l'une d'entre elles seulement ou auprès d'une source tierce, ou lorsque des listes de personnes déplacées sont obtenues auprès d'autorités ou d'autres organisations pour la distribution de l'aide.

2.11 DROITS DES PERSONNES CONCERNÉES

2.11.1 INTRODUCTION

Le respect des droits des personnes concernées est un élément clé de la protection des données. Toutefois, comme il est expliqué ci-dessous, l'exercice de ces droits est assorti de conditions et peut être limité.

Une personne doit pouvoir exercer ces droits en utilisant les procédures internes de l'organisation humanitaire concernée, par exemple en adressant une demande d'informations ou une réclamation au responsable de la protection des données de l'organisation. Toutefois, en fonction du droit applicable et lorsque le responsable du traitement n'est pas une organisation internationale bénéficiant de l'immunité de juridiction, la personne peut aussi avoir le droit de former un recours en justice ou auprès d'une autorité de protection des données. Dans le cas des organisations internationales, les recours peuvent être formés devant un organe équivalent chargé de l'examen indépendant des dossiers pour l'organisation⁵².

2.11.2 DROIT D'ACCÈS

Les personnes concernées doivent pouvoir présenter une demande d'accès orale ou écrite à l'organisation humanitaire. Elles doivent pouvoir examiner et vérifier leurs données personnelles. L'exercice de ce droit peut être restreint si la protection des droits et des libertés d'autres personnes le requiert ou si cela s'avère nécessaire pour documenter des violations présumées du droit international humanitaire ou du droit des droits humains.

⁵² Voir Commission de contrôle des fichiers d'INTERPOL : <https://www.interpol.int/fr/Qui-nous-sommes/Commission-de-contrôle-des-fichiers-d-INTERPOL-CCF> et Commission de protection des données du CICR : <https://www.icrc.org/fr/document/icrc-data-protection-commission>.

En tenant dûment compte de la situation et des contraintes de sécurité, les personnes concernées doivent avoir la possibilité d'obtenir, de la part de l'organisation humanitaire, confirmation que leurs données personnelles sont ou non traitées, et ce, à intervalles raisonnables et gratuitement. Lorsque des données personnelles sont traitées, les personnes concernées doivent pouvoir y accéder, sauf dans les cas prévus ci-dessous.

Le personnel de l'organisation humanitaire ne doit donner aucune information sur les personnes concernées, sauf si celles-ci ou leur représentant autorisé lui présentent une preuve d'identité suffisante.

L'accès aux documents peut être refusé lorsque des intérêts prioritaires l'exigent. Une organisation humanitaire peut donc refuser l'accès aux données à une personne concernée si l'intérêt public ou les intérêts d'autres personnes l'emportent. C'est notamment le cas lorsqu'il est impossible de donner accès aux données sans révéler les données personnelles d'autres personnes, excepté lorsque toute référence à autrui peut être effacée du document ou des informations sans effort disproportionné ou lorsque le consentement à la divulgation est obtenu auprès de la ou des personnes concernées, là encore sans effort disproportionné.

Un accès qui compromettrait la capacité d'une organisation humanitaire à poursuivre les objectifs de son action humanitaire ou qui engendre des risques pour la sécurité de son personnel constitue toujours un intérêt prioritaire. Ce peut être également le cas pour les documents internes des organisations humanitaires, dont la divulgation peut nuire à l'action humanitaire. Dans ce cas, l'organisation humanitaire s'efforce, dans la mesure du possible et compte tenu des circonstances actuelles, de documenter la nature des intérêts prioritaires.

La communication aux personnes concernées des informations énoncées dans cette section doit être intelligible, ce qui signifie que l'organisation humanitaire peut avoir à fournir des traductions ou à expliquer plus précisément le processus de traitement aux personnes concernées. À titre d'exemple, il ne suffit pas, en général, de citer des abréviations techniques ou des termes médicaux en réponse à une demande d'accès, même si seuls ces abréviations ou termes sont enregistrés.

Il peut être opportun de divulguer des données personnelles aux membres de la famille ou aux représentants légaux lorsque les personnes concernées sont portées disparues, inconscientes ou décédées ou lorsque leur famille demande l'accès à leurs données pour des raisons humanitaires ou administratives ou dans le cadre de recherches sur les antécédents familiaux. Là encore, le personnel des organisations humanitaires ne doit révéler aucune information sauf si le demandeur apporte la preuve suffisante de son identité, de son statut de représentant légal ou de son lien de parenté, le cas échéant, et qu'il a déployé tous les efforts raisonnables pour attester de la validité de la demande.



O. Saltbones/CICR

Pristina (Kosovo)*. Fleurs fraîches accrochées aux photographies de personnes disparues depuis la fin de la guerre en 1999.

2.11.3 DROIT DE RECTIFICATION

La personne concernée doit aussi pouvoir s'assurer que l'organisation humanitaire rectifie les données personnelles inexactes qui la concernent. Compte tenu des finalités pour lesquelles les données ont été traitées, la personne concernée doit pouvoir rectifier des données personnelles incomplètes, par exemple en donnant des informations complémentaires.

Lorsque la demande de rectification porte simplement sur des données factuelles (correction de la graphie d'un nom, modification d'une adresse ou d'un numéro de téléphone, par exemple), la preuve de l'inexactitude n'est pas toujours indispensable. Si, en revanche, la demande a trait aux constatations ou aux dossiers d'une organisation humanitaire (comme l'identité légale de la personne concernée, son lieu de résidence pour la remise d'actes juridiques, ou des données plus sensibles sur son statut humanitaire ou son état de santé), le responsable du traitement devra peut-être exiger la preuve de l'inexactitude alléguée et apprécier la crédibilité de l'allégation. Ces demandes ne doivent pas faire peser sur la personne concernée une charge de la preuve excessive qui l'empêcherait de faire rectifier ses données. En outre, avant d'effectuer toute rectification, le personnel de l'organisation humanitaire doit demander une preuve d'identité suffisante aux personnes concernées ou à leur représentant.

* Résolution 1244 du Conseil de sécurité des Nations Unies.

2.11.4 DROIT DE SUPPRESSION

Une personne doit avoir la possibilité que ses données personnelles soient supprimées des bases de données de l'organisation humanitaire dans les circonstances suivantes :

- les données ne sont plus nécessaires aux finalités de leur collecte, de leur traitement ou de leur traitement ultérieur ;
- la personne concernée a retiré son consentement au traitement et il n'existe aucune autre base juridique pour le traitement des données⁵³ ;
- la personne concernée s'oppose avec succès au traitement des données personnelles qui la concernent⁵⁴ ;
- le traitement ne respecte pas la législation, la réglementation et les politiques en matière de protection des données et de respect de la vie privée.

L'exercice de ce droit peut être limité si cette restriction est nécessaire pour protéger la personne concernée ou les droits et libertés d'autres personnes ; pour documenter des violations présumées du droit international humanitaire ou du droit des droits humains ; pour des raisons d'intérêt public dans le domaine de la santé publique ; pour se conformer à une obligation légale applicable ; pour établir, exercer ou défendre un droit en justice ; ou pour des finalités historiques ou de recherche légitimes, sous réserve de garanties appropriées et de la prise en compte des risques pour la personne concernée et de ses intérêts. L'intérêt de conserver des archives constituant le patrimoine commun de l'humanité peut être un motif valable. En outre, avant d'effectuer toute rectification, le personnel de l'organisation humanitaire doit demander une preuve d'identité confirmant que les personnes concernées sont celles qu'elles prétendent être.

EXEMPLE :

Une organisation humanitaire soupçonne qu'une demande de suppression des données est présentée sous la pression d'un tiers et que la suppression des données empêcherait de protéger la personne concernée ou de documenter une violation présumée du droit international humanitaire ou du droit des droits humains. Dans ce cas, l'organisation humanitaire serait fondée à refuser de supprimer les données en question.

2.11.5 DROIT D'OPPOSITION

Les personnes ont le droit de s'opposer à tout moment, pour des raisons légitimes impérieuses tenant à leur situation particulière, au traitement des données personnelles qui les concernent.

L'exercice de ce droit peut être restreint, au besoin, si l'organisation humanitaire évoque des raisons légitimes impérieuses quant au traitement, qui l'emportent sur les intérêts, droits et libertés de la personne concernée (par exemple, protection de

⁵³ Voir [section 3.2: Consentement](#).

⁵⁴ Voir [section 3.4: Motifs importants d'intérêt public](#), et [section 3.5: Intérêt légitime](#).

la personne concernée ou des droits et libertés d'autres personnes ; documentation des violations présumées du droit international humanitaire ou du droit des droits humains ; établissement, exercice ou défense d'un droit en justice ; finalités historiques ou de recherche légitimes, sous réserve de garanties appropriées et de la prise en compte des risques pour la personne concernée et de ses intérêts). Dans ce cas, l'organisation humanitaire doit :

- informer son responsable de la protection des données, s'il y en a un ;
- informer si possible la personne concernée de son intention de poursuivre le traitement des données sur cette base ;
- informer si possible la personne concernée de son droit à demander la révision d'une de ses décisions par le responsable de la protection des données, l'autorité étatique ou le tribunal compétent, ou par l'organe équivalent dans le cas des organisations internationales.

En outre, avant d'accepter une opposition, le personnel de l'organisation humanitaire doit demander une preuve d'identité confirmant que les personnes concernées sont bien celles qu'elles prétendent être.

2.12 PARTAGE DE DONNÉES ET TRANSFERT INTERNATIONAL DE DONNÉES

Les urgences humanitaires exigent régulièrement que les organisations humanitaires partagent des données personnelles avec des sous-traitants et des tiers, y compris ceux qui sont basés dans d'autres pays, ou avec des organisations internationales. Le droit de la protection des données limite le partage des données personnelles avec des tiers et leur accès à ce type de données, en particulier dans le cas des transferts par-delà les frontières et les juridictions. D'autre part, de nombreuses lois sur la protection des données limitent le transfert international de données, c'est-à-dire tout acte consistant à rendre des données personnelles accessibles hors du pays dans lequel elles ont été initialement recueillies ou traitées, ainsi qu'à une entité différente au sein de la même organisation humanitaire n'ayant pas le statut d'organisation internationale, ou à un tiers, par voie électronique, par Internet ou par d'autres moyens⁵⁵.

Le partage de données exige de tenir dûment compte de toutes les conditions énoncées dans ce manuel. Par exemple, puisque le partage de données est une forme de traitement, il doit avoir une base juridique et il ne peut intervenir que pour la finalité particulière de la collecte initiale ou du traitement ultérieur. En outre, les personnes ont des droits en ce qui concerne le partage des données qui les concernent et elles doivent recevoir des informations à cet égard. Les conditions régissant le transfert international de données sont précisées au [chapitre 4 : Transfert international de données](#).

⁵⁵ Voir [chapitre 4 : Transfert international de données](#).

CHAPITRE 3

FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

3.1 INTRODUCTION

En vertu du principe de licéité du traitement des données énoncé au [chapitre 2: Principes fondamentaux de la protection des données](#), les opérations de traitement des données personnelles doivent avoir une base juridique légitime.

Dans le cadre de leurs activités humanitaires, les organisations humanitaires peuvent prendre s'appuyer sur les fondements juridiques suivants pour traiter des données personnelles :

- l'intérêt vital de la personne concernée ou d'une autre personne ;
- l'intérêt public ;
- le consentement ;
- l'intérêt légitime ;
- l'exécution d'un contrat ;
- le respect d'une obligation légale.

Dans les situations d'urgence dans lesquelles elles sont généralement appelées à intervenir, il peut être difficile pour les organisations humanitaires de satisfaire aux conditions essentielles de validité du consentement, qui doit notamment être éclairé et donné librement. C'est notamment le cas lorsque le consentement au traitement des données personnelles est une condition préalable pour pouvoir bénéficier d'une assistance, ou encore dans le domaine des ressources humaines, si le consentement est une condition lors du recrutement par exemple.

Le traitement opéré par les organisations humanitaires peut souvent se fonder sur un intérêt vital ou sur des motifs importants d'intérêt public⁵⁶ et, par exemple, intervenir dans le cadre de l'exécution d'un mandat conféré par le droit national ou international. Il faut pour cela que soient remplies les conditions suivantes :

- en cas d'intérêt vital, disposer d'éléments suffisants pour considérer que si les données d'une personne ne sont pas traitées, celle-ci pourrait être exposée à un préjudice physique ou moral. S'agissant des motifs importants d'intérêt public, être certain que l'opération de traitement envisagée relève du mandat confié à l'organisation humanitaire en vertu du droit national, régional ou international, ou que l'organisation humanitaire effectue une tâche ou remplit une fonction spécifique qui sert l'intérêt public et est prévue par la loi ;
- donner à la personne concernée des informations claires sur l'opération de traitement envisagée ;
- veiller à ce que la personne ait son mot à dire et puisse exercer son droit d'opposition⁵⁷. Dans tous les cas, la possibilité de s'opposer au traitement doit être donnée au plus tôt et le plus clairement possible, de préférence au moment de la collecte des données. Si la personne concernée justifie de manière

⁵⁶ Voir [section 3.3: Intérêt vital](#), et [section 3.4: Motifs importants d'intérêt public](#).

⁵⁷ Voir [chapitre 2: Principes fondamentaux de la protection des données](#).

adéquate son opposition au traitement et si ce traitement n'est pas nécessaire en vertu de toute autre base juridique (par exemple, [section 3.3: Intérêt vital](#), ou [section 3.4: Motifs importants d'intérêt public](#)), il convient de mettre fin au traitement de ses données personnelles.

Le fait de s'appuyer sur une base juridique appropriée n'exonère pas l'organisation humanitaire de son obligation d'évaluer le risque que comportent la collecte, l'enregistrement ou l'utilisation de données personnelles pour une personne, un groupe ou l'organisation elle-même. Lorsque les risques sont particulièrement élevés, elle doit déterminer s'il n'est pas simplement préférable de ne pas collecter ni traiter les données. Il existe deux cas de figure : soit, de par son expérience, l'organisation humanitaire pourra immédiatement identifier ces risques, soit la complexité des flux de données inhérents à une nouvelle solution technologique masquera ces risques. L'analyse d'impact relative à la protection des données (AIPD) demeure donc un outil essentiel pour détecter et atténuer les risques⁵⁸.

3.2 CONSENTEMENT

Le consentement constitue la base juridique la plus courante du traitement des données personnelles, et la plus souvent privilégiée. Cependant, étant donné la vulnérabilité de la plupart des bénéficiaires et la nature des urgences humanitaires, de nombreuses organisations humanitaires ne sont pas en mesure de s'appuyer sur le consentement pour la plupart de leurs opérations de traitement de données personnelles. Il convient dès lors de choisir une autre base juridique dans les situations suivantes :

- lorsque la personne concernée n'est pas physiquement en mesure d'être informée et de donner son consentement libre, par exemple parce qu'elle est portée disparue ou qu'elle est inconsciente ;
- lorsque les conditions logistiques et sécuritaires qui prévalent dans la zone des opérations ne permettent pas à l'organisation humanitaire d'informer les personnes concernées et d'obtenir leur consentement ;
- lorsque l'ampleur de l'opération à réaliser empêche l'organisation humanitaire d'informer les personnes concernées et d'obtenir leur consentement. Ce peut être le cas i) lorsqu'on établit des listes en vue de la distribution de l'assistance humanitaire à de nombreuses personnes déplacées ou ii) lorsque les autorités donnent aux organisations humanitaires une liste de personnes protégées en vertu d'une disposition découlant du droit international humanitaire ou du droit des droits humains ;
- lorsque le consentement de la personne concernée n'est pas considéré comme valable par l'organisation, par exemple parce que la personne est particulièrement vulnérable (enfants, personnes âgées ou handicapées, etc.)

58 Voir [chapitre 2: Principes fondamentaux de la protection des données](#).

au moment de donner son consentement ou que la situation de nécessité et de vulnérabilité dans laquelle elle se trouve (par exemple, absence d'alternative à l'assistance proposée et au traitement des données qu'elle implique) ne lui laisse pas véritablement le choix de refuser son consentement ;

- lorsque de nouvelles technologies sont en jeu, lesquelles impliquent des flux de données complexes et de nombreuses parties prenantes, ainsi que des sous-traitants et des sous-traitants ultérieurs situés dans plusieurs États. Dans cette situation, une personne a du mal à apprécier pleinement les risques et les avantages d'une opération de traitement et donc à en assumer la responsabilité à travers son consentement. D'autres fondements juridiques, qui exigent que les organisations humanitaires prennent davantage de responsabilités relatives à l'analyse des risques et des avantages du traitement, seraient alors plus appropriés.

Il convient de souligner qu'obtenir le consentement et donner des informations sur le traitement des données sont deux choses différentes ([section 2.10 : Information](#)), c'est-à-dire que même lorsque le consentement ne peut pas être utilisé, l'obligation d'information demeure, y compris sur les droits d'opposition, de suppression, d'accès et de rectification.

Les paragraphes qui suivent précisent les conditions à remplir pour que le consentement soit valable.

3.2.1 CONSENTEMENT UNIVOQUE

Le consentement doit être parfaitement éclairé et donné librement par toute méthode appropriée. Par conséquent, la personne concernée doit signifier qu'elle accepte que ses données personnelles fassent l'objet d'un traitement. Le consentement peut être donné par écrit ou, lorsque c'est impossible, à l'oral ou par tout autre acte positif clair de la part de la personne concernée (ou de son représentant légal, le cas échéant).

3.2.2 MOMENT

Le consentement doit être obtenu au moment de la collecte ou dès qu'il est raisonnablement possible de l'obtenir.

3.2.3 VALIDITÉ

On ne doit pas considérer que le consentement a été donné librement si la personne concernée ne peut réellement ni librement choisir, si elle est incapable de refuser ou de retirer son consentement sans subir aucun préjudice ou si les informations qui lui ont été données sont insuffisantes pour lui permettre de comprendre les conséquences du traitement de ses données personnelles.

3.2.4 VULNÉRABILITÉ

La vulnérabilité de la personne concernée doit être prise en compte pour juger de la validité du consentement. L'évaluation de la vulnérabilité suppose de comprendre les normes sociales, culturelles et religieuses du groupe dont sont membres les personnes concernées et de veiller à ce que chacune soit traitée individuellement comme le propriétaire de ses données personnelles. Le respect de l'individu implique que chaque personne soit considérée comme autonome, indépendante et libre de faire ses propres choix.

La vulnérabilité dépend des circonstances. À cet égard, les facteurs suivants doivent être considérés⁵⁹ :

- les caractéristiques de la personne concernée (analphabétisme, handicap, âge, état de santé, sexe, orientation sexuelle, etc.);
- le lieu où se trouve la personne concernée, (centre de détention, camp de réinstallation, région isolée, etc.);
- les facteurs, environnementaux et autres, (environnement inconnu, langue et concepts étrangers, etc.);
- la position de la personne concernée par rapport aux autres (par exemple, appartenance à un groupe ou à une ethnie minoritaire);
- les normes sociales, culturelles et religieuses des familles, des communautés ou des autres groupes auxquels appartiennent les personnes concernées;
- la complexité de l'opération de traitement envisagée, en particulier si elle fait appel à de nouvelles technologies complexes.

EXEMPLE :

Une organisation humanitaire procède à l'évaluation d'une urgence humanitaire. Ce faisant, elle recueille des données sur les bénéficiaires potentiels, notamment sur les moyens d'existence et les vulnérabilités des ménages, afin de concevoir un programme d'assistance approprié, pouvant comprendre des volets nutrition, santé et protection, ce qui suppose de recueillir et de traiter de nombreuses données personnelles. L'organisation doit informer les personnes qu'elle interroge des finalités de la collecte des données, mais il ne serait pas pertinent que celle-ci repose sur leur consentement. En effet, ces personnes n'ont pas réellement la possibilité de donner leur consentement à la collecte des données parce qu'elles sont extrêmement vulnérables et n'ont pas véritablement d'autre choix que d'accepter l'opération de traitement, quelle qu'elle soit, qui est associée à l'acceptation de l'aide proposée. Il convient alors de rechercher une autre base juridique et de fournir les informations pertinentes, y compris la possibilité de s'opposer au traitement envisagé.

⁵⁹ OIM, *IOM Data Protection Manual*, 2010, p. 45-48 : <https://publications.iom.int/books/iom-data-protection-manual>.

3.2.5 ENFANTS

Les enfants forment une catégorie particulièrement vulnérable et leur intérêt supérieur est primordial dans toutes les décisions qui les concernent. Si le point de vue et l'opinion de l'enfant doivent être respectés à tout moment, il faut particulièrement veiller à déterminer s'il comprend parfaitement les risques et avantages associés au traitement de ses données personnelles et, le cas échéant, s'assurer qu'il puisse exercer son droit d'opposition et fournir un consentement valable. La vulnérabilité des enfants doit être appréciée en fonction de leur âge et de leur maturité.



P. Moore/CICR

Un enfant reçoit un message de sa famille au centre de transit et d'orientation CAJED* pour les enfants auparavant associés à des forces ou des groupes armés, Province du Nord-Kivu (République démocratique du Congo).

Le consentement d'un parent ou du représentant légal peut être nécessaire si l'enfant n'a pas la capacité juridique pour donner son consentement. À cette fin, il convient de :

- fournir des informations complètes au parent ou au représentant légal et obtenir sa signature, laquelle manifeste son consentement ;
- veiller à ce que la personne concernée soit clairement informée, et son point de vue pris en compte.

* CAJED (Concert d'actions pour jeunes et enfants défavorisés).

3.2.6 CONSENTEMENT ÉCLAIRÉ

Pour constituer une base juridique acceptable, le consentement doit être éclairé. Cela suppose que la personne concernée reçoive des explications dans un langage simple, sans jargon, qui lui permet de pleinement apprécier les circonstances, les risques et les avantages du traitement de ses données personnelles⁶⁰.

3.2.7 CONSENTEMENT DOCUMENTÉ

Lorsque le traitement repose sur le consentement de la personne concernée, il est important d'en garder trace afin de pouvoir démontrer qu'elle a consenti au traitement. On pourra à cet effet demander une signature ou une croix en présence de l'organisation humanitaire ou, dans le cas d'un consentement verbal, un document de l'organisation humanitaire attestant l'obtention du consentement. La pratique consistant à demander une empreinte digitale pour confirmer le consentement, qui n'est pas rare dans le monde humanitaire, est très problématique car cela peut revenir à recueillir des données biométriques ; elle doit donc être évitée. Pour une analyse des risques liés à la collecte de données biométriques, voir [chapitre 8 : Biométrie](#).

Lorsqu'on a recours au consentement, il est important d'enregistrer les limites ou conditions éventuelles de son utilisation et la finalité spécifique pour laquelle il est obtenu. Ces éléments doivent être également enregistrés dans toutes les bases de données utilisées par les organisations humanitaires pour traiter les données en question et doivent accompagner les données tout au long du traitement.

Lorsque le consentement n'a pas été enregistré ou qu'on ne trouve pas trace d'un consentement, le traitement des données ne doit pas être poursuivi (ce qui signifie que les données ne doivent pas non plus être transférées à un tiers s'il n'y a pas trace de consentement au transfert) sauf s'il est possible de le faire sur une autre base juridique que le consentement (par exemple, intérêt vital, intérêt légitime ou intérêt public).

3.2.8 REFUS OU RETRAIT DU CONSENTEMENT

Si les personnes concernées refusent expressément leur consentement, elles doivent être informées des implications de ce refus, y compris de l'effet qu'il peut avoir sur l'assistance que les organisations humanitaires et les tiers peuvent ou non apporter. Toutefois, s'il est impossible d'apporter une assistance en l'absence de consentement, ce dernier ne peut être envisagé comme une base juridique du traitement⁶¹.

⁶⁰ Voir [section 2.10 : Information](#).

⁶¹ Voir [section 3.2 : Consentement](#), quatrième point.

Les personnes concernées ont le droit, à tout moment du traitement des données, de s'opposer au traitement et de retirer leur consentement. Lorsqu'une organisation humanitaire soupçonne que le consentement est retiré sous la pression de tiers, elle pourra probablement poursuivre le traitement des données personnelles de la personne concernée sur une autre base, comme les intérêts vitaux en jeu (voir section 3.3 ci-dessous).

3.3 INTÉRÊT VITAL

Même lorsqu'il est impossible d'obtenir un consentement valable, il est possible de traiter les données personnelles si l'organisation humanitaire estime que le traitement des données est dans l'intérêt vital de la personne concernée ou d'une autre personne, c'est-à-dire qu'il est nécessaire pour protéger un intérêt essentiel pour la vie, l'intégrité, la santé, la dignité ou la sécurité de la personne concernée ou d'une autre personne.

Compte tenu de la nature de leur travail et des situations d'urgence dans lesquelles les organisations humanitaires sont appelées à intervenir, le traitement des données peut reposer sur l'intérêt vital d'une personne concernée dans les cas suivants :

- gestion de dossiers de personnes portées disparues ;
- aide apportée aux autorités pour identifier des restes humains ou rechercher les proches d'une personne décédée. Dans ce cas, les données personnelles seraient traitées dans l'intérêt vital de la famille ;
- aide apportée à un individu inconscient ou en danger, mais incapable d'exprimer son consentement ;
- assistance ou soins médicaux apportés ;
- le traitement, divulgation comprise, des informations est la mesure la plus appropriée face à une menace imminente contre l'intégrité physique et mentale des personnes concernées ou d'autres personnes ;
- le traitement est nécessaire pour pourvoir aux besoins essentiels d'un individu ou d'une communauté lors d'une urgence humanitaire ou immédiatement après.

Toutefois, dans de telles circonstances, l'organisation humanitaire doit veiller autant que possible à ce que les personnes concernées soient informées du processus de traitement dès que possible, à ce qu'elles aient suffisamment d'informations pour comprendre et apprécier les finalités spécifiées de la collecte et du traitement de leurs données personnelles et à ce qu'elles puissent s'opposer au traitement si elles le souhaitent. Pour ce faire, il est préférable de donner des explications directes au moment de l'enregistrement des bénéficiaires, de la collecte et des distributions d'aide, par exemple, au moyen d'affiches, de discussions collectives ou de brochures ou de sites Internet contenant des informations supplémentaires⁶².

⁶² Voir [section 2.5.1: Principes de licéité, de loyauté et de transparence du traitement](#), et [section 2.10: Information](#).

EXEMPLE :

Une organisation humanitaire a besoin de recueillir des données personnelles auprès d'individus vulnérables à la suite d'une catastrophe naturelle afin de fournir une aide vitale (nourriture, eau, assistance médicale, etc.). La collecte des données personnelles peut reposer sur les intérêts vitaux des individus sans qu'il soit besoin d'obtenir leur consentement. Toutefois, l'organisation humanitaire doit 1) veiller à utiliser cette base juridique exclusivement pour fournir une telle assistance, 2) donner un droit d'opposition aux individus et 3) traiter les données recueillies conformément à sa politique de protection de la vie privée et communiquer celle-ci aux personnes concernées qui en font la demande. Elle doit fournir toutes les informations pertinentes sur le traitement des données, par exemple, au moyen d'affiches ou d'explications collectives, ou de brochures ou de sites Internet contenant des informations complémentaires, au moment de l'enregistrement des bénéficiaires ou de la distribution d'aide.

3.4 MOTIFS IMPORTANTS D'INTÉRÊT PUBLIC

Des motifs importants d'intérêt public entrent en jeu lorsque l'activité en question relève d'un mandat humanitaire conféré par le droit national ou international ou qu'il s'agit d'une activité effectuée dans l'intérêt public et prévue par la loi. Ce serait le cas, par exemple, pour le CICR, le Fonds des Nations Unies pour l'enfance (UNICEF), le Haut Commissariat des Nations Unies pour les réfugiés (HCR), l'Organisation internationale pour les migrations (OIM), le Programme alimentaire mondial des Nations Unies (PAM), les Sociétés nationales de la Croix-Rouge ou du Croissant-Rouge et d'autres organisations humanitaires qui effectuent une tâche ou remplissent une fonction spécifique prévue par la loi, dans l'intérêt public, dans la mesure où le traitement des données personnelles est nécessaire à l'accomplissement de ces tâches⁶³. Le terme « nécessaire » doit être ici interprété au sens strict (c'est-à-dire que le traitement des données doit être réellement nécessaire et pas seulement commode⁶⁴ pour la finalité en question).

Cette base juridique peut être pertinente pour les distributions d'assistance, lorsqu'il est impossible d'obtenir le consentement de tous les bénéficiaires potentiels et qu'il n'est pas certain que la vie, la sécurité, la dignité et l'intégrité de la personne concernée ou d'autres personnes soient en jeu (auquel cas l'« intérêt vital » pourrait constituer la base juridique la plus appropriée pour le traitement).

⁶³ Le CICR, par exemple, possède un mandat en vertu des quatre Conventions de Genève et du Protocole additionnel I pour agir en cas de conflit armé international. Il a un droit d'intervention humanitaire dans les conflits armés non internationaux : <https://www.icrc.org/fr/notre-mandat-et-notre-mission>.

⁶⁴ Voir exemple à la [section 3.6 : Exécution d'un contrat](#).

Cette base juridique peut être également pertinente dans le cas du traitement des données personnelles de détenus, lorsque ce type d'activité relève du mandat de l'organisation humanitaire. Cela peut arriver, par exemple, lorsque le traitement des données personnelles a trait à des personnes privées de liberté en situation de violence, et notamment lors d'un conflit armé, lorsque l'organisation humanitaire n'a pas encore pu voir ces personnes et donc obtenir leur consentement et, par la suite, si le consentement n'est pas considéré comme une base juridique valable en raison de la vulnérabilité des personnes concernées.



Détenus de la prison centrale de Monrovia (Libéria).

Dans ces situations l'organisation humanitaire doit également, si possible, veiller à ce que les personnes concernées soient informées au plus tôt du traitement de leurs données personnelles, à ce qu'elles aient suffisamment d'informations pour comprendre et apprécier les finalités spécifiées de la collecte et du traitement, et à ce qu'elles puissent s'opposer au traitement à tout moment si elles le souhaitent.

3.5 INTÉRÊT LÉGITIME

Les organisations humanitaires peuvent également traiter des données personnelles lorsqu'elles y ont un intérêt légitime, en particulier lorsque c'est nécessaire pour l'accomplissement d'une activité humanitaire spécifique prévue dans le cadre de leur mission, et sous réserve que les droits et libertés fondamentaux de la personne concernée ne l'emportent pas sur cet intérêt. Dans toutes ces situations, le terme « nécessaire » doit être interprété au sens strict (c'est-à-dire que le traitement des données doit être réellement nécessaire et pas seulement commode⁶⁵ pour la finalité en question).

⁶⁵ Voir exemple à la [section 3.6 : Exécution d'un contrat](#).

On peut parler d'intérêt légitime dans les situations suivantes :

- le traitement est nécessaire à l'accomplissement effectif de la mission de l'organisation humanitaire lorsque aucun motif important d'intérêt public ne peut être invoqué ;
- le traitement est nécessaire pour garantir la sécurité des systèmes d'information et des informations⁶⁶ et celle des services connexes proposés, via ces systèmes d'information, par les autorités publiques, les équipes d'intervention informatique d'urgence (EIIU), les équipes d'intervention en cas d'incident de sécurité informatique (EISI), les fournisseurs de réseaux et de services de communications électroniques et les fournisseurs de technologies et de services de sécurité. Il peut s'agir par exemple de prévenir les accès non autorisés aux réseaux de communications électroniques et la diffusion de codes malveillants, de bloquer les attaques par « déni de service » et de prévenir les dommages aux systèmes informatiques et aux systèmes de communications électroniques ;
- le traitement est nécessaire pour prévenir, mettre en évidence et arrêter une fraude ou un vol ;
- le traitement est nécessaire pour l'anonymisation ou la pseudonymisation des données personnelles⁶⁷ ;
- le traitement est nécessaire pour établir, exercer ou défendre un droit en justice, dans une procédure judiciaire, administrative ou extrajudiciaire.

EXEMPLE :

Une organisation humanitaire traite des données personnelles lorsqu'elle scanne ses systèmes informatiques à la recherche de virus, qu'elle contrôle l'identité des bénéficiaires afin de lutter contre les fraudes et qu'elle se défend dans une procédure judiciaire intentée par un ancien salarié. Toutes ces activités de traitement sont autorisées sur la base de l'intérêt légitime de l'organisation.

⁶⁶ La sécurité de l'information peut comprendre la protection de la confidentialité, de l'intégrité et de la disponibilité des informations, ainsi que d'autres propriétés comme l'authenticité, l'imputabilité, la non-répudiation et la fiabilité. Voir ISO/IEC 17799:2005, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information* : <https://www.iso.org/fr/standard/39612.html>.

⁶⁷ Voir [section 2.3 : Ensembles de données agrégées, pseudonymisées et anonymisées](#). La pseudonymisation consiste à traiter les données personnelles de sorte qu'elles ne peuvent plus être attribuées à une personne précise sans informations complémentaires.

3.6 EXÉCUTION D'UN CONTRAT

Les organisations humanitaires peuvent traiter des données personnelles sur cette base juridique lorsque le traitement est nécessaire pour exécuter un contrat auquel la personne concernée est partie ou pour prendre des mesures, à la demande de la personne concernée, avant de conclure un contrat. Là encore, le terme « nécessaire » doit être interprété au sens strict (le traitement des données doit être réellement nécessaire et pas seulement commode pour atteindre la finalité en question).

C'est généralement le cas lorsque les données sont traitées pour l'une des finalités suivantes :

- la gestion des dossiers de ressources humaines, y compris le recrutement ;
- la gestion des relations avec les fournisseurs et les prestataires ;
- les relations avec les donateurs.

EXEMPLE :

Une organisation humanitaire conserve des dossiers personnels sur ses employés, conformément aux obligations qui lui incombent en tant qu'employeur à l'égard de son personnel. Elle y est autorisée pour exécuter ses obligations contractuelles vis-à-vis de son personnel. En revanche, si cette organisation a externalisé le traitement de ses données à un tiers établi dans le pays où se trouve son siège, autoriser ce tiers à accéder à ses bases de données n'est pas considéré comme nécessaire à l'exécution de son contrat avec l'entreprise car l'externalisation du traitement des données est un choix de commodité et non une nécessité. Dans ce cas, il conviendrait de déterminer si l'intérêt légitime de l'organisation pourrait constituer une base juridique appropriée.

3.7 RESPECT D'UNE OBLIGATION LÉGALE

Les organisations humanitaires peuvent traiter des données personnelles en se fondant sur cette base juridique, lorsque le traitement est nécessaire au respect d'une obligation légale qui leur incombe ou à laquelle elles se soumettent. Ce peut être le cas dans le domaine du droit du travail ou, pour les organisations qui ne bénéficient pas de privilèges et d'immunités, lorsque le traitement est nécessaire pour respecter une obligation légale.

EXEMPLE :

Dans les pays où elle intervient, une organisation humanitaire est tenue par la législation de fournir aux autorités chargées de la sécurité sociale et à l'administration fiscale des informations sur les salaires versés au personnel. Si l'organisation est assujettie à la juridiction nationale, la communication de ces informations se justifie par l'obligation légale à laquelle elle est soumise.

Cependant, étant donné l'environnement de travail des organisations humanitaires, certains facteurs doivent être pris en compte lorsqu'il est envisagé que le traitement repose sur une obligation légale. Les facteurs suivants seront en particulier pertinents lorsque les autorités exigent d'accéder aux données personnelles à des fins de répression, de renseignement ou autres :

- état de droit et séparation des pouvoirs dans le pays qui exige d'accéder aux données ;
- respect des droits humains, dont le droit à un recours judiciaire effectif ;
- existence d'un conflit armé ou d'une situation de violence, lorsque l'autorité qui exige d'accéder aux données peut représenter un parti ;
- nature des données et possibilité ou impossibilité d'en déduire des informations qui entraîneraient une discrimination ou des poursuites (exemple : si les données ou les noms relatifs aux besoins alimentaires révèlent une affiliation religieuse ou une origine ethnique, si les données de santé révèlent l'orientation sexuelle dans un pays où les homosexuels sont persécutés ou si la personne dont les données sont requises encourt la peine de mort) ;
- si l'organisation humanitaire bénéficie de privilèges et d'immunités, auquel cas l'obligation n'est pas applicable.

À cet égard, il convient également de souligner que les organisations humanitaires doivent déterminer si une obligation légale de divulgation des données à laquelle elles sont soumises risque d'exposer les personnes concernées à des mesures de discrimination, persécution, marginalisation ou répression, auquel cas elles doivent envisager de ne pas procéder à la collecte des données.

CHAPITRE 4

TRANSFERT INTERNATIONAL DE DONNÉES

4.1 INTRODUCTION

Les urgences humanitaires ne connaissent pas de frontières et font que les organisations humanitaires ont régulièrement besoin de procéder à des transferts internationaux de données vers d'autres entités pour mener à bien l'intervention qui s'impose; une circulation efficace des données personnelles entre les pays est donc essentielle pour le travail des organisations humanitaires. En outre, l'utilisation de nouvelles technologies dans le cadre des activités humanitaires implique la participation de nombreux sous-traitants et sous-traitants ultérieurs qui seront, presque inévitablement, établis dans d'autres pays que celui en proie à l'urgence humanitaire. Ce peut être le cas, par exemple, lorsque les organisations humanitaires recourent à des solutions basées sur le cloud pour traiter des données personnelles, auquel cas les données peuvent être hébergées sur le territoire du siège de l'organisation et les prestataires de services peuvent agir en qualité de sous-traitants et de sous-traitants ultérieurs depuis d'autres pays⁶⁸.



Camp de réfugiés de Nizip, près de la frontière syrienne, province de Gaziantep (Turquie), novembre 2016.

Comme l'explique la [section 2.4 : Droit applicable et organisations internationales](#), certaines organisations humanitaires sont des organisations internationales qui bénéficient de privilèges et d'immunités afin de pouvoir accomplir en toute indépendance le mandat que la communauté internationale leur a confié en vertu du droit international. En conséquence, elles traitent les données personnelles conformément à leurs règles internes, qui s'appliquent à l'ensemble de leurs

68 Voir [chapitre 10 : Services cloud](#).

activités, indépendamment du territoire dans lequel elles interviennent, et sous le contrôle de leurs propres systèmes de conformité. Elles constituent ainsi leur propre « juridiction » et les flux de données circulant au sein de ces organisations et de leurs entités subordonnées n'entrent pas dans le champ d'application de ce chapitre⁶⁹.

Exemples d'entités avec lesquelles une organisation humanitaire peut avoir besoin de partager des données à l'international :

- bureaux d'une même ONG opérant dans différents pays ;
- autres ONG, organisations internationales et organismes des Nations Unies ;
- autorités publiques ;
- sous-traitants, tels que des prestataires de services, des consultants ou des chercheurs, recueillant ou traitant des données personnelles pour le compte de l'organisation humanitaire ;
- établissements universitaires et chercheurs ;
- entreprises privées ;
- musées.

Le transfert international de données comprend tout acte consistant, par voie électronique, par Internet ou par d'autres moyens, à rendre accessibles des données personnelles dans un autre pays que celui dans lequel elles ont été initialement collectées ou traitées. La publication de données personnelles dans la presse, sur Internet ou par radiodiffusion est habituellement considérée comme un transfert de données si elle permet d'accéder aux données à l'international.

Le transfert international de données recouvre tout acte dont le résultat est le transfert, le partage ou l'accès à des données personnelles par-delà les frontières nationales ou avec des organisations internationales. On parle donc de transfert international de données dans les situations suivantes :

- L'organisation humanitaire transfère des données à une organisation située dans un autre pays. L'entité destinataire est un nouveau responsable du traitement, qui détermine les moyens et les finalités du traitement.
- L'organisation humanitaire transfère des données à une organisation située dans un autre pays, mais c'est elle qui décide des moyens et des finalités du traitement, tandis que l'entité destinataire ne traite les données personnelles que conformément à ses instructions. Dans ce cas, l'entité qui reçoit les données est un sous-traitant.

Le risque inhérent à ces deux scénarios est qu'une fois partagées, les données personnelles perdent tout ou partie de la protection dont elles bénéficiaient lorsqu'elles étaient traitées exclusivement par l'organisation humanitaire. Il est donc important, dans ces situations, que l'organisation qui partage les données

69 Voir [section 2.4 : Droit applicable et organisations internationales](#).

prenne toutes les mesures raisonnables pour éviter d'affaiblir involontairement la protection des données.

Il ne faut pas oublier que le partage de données est une opération de traitement et qu'à ce titre il est soumis à toutes les exigences énoncées dans les chapitres précédents⁷⁰. Les paragraphes qui suivent expliquent les précautions supplémentaires que les organisations humanitaires doivent prendre lorsqu'elles procèdent à un transfert international de données.

4.2 RÈGLES FONDAMENTALES APPLICABLES AU TRANSFERT INTERNATIONAL DE DONNÉES

Pour protéger le transfert international de données, toutes les mesures suivantes doivent être prises :

- les règles de protection des données et les obligations de respect de la vie privée applicables au partage de données⁷¹ (y compris celles prévues par la législation locale, si elle est applicable) ont été respectées préalablement au transfert ;
- Le transfert doit reposer sur une base juridique.
- Une évaluation doit être réalisée pour déterminer si le transfert présente ou non un risque inacceptable pour l'individu (discrimination, répression, etc.).
- L'organisation qui transfère les données doit pouvoir démontrer que l'entité destinataire a pris des mesures adéquates pour garantir le respect des principes de protection des données énoncés dans ce manuel et préserver le niveau de protection des données personnelles établi pour les transferts internationaux de données (responsabilité).
- L'individu doit être informé de l'identité des destinataires du transfert. Le transfert ne doit pas être incompatible avec les attentes raisonnables des personnes dont les données sont transférées.

4.3 FONDEMENT JURIDIQUE APPLICABLE AU TRANSFERT INTERNATIONAL DE DONNÉES

4.3.1 INTRODUCTION

Comme il est indiqué plus haut, ce manuel est conçu pour faciliter l'application et le respect des principes et droits relatifs à la protection des données dans les situations d'urgence humanitaire. Cependant, il ne remplace pas la législation nationale sur la protection des données lorsque celle-ci s'applique à une organisation humanitaire qui ne bénéficie pas des privilèges et immunités d'une organisation internationale,

⁷⁰ Voir [chapitre 2 : Principes fondamentaux de la protection des données](#), et [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

⁷¹ Voir [chapitre 2 : Principes fondamentaux de la protection des données](#).

et il ne donne pas de conseils sur son application. Il convient donc de souligner que les considérations abordées dans ce chapitre s'ajoutent aux autres exigences de la législation locale du pays communiquant les données, dans la mesure où elles s'appliquent à l'organisation humanitaire. Des dizaines de pays à travers le monde ont promulgué des lois sur la protection des données qui régissent le transfert international de données ; pour comprendre les obligations qui en découlent, l'organisation humanitaire doit consulter son bureau de la protection des données, son service juridique ou son conseiller juridique local.

4.3.2 FONDEMENTS JURIDIQUES DU TRANSFERT INTERNATIONAL DE DONNÉES

Le transfert international de données est autorisé :

- lorsque le transfert répond aux intérêts vitaux des personnes concernées ou d'autres personnes ;
- pour des motifs importants d'intérêt public, sur la base du mandat de l'organisation humanitaire ;
- lorsque le transfert des données est dans l'intérêt légitime de l'organisation humanitaire, sur la base de sa mission déclarée, que les droits et les libertés des personnes concernées ne l'emportent pas sur cet intérêt légitime et que l'organisation humanitaire a fourni des garanties appropriées pour les données personnelles ;
- avec le consentement de la personne concernée ;
- aux fins de l'exécution d'un contrat conclu avec la personne concernée.

L'application de ces fondements juridiques est similaire à leur application dans le cadre du traitement des données personnelles⁷². En outre, comme le transfert international de données comporte des risques supplémentaires, il convient de tenir compte des facteurs indiqués ci-après à la section « Atténuation des risques pour l'individu ».

4.4 ATTÉNUATION DES RISQUES POUR L'INDIVIDU

Dans le cadre d'un transfert international de données, il est important de tenir compte des facteurs suivants :

- Les risques peuvent être moindres si les données sont transférées à une organisation soumise à la juridiction d'un pays ou à une organisation internationale qui offrent une protection des données formellement jugée adéquate. Globalement, cela signifie que le destinataire des données se situe dans un pays dont le régime réglementaire de la protection des données, qui a été formellement jugé conforme à des normes internationales élevées, comprend une autorité de contrôle indépendante et garantit l'absence de

⁷² Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

surveillance de masse et l'accès à un recours judiciaire pour les individus. Cependant, il s'avère que les autorités publiques nationales ou régionales n'offrent une protection formelle adéquate que dans un petit nombre de pays. Les organisations humanitaires pourront donc rarement compter sur un constat d'adéquation. L'adéquation n'est pas un prérequis du transfert international de données, mais c'est un facteur à prendre en compte.

- Lorsque les moyens logistiques le permettent, des garanties appropriées doivent être prises pour le transfert international de données, par exemple, prévoir des clauses contractuelles obligeant le destinataire à offrir une protection des données appropriée ou vérifier que le destinataire s'est engagé à respecter un code de conduite sur la protection des données personnelles.
- L'organisation humanitaire doit rendre compte du transfert international de données qu'elle entreprend.

Ces deux facteurs sont étudiés plus amplement ci-dessous.

EXEMPLE :

Une ONG humanitaire a son siège dans le pays X et souhaite transférer à une autre ONG présente dans le pays Y des dossiers contenant des données personnelles sur des individus vulnérables auxquels elle fournit des services humanitaires. Elle mettra les dossiers à disposition de l'ONG du pays Y sur sa plateforme Internet sécurisée, et celle-ci pourra ainsi y accéder. Une évaluation formelle a conclu que les autorités publiques du pays Y offrent un niveau adéquat de protection des données. La mise à disposition de dossiers sur une plateforme Internet répond aux critères du transfert international de données, mais le transfert peut intervenir sur la base d'un niveau de protection adéquat dans le pays Y, sous réserve des autres considérations exposées ci-dessous à la section 4.4.1.

4.4.1 GARANTIES APPROPRIÉES/CLAUSES CONTRACTUELLES

Lorsqu'elle décide d'atténuer les risques liés au transfert international de données, une organisation humanitaire doit veiller à ce que le destinataire instaure des garanties appropriées pour protéger les données personnelles.

En pratique, ces garanties peuvent être apportées par un contrat, établi par l'organisation humanitaire elle-même ou inspiré d'autres sources internationalement reconnues, par lequel l'organisation et la partie à laquelle les données personnelles sont transférées s'engagent à protéger les données en question sur la base des normes de protection des données qui s'appliquent à l'organisation humanitaire.

La Commission européenne a publié des clauses contractuelles types pour les transferts opérés par les responsables du traitement à destination de responsables du traitement et de sous-traitants établis hors de l'Union européenne/Espace économique européen⁷³ à l'intention des organisations humanitaires qui sont soumises au droit de l'Union européenne sur la protection des données ou qui souhaitent utiliser ces clauses.

Lorsqu'on décide d'atténuer les risques, il convient également de déterminer si l'autre partie impliquée dans le partage des données s'est engagée à respecter un code de conduite couvrant le traitement des données personnelles⁷⁴ et dans quelle mesure ce code de conduite est effectivement appliqué, et s'il est contraignant et opposable ou non.

Même lorsqu'il existe une base juridique pour le transfert et que des mesures d'atténuation sont en place, le transfert international des données peut être inopportun pour les raisons suivantes :

- La nature des données peut exposer les personnes concernées à des risques.
- Il y a de bonnes raisons de penser que les parties qui reçoivent les données ne sont pas capables de garantir une protection adéquate.
- Étant donné les conditions qui prévalent dans le pays où les données doivent être envoyées, il est peu probable qu'elles seront protégées.
- Les données sont traitées sur la base d'une protection apportée par l'immunité de juridiction d'une organisation, et l'organisation destinataire des données ne bénéficie pas de cette immunité.

EXEMPLE :

Une organisation humanitaire qui est une organisation internationale ayant des bureaux dans le pays X souhaite transférer à une ONG située dans le même pays des fichiers contenant des données personnelles sur des individus vulnérables auxquels elle fournit des services humanitaires. Le transfert intervenant entre une organisation internationale et une organisation soumise à la juridiction du pays X, il s'agit d'un transfert international de données. L'organisation humanitaire signe des clauses contractuelles types avec l'ONG. Cependant, les locaux de l'ONG sont fortement exposés aux violentes attaques d'un groupe armé et il lui est déjà arrivé de perdre les données qui lui avaient été envoyées. L'organisation humanitaire doit sérieusement envisager de ne pas transférer les données, avec ou sans clause contractuelle.

⁷³ Voir Commission européenne, « Standard contractual clauses for data transfers between EU and non-EU countries » : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_fr.

⁷⁴ Voir par exemple, Réseau des liens familiaux du Mouvement international de la Croix-Rouge et du Croissant-Rouge, « Code de conduite relatif à la protection des données à caractère personnel » : <https://www.icrc.org/fr/document/le-code-de-conduite-en-matiere-de-protection-des-donnees-dans-le-cadre-du-retablissement>.

Pour détecter et résorber ou atténuer correctement ces risques, il convient d'effectuer une AIPD⁷⁵. En cas d'hésitation, le bureau de protection des données de l'organisation humanitaire doit être consulté.

4.4.2 RESPONSABILITÉ

Il est important que l'organisation humanitaire à l'origine du transfert puisse démontrer que des mesures adéquates et proportionnées ont été prises pour garantir le respect des principes fondamentaux de protection des données dans le cadre du transfert international de données. L'organisation humanitaire est responsable devant la personne concernée dont les données sont partagées. Il peut s'agir des mesures suivantes :

- tenue de dossiers internes relatifs au traitement des données et, en particulier, tenue d'un registre des transferts et conservation d'un exemplaire de l'accord de transfert conclu avec la partie à laquelle sont transférées les données personnelles, le cas échéant ;
- nomination d'un responsable de la protection des données ;
- élaboration de politiques de traitement des données personnelles, notamment d'une politique de sécurité des données ;
- exécution d'AIPD relatives au transfert et conservation des documents y afférents ;
- enregistrement du transfert auprès des autorités compétentes (à savoir les autorités de protection des données) si le droit applicable l'exige.

Pour tout transfert international de données, des mesures appropriées doivent être prises afin de sécuriser la transmission de données personnelles à des tiers. Le niveau de sécurité⁷⁶ assuré et le mode de transmission doivent être proportionnés à la nature et à la sensibilité des données personnelles ainsi qu'aux risques en jeu. Il est également conseillé d'examiner cet aspect dans toute AIPD afin de préciser les précautions à prendre.

⁷⁵ Voir [chapitre 5 : Analyses d'impact relatives à la protection des données](#).

⁷⁶ Voir [section 2.8 : Sécurité des données et du traitement](#).

4.5 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Si un responsable du traitement fait appel à un sous-traitant, établi ou non dans le même pays, leur relation doit être autant que possible régie par un contrat qui les oblige à protéger le traitement des données personnelles qu'ils partagent.

Afin de garantir une protection adéquate des données personnelles, les documents contractuels doivent notamment préciser les aspects suivants :

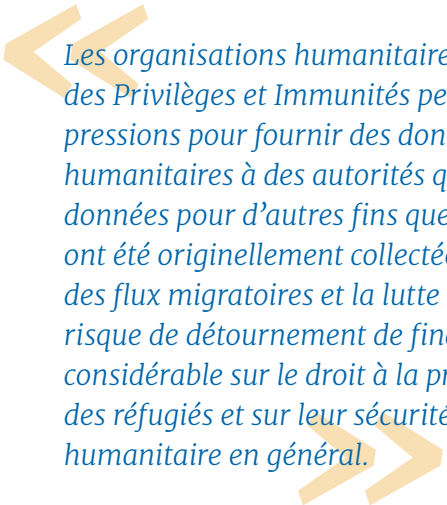
- si le sous-traitant est soumis à des obligations de conservation acceptables (les opérateurs de téléphonie mobile et les établissements financiers, par exemple, ont des obligations nationales de conservation des données) ;
- les autres types de données collectées par le sous-traitant dans le cadre du traitement (pour les opérateurs de téléphonie mobile, par exemple, données de géolocalisation et autres métadonnées téléphoniques) ;
- si le traitement des données personnelles effectué par le sous-traitant est conforme aux instructions du responsable du traitement ;
- ce que le sous-traitant fera des données personnelles une fois le traitement contractuel effectué.

4.6 DIVULGATION DES DONNÉES PERSONNELLES AUX AUTORITÉS

Pour les organisations humanitaires, divulguer et transférer des données personnelles aux autorités peut poser problème, en particulier lorsque ces dernières sont parties à un conflit ou impliquées dans d'autres situations de violence. Cette divulgation peut être contraire à une action humanitaire neutre, impartiale et indépendante, notamment si elle porte préjudice à une personne concernée compte tenu de sa situation humanitaire, ou lorsque le transfert compromettrait la sécurité de l'organisation ou son accès futur à des personnes touchées par un conflit armé ou des violences, aux parties à un conflit ou aux informations nécessaires pour accomplir son mandat.

Les organisations humanitaires qui ont le statut d'organisation internationale et qui bénéficient à ce titre de privilèges et d'immunités doivent veiller à ce que leur statut soit respecté et refuser d'accéder à de telles demandes sauf si cela est justifié dans l'intérêt supérieur des personnes concernées et de l'action humanitaire. Lorsqu'une organisation humanitaire bénéficiant de privilèges et d'immunités a besoin de transférer des données à des organisations humanitaires qui n'ont pas ces privilèges et immunités, le risque que le destinataire ne puisse pas s'opposer à

de telles demandes doit être pris en compte. Ce risque est expressément reconnu dans la Résolution de 2015 sur la protection des données personnelles et l'action humanitaire internationale de la Conférence internationale des commissaires à la protection des données et à la vie privée⁷⁷ :



Les organisations humanitaires qui ne bénéficient pas des Privilèges et Immunités peuvent faire l'objet de pressions pour fournir des données collectées à des fins humanitaires à des autorités qui souhaitent utiliser ces données pour d'autres fins que celles pour lesquelles elles ont été originellement collectées (par exemple le contrôle des flux migratoires et la lutte contre le terrorisme). Le risque de détournement de finalité peut avoir un impact considérable sur le droit à la protection des données des réfugiés et sur leur sécurité, ainsi que sur l'action humanitaire en général.

⁷⁷ ICDPPC, Résolution sur la protection des données personnelles et l'action humanitaire internationale, Amsterdam, 2015 : https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2015/11/resolution_sur_laprotectiondesdonneespersonnellesetlactionhumani.pdf.download.pdf/resolution_sur_laprotectiondesdonneespersonnellesetlactionhumani.pdf.

CHAPITRE 5

ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

5.1 INTRODUCTION

Le traitement des données personnelles peut accroître les risques auxquels sont exposés les individus, les groupes, les organisations, et la société en général. L'objet d'une analyse d'impact relative à la protection des données (AIPD)⁷⁸ est de détecter, d'évaluer et de gérer les risques pour les données personnelles – et en fin de compte, pour les personnes concernées – qui découlent d'un projet, d'une politique, d'un programme ou d'une autre initiative. Une AIPD doit conduire à prendre des mesures qui contribueront à éviter ces risques ou à les limiter, les transférer ou les partager. Elle doit suivre un projet ou une initiative nécessitant de traiter des données personnelles tout au long de son cycle de vie et être revue lorsque le projet est modifié ou que de nouveaux risques surviennent ou apparaissent.

Exemples de situations dans lesquelles il convient d'effectuer une AIPD :

- Les bureaux de l'organisation humanitaire ont été victimes d'un nouveau pillage. L'organisation humanitaire souhaite que ses bureaux extérieurs se débarrassent de leurs dossiers papier ou qu'ils les envoient au siège et utilisent un système de stockage basé sur le cloud. Les bureaux extérieurs doivent-ils totalement éliminer les supports papier, les CD et les clés USB ?
- Une ONG ou une autorité locale contacte une organisation humanitaire et déclare qu'elle désire réunir les familles séparées par les violences qui sévissent dans le pays. Elle souhaite que l'organisation humanitaire lui transmette toutes les informations qu'elle possède sur les personnes portées disparues dans le pays. Ces informations doivent-elles être partagées ? Le cas échéant, quelles informations faut-il partager pour retrouver les personnes disparues ? Dans quelles conditions des informations personnelles doivent-elles être transmises au gouvernement d'un pays hôte ?
- Un tsunami détruit une dizaine de villages côtiers. Des milliers de personnes sont portées disparues. Quelles informations personnelles l'organisation humanitaire doit-elle recueillir auprès des familles des personnes portées disparues ? Doit-elle en recueillir beaucoup ou peu ? Ces informations doivent-elles comprendre des données génétiques ou de santé ou des données sur l'affiliation religieuse ou les opinions politiques qui, si elles sont divulguées, pourraient causer un grave préjudice aux individus ?
- Les organisations humanitaires doivent-elles publier des photos d'enfants portés disparus sur Internet ? Doivent-elles créer des affiches ? Dans quelles circonstances ?

L'AIPD peut jouer un rôle décisif lorsqu'il s'agit de déterminer qui pourrait pâtir des risques liés à la protection de la vie privée et des données personnelles, et de quelle manière.

⁷⁸ Les auteurs remercient Trilateral Research qui les a autorisés à utiliser les documents sur les AIPD.



L'hôpital du district de Chikwawa (Malawi) se sert d'un téléphone pour transmettre des résultats aux cliniques locales, 2014.

Ce chapitre explique pas à pas aux organisations humanitaires comment effectuer une AIPD et les éléments que doit contenir un rapport d'AIPD. Un modèle de rapport d'AIPD figure à l'annexe I⁷⁹. Le rapport d'AIPD ne marque pas la fin du processus d'analyse, mais il est essentiel à sa réussite. Il permet à l'organisation humanitaire de déterminer l'incidence du projet envisagé sur le droit à la vie privée et les mesures à prendre pour protéger les données personnelles. Il permet aussi à l'organisation humanitaire de montrer aux parties prenantes qu'elle prend au sérieux le droit au respect de la vie privée et à la protection des données et qu'elle s'enquiert de l'avis de ceux qui peuvent être affectés ou intéressés par le programme. Les organisations humanitaires doivent envisager de mettre le rapport d'AIPD, ou au moins un résumé, à la disposition des parties prenantes.

⁷⁹ Voir [annexe I : Modèle de rapport d'AIPD](#).

5.2 DÉROULEMENT DE L'AIPD

Cette section donne des instructions sur les mesures à prendre pour réaliser une AIPD. La conduite d'une AIPD peut suivre différentes approches. Les indications ci-après s'inspirent des bonnes pratiques issues de plusieurs sources⁸⁰.

5.2.1 UNE AIPD EST-ELLE NÉCESSAIRE ?

Toute organisation qui recueille, traite, stocke et transfère des données personnelles à d'autres organisations doit envisager de mener une AIPD, dont l'ampleur dépendra de la gravité des risques estimée. Une organisation humanitaire ne connaît pas toujours d'emblée tous les risques pour la protection des données ; certains peuvent être mis en lumière par l'AIPD. Elle peut considérer que les risques ne sont pas suffisamment importants pour justifier la réalisation d'une AIPD. Certains risques peuvent être réels, mais relativement minimes, de sorte que l'AIPD et le rapport peuvent être abrégés. D'autres risques peuvent être très graves, et inciter l'organisation humanitaire à réaliser une AIPD plus approfondie. Il n'y a pas de solution universelle.

5.2.2 L'ÉQUIPE CHARGÉE DE L'AIPD

La deuxième étape consiste à former l'équipe de l'AIPD et à élaborer le cahier des charges. L'équipe doit comprendre ou consulter le responsable de la protection des données de l'organisation humanitaire. En fonction de l'ampleur de l'AIPD à réaliser, elle pourrait réunir des spécialistes du service informatique, du service juridique, des opérations, de la protection, des politiques humanitaires, de la planification stratégique, des archives et de la gestion des informations ainsi que des groupes des relations publiques. L'équipe qui entreprend l'AIPD doit connaître les exigences en matière de protection des données ainsi que les règles de confidentialité et les codes de conduite de l'organisation humanitaire. Plus important encore, elle doit également inclure des personnes qui connaissent le projet. L'élaboration du cahier des charges suppose de prévoir le délai de réalisation de l'AIPD, son périmètre, les parties prenantes à consulter, son budget ainsi que les mesures de contrôle et d'audit qui seront prises ultérieurement.

80 David Wright, « Making Privacy Impact Assessment More Effective », *The Information Society* (vol. 29, n° 5, 2013), p. 307–315 ; Bureau du Commissaire à la vie privée de Nouvelle-Galles du Sud. *Guide to Privacy Impact Assessments in NSW*, octobre 2016, Sydney (Nouvelle-Galles du Sud, Australie) ; Secrétariat de l'ISO/IEC JTC 1/SC 27, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'étude d'impacts sur la vie privée*, ISO/IEC 29134:2017, 23 octobre 2014 : <https://www.iso.org/fr/standard/62289.html>.

5.2.3 DESCRIPTION DU TRAITEMENT DES DONNÉES PERSONNELLES

L'équipe de l'AIPD doit établir un descriptif du programme ou de l'activité à évaluer, qui doit préciser :

- les objectifs du projet ;
- la portée du projet ;
- les liens avec d'autres projets ou programmes ;
- l'équipe responsable du programme ou de l'activité ;
- une brève description des données qui seront recueillies.

La cartographie des flux de données est une étape clé de toute AIPD. Lorsqu'elle cartographie les flux d'informations d'un programme ou d'une activité, l'équipe chargée de l'AIPD doit réfléchir aux questions suivantes :

- Quelles catégories de données personnelles sont recueillies, pour qui et pourquoi ?
- Comment ces données seront-elles utilisées, conservées ou transférées ?
- Qui aura accès aux données personnelles ?
- Quelles mesures de sécurité sont en place pour protéger les données personnelles ?
- Combien de temps ces données seront-elles conservées ou quand seront-elles supprimées ? A-t-on prévu plusieurs niveaux de conservation ? À savoir :
 - 1) conservation des données jugées sensibles pendant un maximum de X jours,
 - 2) pseudonymisation des données et durée de conservation plus longue,
 - et enfin 3) suppression complète des données.
- Les données seront-elles nettoyées ou anonymisées afin de protéger les informations sensibles ?

5.2.4 CONSULTATION DES PARTIES PRENANTES

L'identification des parties prenantes est une étape importante de l'AIPD. Ce sont toutes les personnes qui sont intéressées ou affectées par un risque pour la protection des données. Elles peuvent être membres d'une organisation ou non. La gravité des risques appréciée par l'organisation humanitaire déterminera s'il est nécessaire ou opportun de consulter les parties prenantes. Pour une organisation humanitaire, consulter les parties prenantes est un moyen de découvrir des risques et des solutions qu'elle n'a peut-être pas envisagés, mais aussi de sensibiliser à la protection des données et au respect de la vie privée. Le rapport d'AIPD et les recommandations formulées doivent prendre en compte les points de vue des parties prenantes. Pour une consultation efficace, celles-ci doivent avoir suffisamment d'informations sur le programme et pouvoir exprimer leurs points de vue. Différents moyens permettent de les associer à la démarche ; l'équipe chargée de l'AIPD doit donc déterminer le plus approprié en fonction du programme ou de l'activité prévus.

5.2.5 IDENTIFICATION DES RISQUES

On peut identifier les risques à l'aide d'un tableau indiquant les principes de respect de la vie privée, les menaces qui pèsent sur ces principes, les vulnérabilités (sensibilité aux menaces) et les risques qui découlent des menaces et des vulnérabilités. Une menace sans vulnérabilité n'est pas un risque et inversement. Il y a risque lorsqu'une menace exploite une vulnérabilité.

5.2.6 ÉVALUATION DES RISQUES

Une évaluation des risques liés à la protection des données estime la probabilité d'un certain événement et ses conséquences (ses impacts). L'évaluation des risques peut faire appel aux mesures suivantes :

- consulter les parties prenantes internes et externes et déterminer avec elles les risques, les menaces et les vulnérabilités ;
- évaluer les risques par rapport à des critères de risques convenus⁸¹ ;
- évaluer les risques en termes de probabilité et de gravité de l'impact ;
- évaluer les risques par rapport aux critères de nécessité, d'adéquation et de proportionnalité.

5.2.7 CHOIX DES SOLUTIONS

Cette étape consiste à concevoir des stratégies pour éliminer, éviter, réduire ou transférer les risques d'atteinte à la vie privée. Ces stratégies peuvent comprendre des solutions techniques, des contrôles opérationnels et organisationnels et des stratégies de communication (par exemple pour sensibiliser).

5.2.8 RECOMMANDATIONS

L'équipe chargée de l'AIPD doit produire un ensemble de recommandations en fonction du résultat des étapes précédentes. Ces recommandations peuvent comprendre un ensemble de solutions, des changements organisationnels, et éventuellement les modifications à apporter à la stratégie globale de protection des données de l'organisation humanitaire ou de celle du programme et doivent être présentées dans le rapport d'AIPD.

5.2.9 APPLICATION DES RECOMMANDATIONS CONVENUES

L'équipe chargée de l'AIPD doit rédiger un rapport sur les considérations et les constats de l'AIPD. Étant donné que les organisations auront régulièrement besoin de réaliser des AIPD, la longueur et le niveau de précision des rapports d'AIPD seront très variables. À titre d'exemple, une organisation qui envisage de publier des données personnelles à des fins de recherche doit produire une documentation détaillant son AIPD. En revanche, une organisation qui détermine s'il y a lieu de

81 Pour une définition des termes liés au risque, voir ISO/Guide 73:2009(fr), *Management du risque – Vocabulaire* : <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:vl:fr>.

passer d'une marque de logiciel de traitement de texte à une autre doit prendre la protection des données en considération puisque le logiciel sera utilisé pour traiter des informations personnelles, mais elle n'aura peut-être pas besoin d'effectuer une AIPD détaillée (sauf si le logiciel implique de nouveaux flux de données dans un environnement cloud).

Outre la documentation et l'exécution des décisions en matière de protection des données, une organisation humanitaire doit déterminer s'il serait utile aux personnes concernées ou au public de comprendre les considérations qui sous-tendent ses décisions dans ce domaine. Elle pourrait alors communiquer le rapport (complet ou partiel) aux parties prenantes concernées et montrer ainsi qu'elle prend au sérieux la question de la protection des données. La communication du rapport d'AIPD peut aussi permettre de sensibiliser les parties prenantes et de solliciter de nouvelles remarques ou suggestions de leur part. Cela dit, dans certains cas, l'organisation humanitaire peut décider qu'il n'est pas opportun de communiquer le rapport d'AIPD s'il contient des informations sensibles (pour des raisons de sécurité physique, de continuité des opérations, d'accès, etc.). Dans ce cas, elle doit déterminer s'il convient d'en communiquer un résumé ou une version expurgée.

5.2.10 CONTRÔLE OU AUDIT DE L'AIPD PAR UN EXPERT

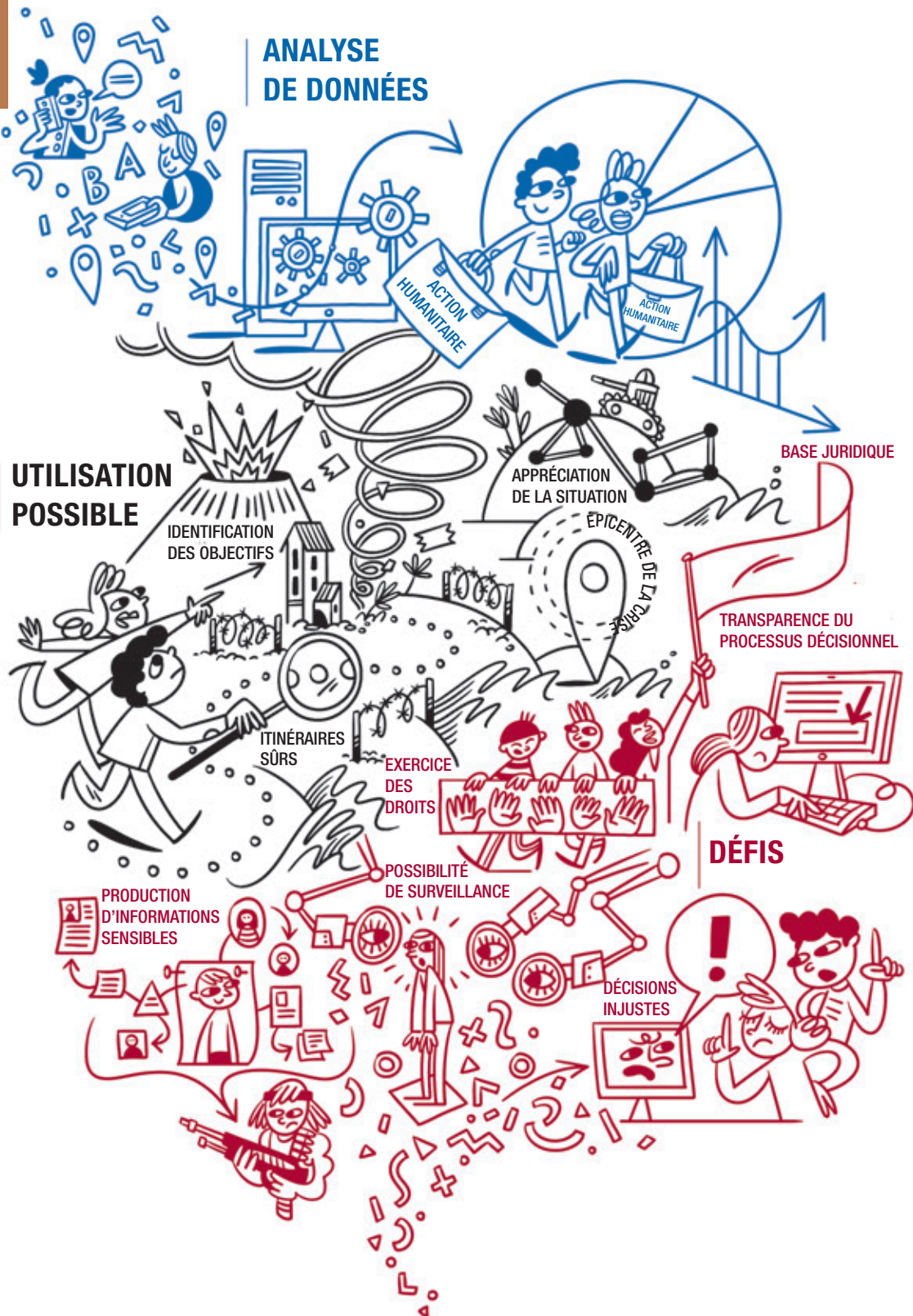
L'organisation humanitaire doit veiller à ce qu'un contrôle ou un audit de la mise en œuvre de l'AIPD soit effectué par un expert de la protection des données tel que le responsable de la protection des données ou son équipe. Pour garantir l'exactitude de l'audit, le rapport d'AIPD doit contenir une section sur la méthode.

5.2.11 ACTUALISATION DE L'AIPD EN CAS DE MODIFICATION DU PROJET

L'organisation humanitaire doit actualiser l'AIPD si l'activité couverte subit des modifications importantes ou si de nouveaux risques apparaissent.

ANALYSE DE DONNÉES

UTILISATION POSSIBLE



CHAPITRE 6

ANALYSE DE DONNÉES ET BIG DATA

6.1 INTRODUCTION

L'action humanitaire reposant sur l'information⁸², l'analyse de données à travers le traitement d'informations personnelles peut présenter un grand intérêt pour les organisations humanitaires. Le terme « analyse de données » (data analytics, en anglais) désigne la pratique consistant à combiner de très grands volumes d'informations émanant de sources diverses (big data) et à les analyser au moyen d'algorithmes complexes pour éclairer les décisions. Le big data repose non seulement sur la capacité croissante des technologies à faciliter la collecte et la conservation de grandes quantités de données, mais aussi sur la possibilité d'analyser, de comprendre et d'exploiter la pleine valeur de ces données (en particulier au moyen d'applications à visée analytique). Aux fins de ce chapitre, les termes « analyse de données » et « big data » seront employés indifféremment.

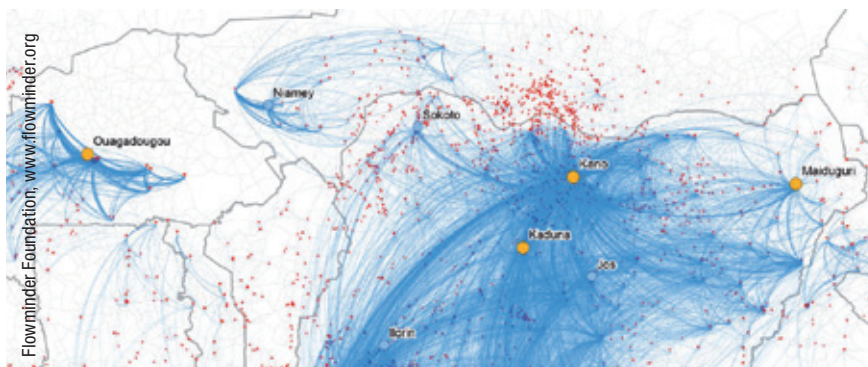
L'analyse de données peut être employée, par exemple, pour détecter des menaces potentielles pour l'action humanitaire, améliorer l'état de préparation, identifier les individus ou les catégories d'individus dans le besoin ou prévoir l'évolution de maladies contagieuses, de conflits, de tensions et de catastrophes naturelles.

Elle peut nettement renforcer l'efficacité du travail des organisations humanitaires. Elle permet notamment de cartographier ou d'identifier :

- des événements types dans des situations d'urgence humanitaire impliquant des personnes protégées dans les conflits et d'autres situations de violence ;
- la propagation de maladies ou de catastrophes naturelles, ce qui permet de prévoir les évolutions possibles et de s'y préparer pour prévenir tout préjudice ;
- l'épicentre d'une crise ;
- des itinéraires sûrs ;
- des incidents humanitaires individuels ;
- des individus ou communautés vulnérables qui pourraient avoir besoin d'une assistance humanitaire ;
- des correspondances en vue de retrouver des personnes séparées de leur famille à la suite d'une urgence humanitaire.

Le recours à l'analyse de données dans les situations humanitaires peut donc trouver deux grandes catégories d'application : la mise en évidence de tendances générales et l'identification d'individus ou de groupes d'individus intéressant les acteurs humanitaires.

⁸² Bureau de la coordination des affaires humanitaires des Nations Unies (OCHA), *Humanitarianism in the Age of Cyber-warfare* (OCHA – Série Politiques et études, 2014).



Les données de téléphonie mobile de l'Afrique de l'Ouest ont été utilisées pour cartographier les mouvements de population et prévoir comment le virus Ebola pourrait se propager.

On accuse souvent l'analyse de données de produire des résultats trompeurs et inexacts, de justifier des décisions arbitraires et automatisées qui ne tiennent pas compte des circonstances, de générer des données susceptibles d'être utilisées pour une surveillance plus efficace au moyen des empreintes numériques, et d'ouvrir la porte à des violations du principe d'anonymat à travers l'ingénierie inverse, et donc à la réidentification des individus dont les données personnelles ont été traitées. Les implications du big data en termes de protection des données ont été soulignées par la Conférence internationale des commissaires à la protection des données et à la vie privée dans sa Résolution sur le big data, adoptée à Maurice en 2014⁸³.

L'application des principes fondamentaux de la protection des données à l'analyse de données peut également susciter des préoccupations, notamment en ce qui concerne 1) la spécification des finalités, dans la mesure où le traitement à des fins analytiques utilise des données personnelles pour des finalités qui n'étaient pas prévues ; 2) les exigences de transparence, car en général, les personnes concernées reçoivent peu d'informations ; et 3) le principe de légitimité du traitement, qui n'est pas toujours une base juridique appropriée pour le traitement⁸⁴.

Ce chapitre donne des éléments d'orientation aux organisations humanitaires qui mènent des activités d'analyse de données. Il explique comment réaliser une analyse conforme aux principes de protection des données et recense les défis potentiels.

⁸³ ICDPPC, Resolution on Big Data, Fort Balaclava (Maurice), 2014 : http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf?mc_phishing_protection_id=28047-br1tehqud81eaoar3q10.

⁸⁴ Voir [chapitre 2 : Principes fondamentaux de la protection des données](#).

Plusieurs spécificités liées à la protection des données doivent être soulignées d'emblée dans cette analyse :

- *Sources des données.* Premièrement, il importe de déterminer la source des données. Une part importante des opérations d'analyse entreprises par les organisations humanitaires porte sur des données publiques, comme les informations émanant d'administrations ou de dossiers publics, de réseaux sociaux, de recensements et d'autres enquêtes démographiques accessibles au public. Dans d'autres cas, les organisations humanitaires peuvent s'associer à des entreprises privées, comme des sociétés de télécommunications ou d'infrastructures, des services Internet, des prestataires de services de santé ou d'autres organisations commerciales, afin d'améliorer l'aide humanitaire et les interventions en cas de catastrophe.
- *Intervention d'urgence.* Bien que les résultats de l'analyse de données présentent un intérêt indéniable pour les organisations humanitaires, ils ne sont pas toujours exploitables pour une urgence en cours ou pour répondre aux intérêts vitaux des individus concernés. Il peut arriver, par exemple, que les opérations d'analyse soient réalisées après la survenue d'un incident et une fois celui-ci réglé, à l'appui de tâches administratives ou dans le cadre de stratégies visant à améliorer les interventions futures.
- *Exactitude.* Il arrive que les données utilisées pour l'analyse ne soient ni représentatives ni exactes et qu'elles contiennent des biais pouvant fausser les résultats⁸⁵. Travailler sur des données anonymisées ou agrégées, même si celles-ci peuvent être moins intrusives vis-à-vis de la vie privée des individus concernés, accroît ce risque.
- *Décision automatisée.* L'analyse de données sans intervention humaine ni informations contextuelles peut aussi donner un éclairage incorrect et fausser les décisions⁸⁶.
- *Réutilisation de données pour d'autres finalités.* Le recours au big data pose souvent la question de savoir si les données personnelles peuvent être utilisées pour d'autres finalités que celles de la collecte. En effet, le droit de la protection des données exige généralement que les données personnelles soient recueillies pour des finalités spécifiées, qu'elles soient traitées exclusivement pour ces finalités ou pour des finalités compatibles, et qu'elles ne soient pas réutilisées à d'autres fins sans le consentement de la personne concernée ou sans autre base juridique.

⁸⁵ UN Global Pulse, *Big Data for Development and Humanitarian Action: Towards Responsible Governance*, Rapport du Groupe consultatif sur la vie privée, 2016, p. 12 : http://unglobalpulse.org/sites/default/files/Big_Data_for_Development_and_Humanitarian_Action_Report_Final_o.pdf.

⁸⁶ *Ibid.*, p. 12 : « Pour bien éclairer les décisions, les données doivent être représentatives. Il faut donc tenir compte de la présence possible de biais dans certains ensembles de données ou algorithmes. Pour éviter les biais, la qualité des données, l'exactitude et l'intervention humaine dans les activités de traitement des données sont essentielles. »

- *Sensibilité des données résultant du traitement de données personnelles en situation humanitaire.* Il faut bien comprendre que des données publiquement accessibles, comme les informations figurant sur les réseaux sociaux et celles qui ne sont pas généralement considérées comme sensibles, peuvent générer des données sensibles lorsqu'elles sont traitées à des fins analytiques en situation humanitaire. C'est notamment le cas lorsque le traitement de données anodines permet d'établir le profil des individus, ce qui pourrait entraîner des discriminations ou des mesures de répression contre, notamment, des victimes potentielles, des personnes affiliées à un groupe particulier dans une situation de violence ou les porteurs de certaines maladies. Dans cette situation, le lissage de données peut être une option intéressante pour protéger la vie privée d'individus ou de groupes tout en autorisant l'accès aux données⁸⁷. Il faut toutefois souligner que le lissage étant à la fois temporel et spatial, la clarté des constats s'en trouve diminuée.
- *Anonymisation.* Des doutes peuvent exister quant à l'efficacité de l'anonymisation des données personnelles et à la possibilité de réidentification dans les opérations d'analyse de données, que ce soit à des fins humanitaires ou non. Là encore, le lissage des données peut compléter l'anonymisation afin d'apporter un autre niveau de protection contre la réidentification.
- *Fragmentation réglementaire.* Bien que de nombreux États aient promulgué des lois sur la protection des données et que de nombreuses organisations humanitaires mettent déjà en œuvre des politiques et des directives en la matière, la question relative aux modalités de réglementation internationale du big data en situation de crise humanitaire reste ouverte⁸⁸.

Il faut bien comprendre que l'analyse de données à des fins humanitaires peut avoir des implications bien plus graves pour les individus que dans d'autres cadres (dans un environnement commercial par exemple). Ainsi, même lorsque les données analysées ont été anonymisées, les résultats peuvent avoir de graves conséquences pour les individus et les groupes d'individus. Les organisations humanitaires doivent déterminer si les données qu'elles publient ou les conclusions qu'elles tirent de l'analyse des données peuvent être utilisées, même dans leur ensemble, pour cibler les personnes qu'elles cherchent à protéger. En outre, ces groupes d'individus susceptibles d'être affectés ne comprennent pas toujours les personnes concernées. Dans bien des cas, des populations invisibles peuvent soudainement devenir visibles parce qu'elles sont séparées du groupe identifié dans l'ensemble de données⁸⁹. Il convient donc de garder à l'esprit l'ensemble des implications potentielles de l'analyse de données pour les individus vulnérables.

⁸⁷ Le lissage de données consiste à éliminer les bruits d'un ensemble de données afin de dégager les tendances.

⁸⁸ UN Global Pulse, 2016, p. 7-9.

⁸⁹ *Ibid.*, p. 12.

EXEMPLE :

L'extraction et l'analyse de tweets et d'autres éléments figurant sur les réseaux sociaux, en vue de localiser l'épicentre et les flux de manifestations publiques et d'éviter ainsi toute perte de vies humaines, et la communication des résultats aux autorités peuvent permettre à ces dernières d'utiliser ces résultats pour identifier les individus qui ont (ou n'ont pas) pris part à ces manifestations, ce qui peut avoir pour eux de graves conséquences.

L'analyse de données peut impliquer les scénarios de traitement suivants :

EXEMPLE 1 : Extraction et analyse des communications publiques via les médias sociaux, les moteurs de recherche ou les services de télécommunications, ainsi que des sources d'informations et de nouvelles pour démontrer comment des méthodes telles que l'analyse du sentiment, la classification par sujet et l'analyse de réseau peuvent être mises au service des travailleurs de la santé publique et des campagnes de communication.

EXEMPLE 2 : Développement d'outils interactifs de visualisation des données lors d'un incident humanitaire pour démontrer comment les signaux de communication ou les données de satellites pourraient être utiles à la gestion des interventions d'urgence.

EXEMPLE 3 : Analyse des messages reçus sur la plateforme citoyenne de signalement d'une organisation humanitaire.

EXEMPLE 4 : Analyse des médias sociaux, des métadonnées des réseaux de téléphonie mobile et des données de cartes de crédit pour identifier les individus qui risquent d'être victimes d'une disparition forcée ou pour localiser des personnes portées disparues.

Les ensembles de données suivants peuvent être pertinents :

- ensembles de données publics (c'est-à-dire ensembles de données accessibles au public, comme les dossiers publics publiés par les gouvernements ou les informations que des personnes ont volontairement rendues publiques dans les médias d'information ou sur Internet, notamment sur les réseaux sociaux);
- ensembles de données détenus par des organisations humanitaires (listes de bénéficiaires de distributions, de patients, d'individus protégés, d'individus dont la famille a signalé la disparition, d'individus signalant des violations du droit international humanitaire ou des droits humains);

- ensembles de données détenus par des tiers de droit privé (prestataires de services mobiles, de télécommunications, établissements bancaires et financiers, fournisseurs de services Internet et données de transactions financières, données de capteurs à distance, qu’elles soient ou non agrégées ou anonymisées) ;
- combinaison ou agrégation d’ensembles de données détenus par des organisations humanitaires, des autorités ou des entreprises (y compris les organisations mentionnées plus haut).

Une organisation humanitaire peut jouer les rôles suivants dans le traitement de données :

- traiter les données qu’elle détient (en qualité de responsable du traitement) ;
- recourir à des sous-traitants (c’est-à-dire des entités commerciales qui procéderont à l’analyse des données qu’elle détient) ;
- charger des entités commerciales, qui sont et demeurent les responsables du traitement, de procéder à des analyses des données à des fins humanitaires et de lui transmettre leurs conclusions et constats. Ces conclusions pourraient concerner des données agrégées ou anonymisées ou des données identifiant des individus susceptibles d’intéresser l’action humanitaire ;
- partager des ensembles de données avec d’autres organisations humanitaires, des autorités publiques ou des entités commerciales en tant que responsables du traitement ou sous-traitants conjoints.

Ces scénarios peuvent être présentés comme suit :

	Données détenues par l'organisation humanitaire	Données détenues par des tiers (autorités/entreprises)
L'organisation humanitaire est le responsable du traitement	L'organisation humanitaire peut procéder elle-même à des analyses ou recourir aux services d'un sous-traitant externe	Le partenaire externe fournit des données à l'organisation humanitaire qui les traite
Le tiers est le responsable du traitement	L'organisation humanitaire fournit les données à un partenaire externe qui les traite	Le partenaire externe traite les données à la demande de l'organisation humanitaire

Il faut souligner que l’organisation humanitaire et le tiers peuvent être simultanément responsables du traitement et sous-traitants. À titre d’exemple, les données peuvent être détenues par une organisation tierce, être traitées par l’organisation tierce à la demande de l’organisation humanitaire, puis être partagées par celle-ci avec d’autres parties prenantes.

6.2 APPLICATION DES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

Le traitement de données personnelles à des fins analytiques présente d'importants défis pour la protection des données individuelles. En effet, le traitement de larges ensembles de données à des fins autres que celles pour lesquelles elles ont été collectées risque de violer les principes fondamentaux de la protection des données, notamment celui de la limitation de(s) la finalité(s), la minimisation des données ou la conservation de données limitée au temps nécessaire pour atteindre les finalités de la collecte. Fondamentalement, l'analyse de données prospère dans les environnements de traitement ouverts et dénués de restrictions alors que la protection des données personnelles privilégie le traitement limité et bien défini. La protection des données doit donc être appliquée de façon innovante au big data⁹⁰.

Les principes fondamentaux de la protection des données sont les bases à respecter lorsqu'on entreprend des opérations d'analyse de données. Comme il est précisé au [chapitre 2: Principes fondamentaux de la protection des données](#), les principes à respecter dans le cadre de ces opérations sont le principe de licéité et de loyauté du traitement, le principe de transparence, le principe de limitation de(s) la finalité(s), le principe de minimisation des données et le principe de qualité des données. Bien que certains de ces principes soient compatibles avec les finalités de l'analyse de données, d'autres peuvent soulever des questions ou susciter des conflits ; les organisations humanitaires doivent donc prendre des précautions particulières lorsqu'elles les appliquent. Certaines organisations humanitaires ont établi des principes pour la gestion du big data qui complètent l'analyse de ce chapitre⁹¹.

L'analyse de la protection des données présentée dans ce chapitre s'appuie sur les principes énoncés dans la première partie, où ils sont examinés en plus amples détails.

L'un des défis les plus sérieux posés par l'analyse de données dans le domaine humanitaire est que les opérations d'analyse sont le plus souvent effectuées sur des ensembles de données déjà collectées par l'organisation humanitaire ou par des tiers pour une autre finalité. La question essentielle est alors de savoir si l'analyse envisagée est compatible avec la finalité initiale de la collecte. Dans l'affirmative,

⁹⁰ Contrôleur européen de la protection des données (CEPD), Avis n° 7/2015, *Relever les défis des données massives*, 19 novembre 2015, p. 4 : https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_fr.pdf

⁹¹ Voir UN Global Pulse, *Data Privacy and Data Protection Principles* : <http://www.unglobalpulse.org/privacy-and-data-protection-principles> ; Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, janvier 2017 : <https://rm.coe.int/16806ebf23>.

elle peut être exécutée sur la base juridique existante. Dans le cas contraire, il faut identifier une nouvelle base juridique pour le traitement.

6.2.1 LIMITATION DE(S) LA FINALITÉ(S) ET TRAITEMENT ULTÉRIEUR

Comme expliqué au [chapitre 2: Principes fondamentaux de la protection des données](#), au moment de la collecte des données, l'organisation humanitaire doit déterminer et exposer les finalités spécifiques du traitement des données. Ces finalités doivent être explicites et légitimes et peuvent comprendre tout objectif allant du rétablissement des liens familiaux à la protection des individus en détention, aux activités médico-légales ou à la protection de l'eau et de l'habitat. Idéalement, la finalité de l'analyse envisagée doit être spécifiée dès le début de la collecte de données.

En ce qui concerne le traitement ultérieur, indépendamment de la base juridique retenue pour le traitement initial, les organisations humanitaires peuvent traiter des données personnelles pour d'autres finalités que celles qui ont été spécifiées au moment de la collecte lorsque ce traitement ultérieur est compatible avec ces finalités initiales et, en particulier, lorsqu'il est nécessaire à des fins historiques, statistiques ou scientifiques⁹².

Les opérations d'analyse exigent fréquemment de traiter des données à d'autres fins que celles de la collecte initiale. Cependant, les finalités de l'analyse de données sont rarement prévisibles au moment de la collecte initiale des données personnelles.

Pour déterminer si l'opération d'analyse peut être considérée comme un traitement ultérieur compatible avec la finalité de la collecte initiale, il convient de prêter attention aux facteurs suivants :

- tout lien entre les finalités de la collecte et celles du traitement ultérieur envisagé ;
- la situation dans laquelle les données personnelles ont été recueillies et, en particulier, la relation entre les personnes concernées et le responsable du traitement ainsi que les attentes éventuelles des personnes concernées ;
- la nature des données personnelles ;
- les conséquences que le traitement ultérieur envisagé pourrait avoir pour les personnes concernées ;
- l'existence de garanties appropriées.

La finalité humanitaire du traitement des données doit être gardée à l'esprit lors de l'examen des facteurs ci-dessus. En général, les finalités humanitaires sont compatibles les unes avec les autres. Lorsque, en raison de la valeur des ensembles de données pour l'action humanitaire, des données de tiers sont traitées pour d'autres finalités que celles de la collecte initiale, il est possible d'utiliser ces données

⁹² Voir [section 2.6.3: Traitement ultérieur](#).

– et ce traitement ultérieur sera alors considéré comme compatible – tant que cela n'expose pas les personnes concernées à de nouveaux risques ou dangers, comme il est expliqué plus amplement ci-dessous. Un nouveau traitement, même à des fins humanitaires, ne serait pas compatible s'il engendre de nouveaux risques ou si les risques pour la personne concernée l'emportent sur les avantages du traitement ultérieur. La compatibilité dépend des circonstances. Le traitement ultérieur ne serait pas non plus compatible lorsqu'il risque de nuire à la personne à laquelle les informations ont trait ou à sa famille, en particulier s'il risque de porter atteinte à leur vie, à leur intégrité, à leur dignité, à leur sécurité psychologique ou physique, à leur liberté ou à leur réputation, par exemple s'il engendre les risques suivants :

- harcèlement ou persécution de la part des autorités ou de tiers ;
- poursuites judiciaires ;
- problèmes sociaux et privés ;
- restriction de la liberté ;
- souffrances psychologiques.

EXEMPLE 1 : Les ensembles de données recueillis par une organisation humanitaire lors d'un incident, par exemple pour distribuer de l'aide, peuvent être utilisés ultérieurement pour comprendre les profils tendanciels de déplacement et pré-déployer l'aide lors d'urgences humanitaires ultérieures.

EXEMPLE 2 : Les ensembles de données recueillis par un prestataire de services de télécommunications dans le cadre de la fourniture de services à ses abonnés ne peuvent pas être utilisés sans le consentement de ces abonnés dans le cadre d'un traitement à des fins analytiques effectué par des organisations humanitaires s'il peut aboutir au profilage de ces individus comme de possibles porteurs de maladie, avec à la clé des restrictions aux déplacements imposées par les autorités. Dans ce cas, les organisations humanitaires et leurs partenaires doivent déterminer si des mesures d'atténuation, comme l'agrégation des données, seraient suffisantes pour éliminer le risque détecté.

6.2.2 FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

Si les finalités de l'analyse sont jugées incompatibles avec la finalité initiale du traitement, il faut trouver une nouvelle base juridique. Les organisations humanitaires pourraient justifier l'analyse de données par un ou plusieurs des fondements légaux suivants⁹³ :

- l'intérêt vital de la personne concernée ou d'une autre personne ;
- l'intérêt public, en particulier basé sur le mandat confié à une organisation en vertu du droit national ou international ;
- le consentement ;

⁹³ Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

- l'intérêt légitime de l'organisation ;
- l'exécution d'un contrat ;
- le respect d'une obligation légale.

L'utilisation du consentement pose des problèmes pour les opérations d'analyse portant sur des données personnelles recueillies et organisées en ensembles de données. En outre, en raison de la complexité de l'opération de traitement et des implications qui n'apparaissent pas toujours clairement au moment de la collecte, il peut être difficile de s'assurer à ce stade que les personnes concernées apprécient pleinement les risques et les avantages de l'analyse des données.

Dans certains cas, l'analyse de données proposée par les réseaux sociaux ou les opérateurs de téléphonie mobile pour aider les organisations humanitaires pourrait être fondée sur le consentement si la plateforme du réseau social ou l'opérateur de téléphonie mobile en question est capable d'informer les personnes concernées du traitement envisagé au moyen d'une fenêtre contextuelle ou d'un message contenant les informations requises et la demande de consentement. Dans ce scénario toutefois, il convient de réfléchir aux implications d'un refus de consentement pour la fiabilité de l'analyse et les conclusions qui en seront tirées.

Pour garantir un consentement réellement éclairé, les informations données doivent tenir compte du résultat de l'AIPD (le cas échéant)⁹⁴ et peuvent être également données au moyen d'une interface simulant les effets de l'utilisation des données et son impact potentiel sur la personne concernée, dans le cadre d'une approche d'apprentissage par l'expérience⁹⁵. Les sous-traitants doivent offrir des moyens techniques conviviaux et faciles d'utilisation aux personnes concernées pour leur permettre de retirer leur consentement et de réagir à un traitement des données incompatible avec les finalités initiales⁹⁶.

Il est important d'évaluer la validité du consentement même lorsque des informations adéquates ont été données aux personnes concernées au moment de la collecte et que la finalité du traitement ultérieur est compatible. Cette évaluation doit tenir compte du niveau d'alphabétisation des personnes concernées ainsi que des risques et des préjudices auxquels le traitement de leurs données pourrait les exposer⁹⁷.

⁹⁴ Voir [section 6.7: Analyses d'impact relatives à la protection des données](#).

⁹⁵ Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, janvier 2017.

⁹⁶ *Ibid.*

⁹⁷ Programme des Nations Unies pour le développement (PNUD), UN Global Pulse, *Risks, Harms and Benefits Assessment Tool* : <https://www.unglobalpulse.org/policy/risk-assessment/>.

Même lorsqu'il est impossible d'obtenir le consentement de la personne qui fournit les données ou de la personne concernée, il est possible de traiter les données personnelles s'il est établi que le traitement est dans l'intérêt vital de la personne concernée ou d'une autre personne, c'est-à-dire lorsqu'il est nécessaire pour protéger un intérêt essentiel pour la vie, l'intégrité, la santé, la dignité ou la sécurité de la personne concernée, d'une autre personne ou d'un groupe de personnes. En outre, d'autres fondements juridiques comme l'intérêt public, l'intérêt légitime de l'organisation et l'exécution d'un contrat ou le respect d'une obligation légale peuvent justifier le traitement.

En ce qui concerne l'intérêt vital en tant que base juridique du travail d'urgence des organisations humanitaires dans les conflits armés et d'autres situations de violence, le traitement des données effectué par les organisations humanitaires peut être présumé conforme à l'intérêt vital d'une personne concernée ou d'une autre personne dans plusieurs hypothèses (par exemple, si les données sont traitées dans le cas de personnes portées disparues ou s'il existe des menaces imminentes contre l'intégrité physique et mentale des personnes concernées). Cependant, la condition de l'intérêt vital ne sera peut-être pas satisfaite si le traitement des données n'est pas entrepris dans une situation d'urgence, par exemple à des fins administratives.

EXEMPLE :

La base juridique de l'intérêt vital ne s'applique pas lorsque l'analyse de données est entreprise pour des finalités administratives ou de recherche pure.

Lorsque des motifs importants d'intérêt public sont en jeu, les organisations humanitaires doivent soigneusement vérifier qu'ils ont un lien suffisamment étroit avec l'opération d'analyse envisagée pour servir de base juridique au traitement des données personnelles. L'intérêt public pourrait être une base juridique appropriée pour l'analyse de données lorsqu'une action humanitaire est mandatée par le droit national, régional ou international et lorsqu'aucun consentement n'a été obtenu et qu'aucune urgence ne permettait d'invoquer l'intérêt vital.

Les organisations humanitaires doivent savoir que l'intérêt public en tant que base juridique du traitement des données personnelles n'est pas transférable, parce qu'il est propre au mandat confié à l'organisation par le droit national ou international. Les conditions éventuelles en vertu desquelles un tiers peut entreprendre des opérations d'analyse pour le compte de l'organisation ou qui sont applicables au transfert international de données doivent être examinées séparément.

Les organisations humanitaires peuvent également traiter des données personnelles lorsqu'elles y ont un intérêt légitime, sous réserve que les droits et libertés fondamentaux de la personne concernée ne l'emportent pas sur cet intérêt.

Cet intérêt légitime peut comprendre le traitement nécessaire pour améliorer l'efficacité de leurs opérations, notamment faciliter la logistique pour pré-déployer l'aide et le personnel en prévision d'urgences humanitaires, lorsque l'analyse des données permettrait d'obtenir ces informations. L'analyse de données à des fins administratives peut aussi entrer dans cette catégorie.

EXEMPLE :

Les organisations humanitaires peuvent entreprendre un traitement à des fins analytiques sur les données de leurs employés pour constituer une base de données du personnel par région.

Les intérêts légitimes peuvent être également utilisés par des entités commerciales disposées à exécuter des opérations d'analyse de données pour aider les organisations humanitaires lorsque la finalité du traitement est exclusivement humanitaire.

6.2.3 TRAITEMENT ÉQUITABLE ET LICITE

Pour être équitable et licite, le traitement doit avoir une base juridique, comme l'explique la [section 2.5 : Principes applicables au traitement des données](#).

L'analyse de données déduit des corrélations possibles en se fondant sur une analyse subjective de faits objectifs ; elle soulève donc de nombreuses questions sur l'équité du traitement, notamment des préoccupations concernant l'échantillonnage, la représentation et les estimations de population. Les chercheurs doivent veiller à bien comprendre la représentativité des données de l'échantillon, s'efforcer de travailler sur des ensembles de données larges et représentatifs et signaler les biais potentiels. En outre, les décideurs politiques doivent tenir compte de ces biais dans leurs décisions. Dans le contexte de l'élaboration de politiques, une analyse reposant sur des données inexactes et une interprétation erronée des constats peuvent entraîner des décisions politiques préjudiciables ou inéquitables, ou les personnes concernées peuvent se trouver affectées par des décisions automatisées potentiellement biaisées et par des généralisations.

En outre, l'obligation d'équité posée par le droit de la protection des données est généralement centrée sur l'information des personnes, la transparence et l'impact du traitement. Étant donné la complexité du traitement et la difficulté à réaliser une analyse satisfaisante des risques, la transparence sur la méthodologie (y compris, lorsque c'est possible, sur l'algorithme) est très importante en matière d'analyse de données, afin que la rigueur de l'approche puisse être évaluée en toute indépendance, au-delà du droit à l'information des personnes concernées⁹⁸. Il faut

⁹⁸ Voir [section 6.3 : Droits des personnes concernées](#), et [section 6.5 : Transfert international de données](#).

veiller à la transparence dans les procédures décisionnelles lorsque la transparence entre en conflit avec la sensibilité des données au niveau individuel ou lorsque la transparence dans le traitement pourrait encourager la ludification (encore appelée « gamification ») du système de traitement des données par des acteurs malveillants et pourrait donc le biaiser.

Le principe de loyauté implique d'évaluer les risques de réidentification avant la désidentification et, si possible, d'informer la personne concernée ou les parties prenantes concernées des résultats. Si le risque de réidentification est élevé, il faut renoncer à l'analyse ou ajuster la méthodologie. Une AIPD est nécessaire pour bien évaluer une telle situation du point de vue de l'analyse de données⁹⁹.

Il importe également que les employés, les sous-traitants et les autres parties qui interviennent dans l'analyse des données suivent une formation aux risques en matière de protection des données et aux procédures de recherche éthiques, et que des mesures soient prises pour atténuer ces risques.

6.2.4 MINIMISATION DES DONNÉES

Les données traitées par les organisations humanitaires doivent être adéquates et pertinentes pour les finalités de la collecte et du traitement. Cela implique en particulier de ne pas recueillir trop de données et de limiter au strict nécessaire la durée de conservation des données avant anonymisation ou archivage. Idéalement, la quantité de données personnelles recueillies et traitées doit être limitée à ce qui est nécessaire pour les finalités spécifiées de la collecte, du traitement ou d'un traitement ultérieur compatible, ou à ce qui est justifié en vertu d'une autre base juridique.

Cela étant, pour produire des résultats optimaux, l'analyse de données requiert généralement de larges ensembles de données contenant un maximum d'informations sur longue période. Ces conditions sont contraires au principe de minimisation des données, qui requiert, comme on l'a vu plus haut, de minimiser le plus possible le contenu des ensembles de données recueillies par les organisations humanitaires au moment de la collecte. Il est donc important que la finalité de la collecte des données soit stipulée le plus précisément possible et que toute conservation de données au-delà des besoins du projet initial soit justifiée par un traitement ultérieur compatible.

En outre, bien que des ensembles de données archivées ou anonymisées puissent également être utilisés pour les opérations d'analyse, leur utilisation présente des défis techniques et juridiques. En effet, la capacité de traitement peut être restreinte par des contraintes d'archivage et il faut être particulièrement attentif

⁹⁹ Voir [section 6.7: Évaluations d'impact relatives à la protection des données](#).

à ce que le résultat du traitement ne permette pas de réidentifier des personnes désidentifiées. Il faut aussi s'interroger sur la fiabilité des résultats de l'analyse de données anonymisées ou agrégées. Les méthodes et le degré d'anonymisation ou d'agrégation doivent donc être soigneusement sélectionnés pour minimiser les risques de réidentification et préserver la qualité et l'utilité voulues des données pour obtenir des résultats crédibles.

Les responsables du traitement et, le cas échéant, les sous-traitants, doivent soigneusement concevoir leur analyse de données afin de minimiser la présence de données redondantes et marginales¹⁰⁰.

Les données personnelles ne doivent être conservées que pendant la durée définie, nécessaire aux finalités de la collecte. Au terme de la durée de conservation initiale, une évaluation doit être réalisée pour déterminer s'il convient de supprimer les données ou de les conserver plus longtemps pour atteindre les finalités. Les opérations potentielles d'analyse de données doivent être traitées en détail dans la politique relative à la conservation des données ou la notice d'information. Si le traitement à des fins analytiques est prévu au moment de la collecte, il doit être mentionné dans la notice d'information initiale, et la durée de conservation envisagée doit couvrir le délai requis pour réaliser les analyses.

Si ce traitement est effectué sur des ensembles de données existants en tant que « traitement ultérieur compatible¹⁰¹ », il doit intervenir pendant la durée de conservation des données autorisée pour les finalités de la collecte initiale. La durée de conservation initiale peut être reconduite si une reconduction est envisagée par la politique de conservation au moment de la collecte pour permettre l'analyse des données en tant que « traitement ultérieur compatible ».

Lorsque le traitement porte sur des ensembles de données existants et que l'analyse de données n'est pas une finalité jugée compatible avec celle de la collecte initiale, une nouvelle base juridique doit être trouvée et une notice d'information spécifique doit être établie, expliquant l'opération d'analyse et indiquant la durée de conservation.

100 Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, janvier 2017.

101 Voir [section 2.6.3: Traitement ultérieur](#).

6.2.5 SÉCURITÉ DES DONNÉES

Pour déterminer si des mesures de sécurité sont appropriées pour protéger des informations dans le cadre d'opérations d'analyse de données, il importe de tenir compte du fait que les résultats du traitement, qui peuvent corréler et analyser des ensembles de données existants, peuvent produire des données plus sensibles que les ensembles de données initiaux. Les résultats, qui peuvent inclure un profilage individuel ou collectif, pourraient être préjudiciables aux individus concernés s'ils tombent entre de mauvaises mains.

Dans ce cas, l'organisation humanitaire qui entreprend l'analyse des données doit, pour protéger le résultat, mettre en place des mesures de sécurité qui sont adaptées aux risques en jeu¹⁰². En outre, une formation régulière à la sécurité et à la confidentialité des données est essentielle pour sensibiliser aux menaces pesant sur la sécurité et éviter des violations de données.

6.3 DROITS DES PERSONNES CONCERNÉES

Les droits des personnes concernées sont présentés à la [section 2.11: Droits des personnes concernées](#). Le droit à l'information, le droit d'accès, le droit de rectification, le droit de suppression et le droit d'opposition sont des éléments cruciaux d'une politique efficace de protection des données. Cependant, le traitement des données personnelles à des fins analytiques pose d'importants défis.

L'exercice du droit à l'information de la personne concernée (également pertinent pour le principe de transparence, voir [section 6.2.1: Limitation de\(s\) la finalité\(s\) et traitement ultérieur](#)) est plus difficile en ce qui concerne l'analyse de données car il n'est pas toujours possible de donner directement des informations précises sur le traitement aux individus concernés, surtout lorsque le traitement porte sur des ensembles de données existants. Il importe donc d'envisager d'autres moyens d'information, par exemple les sites Internet des organisations concernées, d'autres plateformes Internet susceptibles d'être consultées par les personnes concernées ou d'autres moyens de communication de masse (presse, brochures ou affiches). Lorsqu'il s'avère difficile ou impossible d'informer les personnes concernées, il a été suggéré de créer une ressource d'information nationale ou internationale (plus facile à trouver que les sites Internet d'opérateurs individuels). Il peut être également opportun d'étudier la possibilité de donner des informations aux représentants de groupes.

¹⁰² Voir [section 6.2.5: Sécurité des données](#), et [section 2.8: Sécurité des données et sécurité du traitement](#).

Les organisations qui exécutent des opérations d'analyse de données humanitaires sont encouragées à incorporer des procédures de réclamation dans leurs pratiques en matière de traitement des données personnelles et leurs politiques internes de protection des données. Ces procédures doivent permettre de rectifier et de supprimer les données. Il faut toutefois reconnaître que l'exercice de certains droits individuels peut être limité par la base juridique du traitement. À titre d'exemple, il est possible que les demandes de restrictions au traitement soumises par des personnes concernées ne soient pas respectées si le traitement est entrepris sur le fondement de l'intérêt public décrit plus haut.

Les organisations humanitaires doivent s'assurer qu'aucune décision pouvant exclure des individus des programmes humanitaires ou leur être autrement préjudiciable n'est prise automatiquement, sans intervention humaine. Un être humain doit toujours être le décideur ultime lorsque des décisions susceptibles d'avoir des répercussions négatives sur des individus sont prises sur la base des résultats d'une analyse des données.

EXEMPLE :

En ce qui concerne la distribution d'aide, une décision donnant la priorité à une région ou un groupe d'individus précis (au détriment de ceux qui ne sont pas dans cette région ou dans ce groupe) sur la base du résultat d'opérations d'analyse de données doit toujours être contrôlée et validée par un être humain.

6.4 PARTAGE DE DONNÉES

Le traitement à des fins analytiques peut comprendre le partage des données avec des sous-traitants ou des tiers, aussi bien avant l'exécution de l'analyse des données, lorsque les ensembles de données appartiennent à différents responsables du traitement, qu'après son exécution, lorsque les résultats et les constats peuvent être partagés avec des tiers. Il peut donc concerner des données personnelles et des données agrégées ou anonymisées. Les parties avec lesquelles les données sont partagées peuvent être de nouveaux responsables du traitement ou des sous-traitants. En fonction du traitement ou du lieu d'établissement de l'organisation humanitaire, ce partage des données peut impliquer que les données franchissent les frontières nationales ou sont partagées par ou avec des organisations internationales. Il faut souligner que le « partage » couvre non seulement les situations dans lesquelles les données sont activement transférées à des tiers, mais aussi celles dans lesquelles elles sont simplement rendues accessibles à des tiers. Le partage de données comportant un élément international et une relation de type responsable du traitement/sous-traitant est traité ci-après.

6.5 TRANSFERT INTERNATIONAL DE DONNÉES

L'analyse de données implique généralement un transfert international de données personnelles vers diverses parties situées dans différents pays, selon les scénarios énumérés plus haut, qui sont résumés ci-dessous :

- Des organisations humanitaires employant des sous-traitants, c'est-à-dire des entités commerciales, traitent les données personnelles détenues par l'organisation humanitaire.
- Des organisations humanitaires chargent des entités commerciales qui sont et demeurent les responsables du traitement afin de procéder à des analyses de données à des fins humanitaires et de leur transmettre leurs conclusions et leurs constats. Ces conclusions pourraient concerner des données agrégées ou anonymisées ou des données identifiant des individus susceptibles d'intéresser l'action humanitaire.
- Partage d'ensembles de données avec d'autres organisations humanitaires, des autorités publiques ou des entités commerciales (responsables du traitement ou sous-traitants conjoints).
- Partage effectif (ou transfert de données) à une organisation humanitaire aux fins du traitement.

Le droit de la protection des données pose des restrictions aux transferts internationaux de données ; les organisations humanitaires doivent donc mettre en place des mécanismes conférant une base juridique à ces transferts en cas d'opérations d'analyse de données, comme on l'a vu plus haut¹⁰³. Il est essentiel de réaliser une AIPD¹⁰⁴ avant tout transfert international de données à des fins d'analyse, étant donné la complexité de cette dernière, la difficulté de s'assurer que les personnes concernées sont convenablement informées et capables d'exercer pleinement leurs droits (voir ci-dessus), et les conséquences extrêmement étendues que sont susceptibles d'avoir pour elles les opérations d'analyse des données. Une AIPD sera l'outil le plus approprié pour déterminer les risques liés au partage de données et les mesures d'atténuation les plus adaptées (clauses contractuelles, codes de conduite ou renonciation à partager les données)¹⁰⁵.

En outre, lorsque les organisations humanitaires font appel à des prestataires de services pour conduire ou faciliter des opérations d'analyse de données, elles doivent comprendre les finalités pour lesquelles ces entreprises peuvent utiliser les données. Plus précisément, les entreprises qui analysent leurs propres données ou qui traitent les données d'organisations humanitaires peuvent avoir intérêt à exploiter les constats du traitement à des fins commerciales pour mieux comprendre leurs clients ou pour affiner le profilage de leur clientèle. Il est donc très important

¹⁰³ Voir [section 6.2.2 : Fondements juridiques du traitement des données personnelles](#).

¹⁰⁴ Voir [section 6.7 : Analyses d'impact relatives à la protection des données](#).

¹⁰⁵ Voir [chapitre 4 : Transfert international de données](#), et [section 4.4 : Atténuation des risques pour l'individu](#).

que les contrats éventuellement conclus avec elles indiquent très clairement que la finalité du traitement est et doit rester exclusivement humanitaire, et que le prestataire de services maintienne un cloisonnement étanche entre le traitement humanitaire et ses activités commerciales. En cas de doute sur la capacité ou la volonté du prestataire de services de respecter cette condition, l'organisation humanitaire doit renoncer au traitement, car un traitement dont les finalités ne seraient pas exclusivement humanitaires peut avoir de graves implications pour les personnes concernées. Par exemple, les résultats de l'analyse qui identifient les catégories de bénéficiaires potentiels de l'action humanitaire peuvent entraîner un refus de crédit, une augmentation des primes d'assurance, des discriminations, voire des persécutions.

Les organisations humanitaires doivent être également attentives au fait qu'en situation de violence ou de conflit, les parties concernées peuvent chercher à accéder aux résultats de l'analyse de données et à en tirer un avantage, ce qui pourrait compromettre la sécurité des personnes concernées et la neutralité de l'action humanitaire. En conséquence, lorsque les résultats peuvent être sensibles, il est important d'envisager un scénario dans lequel l'organisation humanitaire conduit ses analyses de données en interne sans en communiquer les résultats au fournisseur des données.

6.6 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Le rôle du responsable du traitement et celui du sous-traitant sont souvent assez flous dans le contexte de l'analyse de données. Il est donc indispensable de déterminer quelles sont les parties qui définissent effectivement les finalités et les moyens du traitement des données (et sont donc des responsables du traitement) et celles qui prennent simplement leurs instructions auprès des responsables du traitement (et sont donc des sous-traitants). Il est possible également que plusieurs parties puissent être considérées comme des responsables du traitement conjoints.

EXEMPLE 1 : Les organisations humanitaires qui partagent des ensembles de données et analysent des données avec leurs propres ressources organisationnelles peuvent être considérées comme des responsables du traitement conjoints.

EXEMPLE 2 : Les organisations humanitaires qui partagent des ensembles de données mais externalisent l'analyse des données à un prestataire commercial qui transférera les constats et ne conservera aucun fichier pour son propre usage seront considérées comme des responsables du traitement conjoints ; le prestataire de services sera considéré comme un sous-traitant.

Une AIPD préalable aux opérations d'analyse des données peut être un moyen approprié pour préciser le rôle des différentes parties intervenant dans le traitement.

Une fois que les rôles ont été clairement définis et que les tâches correspondantes ont été allouées, il est important d'établir quels contrats les participants au traitement des données ont besoin de conclure. La collecte de données ou le transfert international de données entre organisations humanitaires, par-delà les frontières ou vers des organismes tiers (privés ou publics) doivent généralement être couverts par des clauses contractuelles, qui peuvent être critiques pour les raisons suivantes :

- Elles doivent clairement distribuer les rôles entre les différentes parties et, en particulier, leur notifier qu'elles agissent en qualité de responsables du traitement ou de sous-traitants (ou les deux).
- Elles doivent décrire les obligations respectives des parties en matière de protection des données et préciser les mesures que les parties doivent prendre pour protéger les données personnelles transférées à l'international.
- Elles doivent prévoir des obligations couvrant la sécurité des données, les mesures à prendre (opposition ou notification à l'autre partie) au cas où les autorités demanderaient à accéder aux données, les procédures de gestion des violations de données, la restitution/la suppression des données par le sous-traitant à l'issue du traitement et la formation du personnel.
- Elles doivent également exiger que les organisations humanitaires concernées soient informées de tout accès non autorisé aux données.

6.7 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

Les AIPD sont des outils importants qui garantissent, lors de la conception des projets, que tous les aspects de la réglementation applicable en matière de protection des données et les risques potentiels sont couverts¹⁰⁶. Les AIPD sont aujourd'hui exigées dans de nombreux États et par certaines organisations humanitaires. Cependant, leur mise en œuvre peut être plus difficile en ce qui concerne les nouvelles technologies, où les risques sont moins évidents. Les AIPD doivent non seulement préciser les détails et les spécifications du traitement, mais doivent aussi traiter les risques inhérents à celui-ci et les mesures d'atténuation.

En conséquence, les AIPD doivent être conduites avant les opérations d'analyse de données. Les outils d'évaluation des risques qui ont été expressément développés pour évaluer les risques inhérents à l'analyse de données dans les situations humanitaires, comme le Data Innovation Risk Assessment Tool du Global Pulse, sont particulièrement importants¹⁰⁷.

¹⁰⁶ Voir [chapitre 5 : Analyses d'impact relatives à la protection des données](#).

¹⁰⁷ PNUD, UN Global Pulse, *Risks, Harms and Benefits Assessment Tool*.

À titre indicatif, les risques à traiter dans une AIPD à des fins analytiques sont les suivants :

- réidentification des individus intéressant l'action humanitaire, lorsque la finalité de l'analyse est de dégager des tendances ;
- risques pour la viabilité et la sécurité des opérations humanitaires, lorsque sont traitées les données d'auteurs présumés de violations du droit international humanitaire ou du droit des droits humains ;
- risques que les demandes présentées par une organisation humanitaire en ce qui concerne des tendances particulières ou des catégories précises d'individus intéressant les autorités ou des entreprises puissent conduire ces tiers à discriminer ces individus ou à s'y intéresser autrement, ce qui aurait des implications néfastes pour ces individus et pour la neutralité de l'action humanitaire ;
- risques que les résultats de l'opération d'analyse de données effectuée par les organisations humanitaires auxquels un tiers a accès soient exploités par des tiers commerciaux ou par les autorités pour des finalités sans aucun lien ;
- risque que des parties dans une situation de violence ou de conflit puissent accéder aux résultats de l'analyse de données pour obtenir un avantage vis-à-vis d'autres parties prenantes et compromettent ainsi la sécurité des personnes concernées et la neutralité de l'action humanitaire ;
- risque que les prestataires commerciaux qui analysent leurs propres données ou qui traitent les données d'organisations humanitaires soient incités à exploiter les constats du traitement à des fins commerciales pour mieux comprendre leurs clients ou pour affiner le profilage de leur clientèle¹⁰⁸.

Les AIPD réalisées à des fins analytiques tiennent également compte de la probabilité, de l'ampleur et de la gravité du préjudice pouvant résulter des risques. Ces risques et ce préjudice doivent alors être évalués une nouvelle fois par rapport aux avantages attendus de l'analyse des données en tenant compte du principe de proportionnalité¹⁰⁹.

Les mesures suivantes peuvent être prises pour atténuer les risques :

- anonymisation en tant que mesure technique ;
- obligations légales et contractuelles pour empêcher la réidentification des personnes concernées¹¹⁰.

108 Voir [section 2.3 : Ensembles de données agrégées, pseudonymisées et anonymisées](#).

109 PNUD, UN Global Pulse, *Risks, Harms and Benefits Assessment Tool*.

110 Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, janvier 2017.

DRONES

UTILISATION POSSIBLE

OPÉRATIONS DE RECHERCHE
ET DE SAUVETAGE

CARTOGRAPHIE
DES SITUATIONS
D'URGENCE

COMPLÉMENT
AUX ACTIVITÉS
D'ASSISTANCE TRADITIONNELLES

DÉFIS

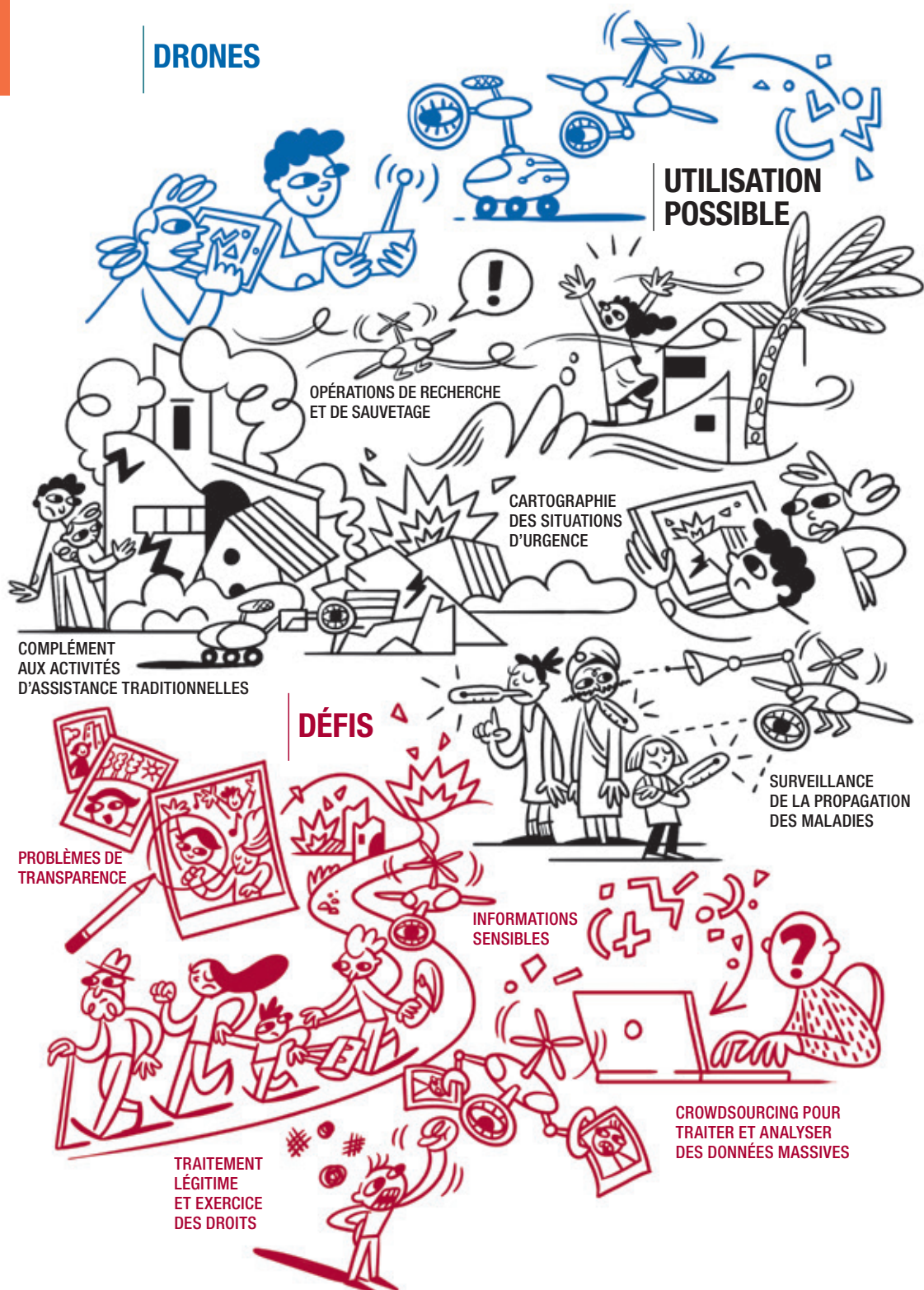
PROBLÈMES DE
TRANSPARENCE

SURVEILLANCE
DE LA PROPAGATION
DES MALADIES

INFORMATIONS
SENSIBLES

TRAITEMENT
LÉGITIME
ET EXERCICE
DES DROITS

CROWDSOURCING POUR
TRAITER ET ANALYSER
DES DONNÉES MASSIVES





CHAPITRE 7

DRONES/UAV ET TÉLÉDÉTECTION

7.1 INTRODUCTION

Les drones sont une nouvelle technologie prometteuse et puissante qui pourrait aider les organisations humanitaires à mieux apprécier une situation et à améliorer leurs interventions à la suite de catastrophes naturelles ou causées par l'homme ainsi que leurs opérations de secours. Ils peuvent compléter l'assistance humaine traditionnelle en rendant les opérations plus efficaces, plus rapides et plus sûres. Déployés correctement, ils pourraient avoir un impact important sur l'action humanitaire.

Les drones sont de petits engins, aériens ou non, fonctionnant de manière autonome ou pilotés à distance. On les appelle aussi UAV (de l'anglais *Unmanned Aerial Vehicles*), véhicules aériens sans pilote, aérodynes sans équipage, télépilotés ou programmés. Selon l'usage qui en est fait, ils peuvent être équipés de caméras, de microphones, de capteurs ou d'appareils GPS qui permettent de traiter des données personnelles.

Du point de vue de la protection des données, l'utilisation de drones suscite des préoccupations. Il faut toutefois préciser d'emblée que ce qui est intéressant dans les drones, ce n'est pas leur utilisation en tant que telle mais les différentes technologies dont ils sont équipés, telles que des caméras à haute résolution, des microphones, des équipements d'imagerie thermique ou des appareils pour intercepter les communications sans fil, autant de technologies qui permettent de collecter et de traiter des données. Dans cette optique, les considérations abordées dans ce chapitre pourraient aussi s'appliquer aux satellites et, plus généralement, à la télédétection.

Ce chapitre se limite aux problématiques posées par les drones du point de vue de la protection des données. D'autres questions et domaines du droit peuvent être pertinents, mais ils ne seront pas abordés ici. Aucune indication ne sera donnée, par exemple, sur le contrôle du trafic aérien, les licences de vol, les certificats de sûreté des équipements ou des questions similaires.

Dans le secteur humanitaire, les drones sont le plus souvent utilisés pour l'observation et la collecte de données afin de mieux évaluer une situation. Ces appareils trouvent ou peuvent trouver les applications suivantes :

- recherche et sauvetage ;
- localisation de personnes portées disparues ;
- collecte d'images aériennes/appréciation d'une situation/évaluation post-crise (surveillance de l'état des lignes d'électricité et des infrastructures, évaluation du nombre de blessés, de logements détruits, de bovins morts, etc.) ;
- surveillance de la propagation d'une épidémie au moyen de détecteurs de chaleur ;
- cartographie de camps d'urgence ;

- information en temps réel et suivi de situation au moyen de vidéos ou de photos permettant d'avoir une vue d'ensemble ;
- localisation de munitions non explosées ;
- cartographie de catastrophes naturelles et de sites de conflit ;
- localisation et suivi de personnes déplacées du fait d'une urgence humanitaire ;
- livraison de médicaments et d'autres matériels de secours dans des zones reculées ;
- installation d'un réseau maillé et rétablissement des réseaux de communication en relayant les signaux.

En situation de catastrophe, « les drones peuvent permettre aux secouristes de mieux apprécier une situation car ils sont capables de localiser les survivants dans les décombres, d'effectuer une analyse structurelle des infrastructures endommagées, d'acheminer les fournitures et les équipements nécessaires, d'évacuer des blessés et d'aider à éteindre les incendies, entre autres nombreuses applications¹¹¹ ». Les drones peuvent également recueillir des données aériennes dans des zones jugées dangereuses pour les prestataires d'aide humanitaire (par exemple les sites ayant subi une contamination radioactive ou en proie à des feux incontrôlés¹¹²).

Cela dit, bien que les drones puissent être une précieuse source d'informations directes et indirectes lors des interventions d'urgence, il est impératif de procéder à une évaluation critique avant d'y recourir car leur utilisation peut présenter des risques importants¹¹³. En dehors des questions de sécurité elles-mêmes (par exemple, accidents au cours du déploiement susceptibles de causer des dommages corporels et même des décès), ils peuvent, dans un scénario de conflit, être perçus comme un outil d'espionnage ou une intrusion, ce qui peut gravement compromettre la sécurité de leurs opérateurs et du personnel des organisations humanitaires et mettre aussi en danger les populations locales qui peuvent donner l'impression aux parties au conflit qu'elles ont consenti à ce que des drones soient utilisés pour leur compte.

¹¹¹ Joint Oversight Hearing by the Joint Legislative Committee on Emergency Management and the Senate Committee on Judiciary, *Drones and Emergencies: Are We Putting Public Safety at Risk?*, Background paper, California State Senate, 2015, p. 2 : https://sjud.senate.ca.gov/sites/sjud.senate.ca.gov/files/background_paper_-_drones_and_emergencies.pdf.

¹¹² Croix-Rouge américaine et al., *Drones for Disaster Response and Relief Operations*, avril 2015, p. 4 : <http://www.issuelab.org/resources/21683/21683.pdf>.

¹¹³ F. Delafoi, « Le drone, l'allié ambigu des humanitaires », Le Temps, 11 avril 2016 : <https://www.letemps.ch/monde/2016/04/11/drone-allie-ambigu-humanitaires> ; « What do Tanzanians Think About Drones? Now We know », ICTworks, 22 février 2016 : <http://www.ictworks.org/2016/02/22/what-do-tanzanians-think-about-drones-now-we-know/>.

EXEMPLE :

Une organisation humanitaire peut avoir été autorisée par les chefs communautaires locaux à se servir de drones pour obtenir des images aériennes d'une zone géographique étendue. Cependant, au cours de son déploiement, un drone peut accidentellement photographier une activité illégale intervenant en un point précis de la zone géographique en question et apporter ainsi des preuves de cette activité illégale. Les groupes qui exercent l'activité illégale, conscients qu'un drone les survole, peuvent vouloir retrouver et punir les chefs communautaires qui ont donné leur autorisation et rechercher aussi les opérateurs des organisations humanitaires pour détruire les preuves recueillies.

Comme mentionné plus haut, les préoccupations relatives à des violations potentielles des droits à la protection des données personnelles ne découlent pas de l'utilisation de drones mais du matériel embarqué, qui peut traiter des données personnelles. Les technologies de l'information intégrées ou connectées aux drones peuvent exécuter diverses activités et opérations de traitement des données (collecte, enregistrement, organisation, conservation et combinaison d'ensembles de données collectés...). Les données habituellement collectées par les drones sont des enregistrements vidéo, « des images (images de personnes, de maisons, de véhicules, de plaques d'immatriculation, etc.), des sons, des données géolocalisées ou tout autre signal électromagnétique relatif à une personne physique identifiée ou identifiable¹¹⁴ ». Des données de bonne qualité permettent d'identifier des personnes directement ou indirectement. Cette identification peut être effectuée par un opérateur humain ou automatiquement, par exemple en captant une image provenant d'un programme ou d'un algorithme de reconnaissance faciale, en scannant pour détecter un smartphone qui permettra d'identifier la personne ou en utilisant des puces d'identification par fréquence radio dans les passeports¹¹⁵.

Les organisations humanitaires peuvent considérer les facteurs suivants lorsqu'elles évaluent les mesures de protection des données à prendre lors de l'utilisation de drones :

- Il est techniquement possible de rendre des drones aériens « flight-specific », sur la base d'identifiants uniques intégrés à leur équipement de base.
- Une autorisation de voler et une licence de pilote à distance émise par les autorités étatiques sont nécessaires dans de nombreux pays¹¹⁶.
- Les données d'image (à divers degrés d'analyse et de qualité) sont les données les plus couramment collectées par les drones.

114 Groupe de travail « Article 29 », *Avis 01/2015 sur les questions de protection des données et de la vie privée liées à l'utilisation de drones*, p. 7 : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640602.

115 *Ibid.*, p. 14.

116 Storyhunter Guide to Commercial Drone Regulations Around the World : <https://blog.storyhunter.com/storyhunter-guide-to-commercial-drone-regulations-around-the-world-5795c31165d9>.

- L'altitude de vol et l'angle de capture des images ont aussi une incidence significative sur la probabilité d'identification directe ou indirecte des individus.
- Aujourd'hui, les drones peuvent capter des images extrêmement fines, mais bien que la technique progresse rapidement, la plupart ne peuvent pas encore saisir les visages. L'image doit être mise en relation avec d'autres ensembles de données pour permettre une identification. Lorsque l'identification faciale n'est pas possible, l'identification peut être réalisée grâce à d'autres données, notamment des données de localisation. L'utilisation de métadonnées (données qui donnent des informations sur d'autres données) est cruciale dans ce contexte.
- Il est important d'établir le lieu où sont conservées les données collectées et le type de traitement ; à cet égard, il existe une corrélation entre les drones et le recours à l'analyse de données¹¹⁷.
- Plusieurs initiatives internationales sont en cours en matière de normes et d'autres spécifications relatives à l'utilisation de drones, dont certaines concernent expressément l'utilisation de drones à des fins humanitaires. Les organisations humanitaires ont intérêt à suivre de près ces initiatives et à appliquer leurs constats dans leur pratique¹¹⁸.
- Les organisations humanitaires confient souvent les opérations par drones à des professionnels, ce qui pose la question de la protection des données (relation responsable du traitement/sous-traitant, accès aux données, etc.).
- Le traitement de données personnelles découlant du recours à des drones implique souvent des transferts internationaux, qui doivent avoir une base juridique en vertu du droit de la protection des données.

Il faut noter toutefois qu'étant donné l'évolution rapide de ces technologies, plusieurs des constats ci-dessus pourraient sensiblement changer dans un avenir proche.

Les organisations humanitaires doivent également réaliser que même lorsque le recours à des drones ne permet pas d'identifier des individus, il peut avoir d'importantes implications pour la vie, la liberté et la dignité des individus et des communautés. C'est pourquoi elles doivent prendre des précautions pour protéger les données recueillies par des drones, même si les individus enregistrés ne sont pas immédiatement reconnaissables.

EXEMPLE :

Si des tiers mal intentionnés accèdent aux données obtenues en suivant les flux de personnes déplacées à l'aide de drones, les individus vulnérables peuvent être exposés à des risques, même s'il est impossible de les identifier individuellement.

¹¹⁷ Voir [chapitre 6 : Analyse de données et big data](#).

¹¹⁸ Voir, par exemple, *Humanitarian UAV Code of Conduct & Guidelines* : <http://uaviators.org/docs>.

7.2 APPLICATION DES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

L'analyse de la protection des données présentée dans ce chapitre s'appuie sur les principes énoncés dans la première partie, où ils sont examinés en plus amples détails.

7.2.1 FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

Les organisations humanitaires peuvent traiter des données personnelles recueillies par des drones sur la base des fondements juridiques suivants¹¹⁹ :

- l'intérêt vital de la personne concernée ou d'une autre personne ;
- l'intérêt public, notamment l'intérêt public découlant du mandat dont une organisation est investie en vertu du droit national ou international ;
- le consentement ;
- l'intérêt légitime de l'organisation ;
- l'exécution d'un contrat ;
- le respect d'une obligation légale.

Dans la pratique, il sera sans doute impossible d'obtenir légalement un consentement pour le travail effectué par des organisations humanitaires à l'aide de drones.

À titre d'exemple, à chaque fois qu'un individu n'est pas libre d'entrer dans une zone surveillée ou d'en sortir, le consentement ne sera pas « librement donné ».

Il s'ensuit que le consentement apparaît globalement impossible à obtenir en tant que base juridique du traitement des données personnelles dans le contexte d'opérations par drones conduites par des organisations humanitaires. Les drones sont utilisés dans la plupart des situations où l'accès aux communautés est limité ou impossible. Même si cet accès était possible, il serait pratiquement impossible d'obtenir le consentement de toutes les personnes susceptibles d'être affectées par le traitement des données obtenues par des drones. En outre, en fonction des circonstances d'utilisation des drones, on peut douter que le consentement de personnes en détresse qui ont besoin d'assistance humanitaire puisse être considéré comme libre.

¹¹⁹ Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).



Les drones sont le plus souvent utilisés lorsque l'accès aux populations est limité ou impossible. Même lorsque cet accès est possible, il serait presque impossible d'obtenir le consentement de toutes les personnes susceptibles d'être affectées par le traitement de données obtenues par des drones.

Il a été suggéré qu'une alternative possible au consentement individuel pour l'utilisation de drones dans l'action humanitaire pourrait être le « consentement de la communauté » ou le « consentement des autorités ». Cela pourrait impliquer, par exemple, de n'obtenir que le consentement des représentants d'un groupe d'individus vulnérables et non des individus eux-mêmes. Cependant, le droit de la protection des données prévoit que le consentement doit être donné par l'individu.

EXEMPLE :

Les chefs communautaires ou les autorités étatiques peuvent consentir à ce qu'une organisation humanitaire déploie des drones en vue de cartographier un camp de réfugiés, mais les individus présents dans la région ne savent peut-être pas que des drones sont utilisés ou bien ils ne souhaitent pas être photographiés ou que leurs données personnelles soient recueillies par des drones.

Même lorsqu'il est impossible d'obtenir le consentement de l'individu concerné, l'organisation humanitaire peut traiter les données personnelles si elle établit que ce traitement peut être dans l'intérêt vital de la personne concernée ou d'une autre personne, ou en vertu d'une autre base juridique applicable (comme mentionné au début de la présente section). Autrement dit, le traitement des données personnelles est possible lorsqu'il est nécessaire pour protéger un intérêt essentiel pour la vie, l'intégrité, la santé, la dignité ou la sécurité de la personne concernée ou d'une autre personne.

Comme il est précisé au [chapitre 3 : Fondements juridiques du traitement des données personnelles](#), étant donné la nature du travail des organisations humanitaires et les situations d'urgence dans lesquelles elles interviennent, il peut exister, dans certaines circonstances, une présomption que le traitement des données nécessaire aux finalités humanitaires est dans l'intérêt vital d'une personne concernée¹²⁰.

Les organisations humanitaires doivent apprécier chaque situation au cas par cas afin de déterminer si la protection des intérêts vitaux de la personne concernée ou d'une autre personne nécessite effectivement le recours à des drones. La contribution des drones à la protection d'intérêts privés prioritaires comme la vie, l'intégrité et la sécurité doit être prouvée ou tout au moins probable compte tenu du type et du niveau de l'urgence, ou de préoccupations relatives à un manque d'information sur l'urgence auxquelles seul le recours à des drones permettrait de remédier. Des normes strictes doivent donc être appliquées pour déterminer si cette base juridique est applicable.

EXEMPLES :

- L'utilisation de drones dans des opérations de recherche et de sauvetage menées par une organisation humanitaire serait très probablement licite parce qu'elle protégerait l'intérêt vital de la personne concernée (c'est-à-dire de la personne disparue).
- En l'absence d'urgence particulière, l'utilisation de drones dans des opérations de cartographie menées par une organisation humanitaire serait très probablement illicite parce qu'il n'y a pas de lien direct avec les intérêts vitaux des personnes concernées qui vivent ou se déplacent dans les zones cartographiées.

Il est important que les organisations humanitaires procèdent à des évaluations soigneuses lorsque des motifs importants d'intérêt public sont en jeu et doivent servir de base juridique au traitement des données personnelles collectées par des drones. Ce sera habituellement le cas, notamment, lorsque l'activité en question est une partie importante d'un mandat humanitaire conféré par le droit national ou international (par exemple, pour le CICR, la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge, les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge, le Haut conseil de la République, le Fonds des Nations Unies pour l'enfance, le Programme alimentaire mondial ou l'Organisation internationale pour les migrations).

¹²⁰ Voir le Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016, considérant 46.

Les organisations humanitaires peuvent également traiter des données personnelles recueillies par des drones lorsqu'elles y ont un intérêt légitime, sous réserve que les droits et libertés fondamentaux des personnes concernées ne l'emportent pas sur celui-ci. L'intérêt légitime d'une organisation peut être établi lorsque le traitement des données personnelles contribue à la réalisation de sa mission ou la facilite. On peut arguer toutefois que lorsqu'il est impossible d'établir un intérêt public ou vital, il peut être difficile d'envisager des circonstances dans lesquelles les droits et les libertés des personnes concernées ne l'emporteraient pas sur l'intérêt légitime de l'organisation, en particulier lorsqu'il est impossible d'informer les individus dont les données personnelles seront probablement recueillies et que ceux-ci ne peuvent pas non plus exercer effectivement leurs droits à la protection des données.

EXEMPLE :

Une organisation humanitaire peut utiliser un drone pour démontrer la réussite d'une action, par exemple pour recueillir des séquences filmées aux fins d'une vidéo promotionnelle. Cette utilisation peut relever de l'intérêt légitime, même s'il serait nécessaire de bien réfléchir au risque de violation des droits et libertés des individus qui apparaissent dans la vidéo. À cet égard, la mesure dans laquelle les personnes concernées peuvent être informées et exercer effectivement leurs droits (y compris le droit d'opposition) est un facteur critique.

7.2.2 TRANSPARENCE/INFORMATION

Le principe de transparence exige de donner un minimum d'informations sur le traitement à la personne concernée. En outre, les informations et communications relatives au traitement doivent être aisément accessibles, faciles à comprendre et exprimées dans une langue claire et simple. Pour des raisons pratiques évidentes, ces exigences peuvent être difficiles à satisfaire dans le cas des drones. Le moment de l'information est également important ; dans les situations non urgentes, les informations doivent être idéalement données avant ou pendant les vols de drones. La participation des chefs communautaires et des autorités ou des campagnes média ciblées sur les personnes concernées envisagées (radio, quotidiens et affiches dans des lieux publics, par exemple) peuvent aider à satisfaire aux obligations de transparence.

EXEMPLE :

Pour s'acquitter de leurs obligations de transparence et d'information, les organisations humanitaires qui utilisent des drones pourraient apposer leur marque et leur signe sur les drones, créer des sites Internet ou donner des informations sur les réseaux sociaux, utiliser les canaux de communication locaux disponibles (radio, télévision, presse) et discuter avec les chefs communautaires.

7.2.3 LIMITATION DE(S) LA FINALITÉ(S) ET TRAITEMENT ULTÉRIEUR

Les finalités spécifiques de la collecte des données personnelles doivent être explicites et légitimes. Les organisations humanitaires peuvent utiliser des drones pour les finalités suivantes :

- recherche et sauvetage ;
- localisation de personnes portées disparues ;
- collecte d'images aériennes/appréciation de la situation, évaluation post-crise (par exemple, localisation de personnes déplacées qui ont besoin d'aide, surveillance de l'état du réseau d'électricité et des infrastructures, évaluation du nombre de blessés, de logements détruits, de bovins morts, etc.) ;
- surveillance de la propagation d'une épidémie au moyen de détecteurs de chaleur ;
- modélisation des foules lors de manifestations ;
- cartographie de camps d'urgence ;
- information en temps réel et suivi de situation au moyen de vidéos ou de photos permettant d'avoir une vue d'ensemble ;
- cartographie des catastrophes naturelles et des sites de conflit ;
- localisation de munitions explosives non explosées ;
- localisation et suivi de personnes déplacées du fait d'une urgence humanitaire ;
- livraison de médicaments et d'autres matériels de sauvetage dans des zones reculées ;
- installation d'un réseau maillé ou rétablissement des réseaux de communication en relayant les signaux.

Il a été établi au [chapitre 2 : Principes fondamentaux de la protection des données](#) qu'indépendamment de la base juridique du traitement, les organisations humanitaires peuvent traiter des données personnelles pour d'autres finalités que celles qui ont été spécifiées au moment de la collecte lorsque ce traitement ultérieur est compatible avec ces finalités initiales.

7.2.4 MINIMISATION DES DONNÉES

Les données personnelles ne peuvent être traitées que si elles sont adéquates, pertinentes et non excessives par rapport aux finalités de la collecte. C'est pourquoi la nécessité et la proportionnalité des données traitées doivent être évaluées strictement¹²¹. En outre, lorsque des drones sont utilisés à des fins humanitaires, le principe de minimisation des données doit être respecté en choisissant une technologie proportionnée et en adoptant, dès la conception et par défaut, des mesures de protection des données et de respect de la vie privée.

¹²¹ Voir [chapitre 2 : Principes fondamentaux de la protection des données](#).

Les organisations humanitaires pourraient, par exemple, envisager les options suivantes :

- Effectuer le paramétrage des services et produits relatif au respect de la vie privée évitant par défaut la collecte et le traitement ultérieur de données personnelles inutiles.
- Appliquer des techniques d'anonymisation.
- Flouter automatiquement des visages ou des individus (ou seulement certaines catégories d'individus particulièrement vulnérables).
- Augmenter l'altitude de vol ou l'angle de capture de l'image afin de réduire le risque de capter des images permettant d'identifier directement des individus.

7.2.5 CONSERVATION DES DONNÉES

Les données personnelles collectées à l'aide de drones ne doivent pas être conservées plus longtemps que ce qui est nécessaire à la finalité du traitement. Autrement dit, elles doivent être effacées ou anonymisées dès lors que la finalité pour laquelle elles ont été recueillies est atteinte. Il est également conseillé d'adopter des plannings de conservation et de suppression. Les appareils de collecte des données embarqués ou connectés à distance doivent être conçus de manière à permettre, s'ils doivent conserver les données, la définition de la durée de conservation et, de ce fait, la suppression automatique des données personnelles suivant un planning défini.

EXEMPLE :

Les données collectées par des drones pour aider une organisation humanitaire à répondre à un incident doivent en principe être effacées une fois l'incident résolu ; si l'organisation humanitaire souhaite archiver ces informations (par exemple à des fins historiques), elle doit prendre des mesures adéquates pour protéger l'intégrité et la sécurité des données et prévenir tout accès non autorisé.

7.2.6 SÉCURITÉ DES DONNÉES

Une organisation humanitaire qui déploie des drones doit instaurer des mesures de sécurité adéquates et appropriées aux risques en jeu¹²². Pour les drones, ces mesures pourraient consister à chiffrer les bases de données ou les dispositifs de stockage temporaire, et, s'il y a lieu, à chiffrer de bout en bout les données en transit entre le drone et la base.

¹²² Voir [chapitre 2 : Principes fondamentaux de la protection des données](#).

7.3 DROITS DES PERSONNES CONCERNÉES

Les droits des personnes concernées ont été décrits au [chapitre 2: Principes fondamentaux de la protection des données](#). Les remarques suivantes complètent ces informations pour ce qui concerne l'utilisation de drones par des organisations humanitaires¹²³.

S'agissant du droit à l'information, les informations suivantes doivent être données aux personnes concernées exposées au traitement de données collectées par des drones :

- l'identité du responsable du traitement des données recueillies par le drone et de son représentant ;
- les finalités du traitement ;
- les catégories de données personnelles recueillies ;
- les destinataires ou catégories de destinataires des données ;
- l'existence du droit d'accès aux données qui les concernent et du droit de rectifier ces données ;
- l'existence du droit d'opposition, lorsque c'est réaliste.

Dans la pratique, les organisations humanitaires pourraient avoir des difficultés à donner ces informations aux personnes concernées lorsqu'elles utilisent des drones pour collecter des données personnelles. Néanmoins, en fonction des circonstances, elles pourraient remédier à ce problème par des campagnes d'information, des notices publiques et d'autres mesures analogues. Les opérateurs de drones doivent publier des informations sur les différentes opérations réalisées et sur les opérations à venir sur leur site Internet ou sur des plateformes dédiées. Dans les zones reculées ou lorsqu'il est peu probable que les individus aient accès à Internet, les informations peuvent être publiées dans des quotidiens, dans des brochures ou sur des affiches ou être fournies par courrier ou par radiodiffusion.

Pour les drones susceptibles de couvrir de larges zones géographiques où il est difficile ou impossible d'informer les personnes concernées, il a été suggéré de créer une ressource nationale ou transnationale (plus facile à trouver que les sites Internet des opérateurs) pour permettre aux individus d'identifier les missions et les opérateurs associés aux drones.

Les personnes concernées doivent également avoir le droit de poser des restrictions au traitement, même si cela peut être difficile dans le cas des drones car elles peuvent se trouver dans l'impossibilité d'éviter la zone surveillée. En outre, les organisations sont vivement encouragées à incorporer des procédures de réclamation dans leurs pratiques en matière de traitement des données personnelles et leurs politiques internes de protection des données. Ces procédures doivent permettre de rectifier

¹²³ Voir [section 2.11: Droits des personnes concernées](#).

et de supprimer les données. Il faut toutefois reconnaître que certains fondements juridiques du traitement des données ne permettent pas l'exercice des droits individuels (à titre d'exemple, il est possible que les demandes de restrictions au traitement soumises par des personnes concernées ne soient pas respectées si le traitement est entrepris sur le fondement de l'intérêt public décrit plus haut).

Enfin, en ce qui concerne le droit d'accès à l'information, l'accès doit être limité afin d'atténuer les risques que l'accès d'une personne concernée puisse exposer les données personnelles d'autres personnes concernées ou que des personnes concernées mal intentionnées prennent des mesures défavorables à des individus vulnérables, qu'ils soient identifiables ou non.

Il est particulièrement difficile de limiter l'accès aux seules images ou vidéos aériennes comprenant les données personnelles d'une personne concernée puisque, par nature, les images ou vidéos peuvent contenir les données personnelles de nombreux autres individus qu'il serait très difficile d'exclure.

EXEMPLE :

Dans le cas de photographies aériennes collectées par des drones, l'exercice du droit d'accès des personnes concernées peut nécessiter le floutage des autres visages ou de données personnelles ne concernant pas le demandeur ; dans certains cas, le droit d'opposition pourrait comprendre la désidentification des données personnelles du demandeur sur la même photographie, mais pas la destruction de la photographie elle-même ou des données personnelles des autres personnes qui y figurent.

7.4 PARTAGE DE DONNÉES

Les circonstances dans lesquelles des organisations humanitaires partagent des informations personnelles entre elles ou avec des tiers doivent être définies et gérées du point de vue de la protection des données. Les informations recueillies par des drones peuvent être partagées au moment de la collecte ou ultérieurement, les organisations humanitaires pouvant externaliser le travail lié aux drones à des sous-traitants. Si une des situations ci-dessus implique un transfert de données personnelles par-delà les frontières nationales, il faut également tenir compte des aspects relatifs aux transferts internationaux de données¹²⁴.

¹²⁴ Voir [chapitre 4 : Transfert international de données](#).

Dans ces situations, il est important de réfléchir aux aspects suivants :

- Le rôle des organisations humanitaires concernées dans la protection des données¹²⁵.
- Si les images ou les autres informations partagées doivent contenir des données personnelles ou s'il suffit de partager les conclusions et les constats de l'analyse et de l'évaluation des images recueillies (pas de partage de données brutes).
- Partage involontaire ou accidentel de données (par exemple capture d'un appareil sur lequel des images sont enregistrées) ou absence de sécurisation ou de chiffrement de la transmission d'un flux d'images aériennes ; l'impact doit aussi être pris en considération par les organisations humanitaires concernées.

Le *crowdsourcing* est un moyen couramment employé pour traiter et analyser de larges ensembles de données recueillies par des drones car il est impossible pour les organisations humanitaires elles-mêmes d'examiner les masses d'images ou de séquence vidéo aériennes recueillies. Une pratique de plus en plus fréquente est de publier les images en ligne et d'inviter des bénévoles à les examiner pour repérer, par exemple, des lignes électriques coupées, des maisons détruites, des personnes affectées, du bétail, etc. Elle peut toutefois avoir de graves conséquences (par exemple permettre à des tiers potentiellement mal intentionnés d'accéder aux documents en ligne). Il est donc important :

- que les bénévoles qui ont accès aux images soient évalués, acceptés et formés par l'organisation humanitaire ;
- que les bénévoles signent un contrat de traitement comprenant des clauses de discrétion et de confidentialité ;
- que les documents ne soient pas publiés ni autrement partagés en dehors du groupe de bénévoles acceptés ;
- que les bénévoles reçoivent une aide appropriée pour comprendre les finalités du traitement des données ;
- que le traitement réalisé par les bénévoles soit dûment consigné dans un journal.

¹²⁵ Voir [section 7.6 : Relation entre le responsable du traitement et le sous-traitant](#).

7.5 TRANSFERT INTERNATIONAL DE DONNÉES

Le droit de la protection des données pose des restrictions aux transferts internationaux de données ; lorsqu'elles recourent à des drones, les organisations humanitaires doivent donc mettre en place des mécanismes conférant une base juridique à ces transferts, comme l'analyse le [chapitre 4 : Transfert international de données](#). Avant de procéder à un transfert international de données, elles doivent examiner s'il y a une base juridique en vertu du droit applicable et de leurs politiques internes. Une AIPD réalisée avant le transfert international de données pourrait conforter la licéité de ce traitement¹²⁶.

7.6 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Dans le cadre de l'utilisation de drones ou du traitement des données recueillies par ces appareils, le rôle du responsable du traitement et celui du sous-traitant peuvent être assez flous. Comme il est dit plus haut, le traitement des données recueillies par des drones est souvent externalisé. Il est donc indispensable de déterminer quelles sont les parties qui définissent effectivement les finalités et les moyens du traitement des données (et sont donc des responsables du traitement) et quelles sont celles qui prennent simplement leurs instructions auprès des responsables du traitement (et sont donc des sous-traitants). Il est possible également que plusieurs parties puissent être considérées comme des responsables du traitement conjoints.

EXEMPLES :

- Une organisation humanitaire dont le personnel utilise des drones pour ses propres finalités est le (seul) responsable du traitement.
- Une organisation humanitaire qui externalise la collecte de données par des drones à une entreprise spécialisée, dont la seule tâche est de piloter les drones, serait le (seul) responsable du traitement ; l'entreprise serait le sous-traitant pour cette opération.
- Deux organisations humanitaires qui souhaitent utiliser des drones et externaliser toutes les tâches opérationnelles à une entreprise qui n'a pas accès aux données recueillies sont des responsables du traitement conjoints. L'entreprise serait le sous-traitant pour cette opération.

¹²⁶ Voir [section 7.7 : Analyses d'impact relatives à la protection des données](#).

7.7 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

Comme il est expliqué au [chapitre 5: Analyses d'impact relatives à la protection des données](#), les AIPD sont des outils importants utilisés lors de la conception des projets pour garantir que tous les aspects de la réglementation applicable en matière de protection des données et les risques potentiels sont couverts. Les AIPD doivent non seulement préciser les détails et les spécifications du traitement, mais elles doivent aussi examiner les risques posés par l'opération et les mesures d'atténuation. À cet égard, il convient de souligner qu'elles doivent être réalisées avant toute opération de drone.

Pour ne pas retarder les opérations humanitaires, il convient d'établir à l'avance des modèles d'AIPD pour l'utilisation de drones. Ces modèles doivent couvrir les risques et considérations décrits dans ce chapitre et être faciles et rapides à compléter et mettre en œuvre.

BIOMÉTRIE



NIVEAU DE SENSIBILITÉ

UTILISATION POSSIBLE



IDENTIFICATION EFFICACE DES PERSONNES



IDENTIFICATION UNIQUE EN L'ABSENCE D'AUTRES MOYENS DE PROUVER SON IDENTITÉ

DÉFIS



FIABILITÉ DES DONNÉES



MINIMISATION DES DONNÉES



PROBLÈMES TECHNIQUES



IRRÉVERSIBILITÉ



DIFFICULTÉS LIÉES AU CONSENTEMENT



CONSIDÉRATIONS ÉTHIQUES

CHAPITRE 8

BIOMÉTRIE

8.1 INTRODUCTION

L'Organisation internationale de normalisation définit la reconnaissance biométrique et la biométrie comme la « reconnaissance automatisée des individus sur la base de leurs caractéristiques biologiques et comportementales¹²⁷ ». Les données biométriques sont donc des signatures humaines uniques et mesurables, qui peuvent être des empreintes digitales, un scan de l'iris ou des caractéristiques comportementales comme la démarche d'une personne.

Les implications, sur le plan de la protection des données, de l'utilisation de données biométriques, en particulier dans les passeports, cartes d'identité et documents de voyage, ont été soulignées par la Conférence internationale des commissaires à la protection des données et à la vie privée dans sa Résolution sur l'utilisation de la biométrie, adoptée en 2005 à Montreux, en Suisse¹²⁸.

Les organisations humanitaires du monde entier déploient de plus en plus la reconnaissance biométrique dans le cadre de leurs systèmes d'identification en raison des avantages qu'elle peut apporter sur le plan de la fiabilité de l'identification des individus et de la prévention des fraudes ou des détournements de l'aide humanitaire. Il est certain que les mécanismes d'identification sur papier (cartes d'identité, cartes de ration, bracelets, etc.) qui constituent l'alternative non numérique ont des limites car il est facile de les perdre et de les contrefaire, leur contrôle mobilise d'importantes ressources (ce qui peut donner lieu à des doublons et des inefficacités) et le traitement automatisé est rarement possible. Dans certaines situations, il est dès lors recommandé d'utiliser des systèmes d'identification biométrique (souvent comme moyen de vérification complémentaire) pour pallier ces insuffisances. Les données biométriques sont plus difficiles à contrefaire et, étant produites et conservées sous forme numérique, elles permettent d'assurer plus facilement une gestion efficace de l'aide humanitaire sur le terrain. Elles peuvent être également utilisées pour l'analyse de données ou d'autres types d'opérations avancées de traitement des données. En outre, étant axée sur les caractéristiques uniques de l'individu, la biométrie permet de confirmer l'identité de personnes qui n'ont pas d'autre moyen de prouver leur identité, ce qui arrive souvent dans le cas de personnes déplacées, contribuant ainsi à mettre l'identité et la dignité des personnes au cœur de l'action humanitaire¹²⁹.

¹²⁷ Voir ISO/IEC 2382-37:2017, *Technologies de l'information – Vocabulaire – Partie 37: Biométrie* : <https://www.iso.org/fr/standard/66693.html>.

¹²⁸ ICDPPC, Résolution sur l'utilisation de la biométrie dans les passeports, cartes d'identité et documents de voyage, Montreux, Suisse, 2005 : https://edps.europa.eu/sites/edp/files/publication/05-09-16_resolution_biometrics_fr.pdf.

¹²⁹ Voir, par exemple, Hugo Slim, « Eye Scan Therefore I am: The Individualization of Humanitarian Aid », European University Institute Blog, 2015 : <https://iow.eui.eu/2015/03/15/eye-scan-therfore-i-am-the-individualization-of-humanitarian-aid/> ; Paul Currión, « Eyes Wide Shut: The challenge of humanitarian biometrics », IRIN, 2015 : <http://www.irinnews.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics>.

Il faut noter toutefois que le déploiement des systèmes d'identification biométrique n'a pas toujours tenu ces promesses. Selon certaines sources, de graves problèmes de fiabilité des systèmes se seraient posés lors de la mise en œuvre de certains projets¹³⁰. Les limitations intrinsèques de la biométrie – comme le fait que les empreintes digitales ne sont pas toujours lisibles – posent aussi des difficultés. L'utilisation de données biométriques dans les systèmes d'identification nationaux et les problèmes hérités de ces systèmes dans certains pays peuvent aussi soulever des questions éthiques¹³¹. En outre, en raison de l'intérêt que présentent les données biométriques pour les forces de l'ordre et la sécurité nationale, les organisations humanitaires peuvent subir des pressions croissantes de la part des autorités nationales ou régionales qui leur demandent de partager leurs données pour des finalités allant au-delà du travail humanitaire. Étant donné l'intérêt suscité par les données biométriques, le risque d'accès non autorisé, c'est-à-dire de piratage, est important.

Les organisations humanitaires peuvent utiliser des technologies biométriques pour des opérations de traitement comme la collecte et la gestion de données relatives à des personnes déplacées qui doivent être enregistrées aux fins de la distribution de l'aide humanitaire, notamment l'aide fournie sous forme d'espèces ou de bons¹³².

Pour l'heure, les technologies déployées pour les opérations de traitement ci-dessus sont essentiellement des systèmes de reconnaissance automatique des empreintes digitales (les empreintes digitales étant la forme dominante de données biométriques collectées) et de reconnaissance de l'iris. D'autres formes de reconnaissance des données biométriques pourraient toutefois être envisagées, notamment :

- la reconnaissance des veines de la paume de la main ;
- la reconnaissance vocale ;
- la reconnaissance faciale ;
- la reconnaissance des caractéristiques comportementales.

Pour les organisations humanitaires, les technologies biométriques peuvent présenter les avantages suivants :

- identification fiable des individus ;
- lutte contre la fraude et la corruption ;
- soutien accru des donateurs et crédibilité renforcée des programmes (conséquence des points ci-dessus) ;
- gain de performance grâce au traitement numérique des données d'identification ;
- gains de performance sur le plan de la protection physique des individus et de la réduction du risque de disparition ;

¹³⁰ Gus Hosein et Carly Nyst, *Aiding surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*, IDRC/UKaid, 2014, p. 16 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229.

¹³¹ *Ibid.*, p. 19.

¹³² Voir [chapitre 9 : Programmes de transferts monétaires](#).

- identité et dignité des individus placées au cœur de l'action humanitaire ;
- renforcement du droit à la libre circulation des individus ;
- amélioration de la réinstallation d'individus dans des pays tiers ;
- possibilité d'ouvrir un compte bancaire.

Cela dit, des risques et défis ont également été pointés :

- fiabilité et exactitude des données (risques de faux positif) ou des systèmes – en dernier ressort, la qualité du système d'identification biométrique dépend de la qualité des capteurs et des données biométriques fournies ;
- difficultés techniques intrinsèques (par exemple, illisibilité des empreintes digitales de certains bénéficiaires dont les empreintes digitales sont partiellement effacées) ;
- caractère unique et non modifiable des données biométriques ;
- questions éthiques (sensibilités culturelles, perception des bénéficiaires ou préoccupations relatives à la surveillance) ;
- détournement d'usage (systèmes identiques utilisés à d'autres fins que celles pour lesquelles ils ont été initialement conçus, y compris à des fins non humanitaires) ;
- pressions possibles de diverses autorités nationales ou régionales (y compris les donateurs) en vue d'acquérir les ensembles de données biométriques recueillis par les organisations humanitaires, avec le risque que les données soient utilisées à d'autres fins que des fins strictement humanitaires (répression, sécurité, contrôle aux frontières ou surveillance des flux migratoires).

Il est donc très important que les organisations humanitaires analysent attentivement et prennent en compte le besoin éventuel d'utiliser des données biométriques, et qu'elles établissent de manière claire et transparente la façon dont elles comptent les utiliser en respectant les exigences en matière de protection des données, et ce, idéalement par le biais de politiques publiques sur l'utilisation des données biométriques¹³³.

8.2 APPLICATION DES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

L'utilisation des technologies biométriques soulève d'importantes questions de protection des données. Les données biométriques sont considérées comme des données personnelles et sont à ce titre couvertes par la législation relative à la protection des données. Le Règlement général européen sur la protection des données, par exemple, régit expressément les données biométriques et les

¹³³ Voir, par exemple, la politique sur le traitement des données biométriques par le CICR : <https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/>.

définit comme des « données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques¹³⁴ ». Dans de nombreux systèmes juridiques, les données biométriques sont considérées comme des « données sensibles¹³⁵ ». Par conséquent, des exigences particulières et précises s'appliquent au traitement de ces données et affectent directement la licéité du traitement si elles ne sont pas respectées.

Ce niveau supérieur de protection se justifie par les caractéristiques particulières des données biométriques ci-après :

- elles sont uniques et non modifiables, ce qui accroît les risques de vol d'identité ;
- l'évolution des technologies peut avoir des effets imprévisibles sur leur traitement parce que le type de données biométriques personnelles collectées aujourd'hui pourrait ultérieurement révéler beaucoup plus d'informations sur un individu (informations rétinienne révélant des informations génétiques, l'origine ethnique, l'état de santé et l'âge).

En conséquence, même si un des postulats de base de ce manuel est qu'il est impossible dans l'action humanitaire d'établir des catégories bien délimitées de données personnelles exigeant une protection particulière (parce que des données qui ne sont pas sensibles dans une situation d'urgence peuvent l'être dans une autre et inversement), le principe est que les données biométriques exigent une protection particulière, indépendamment de la situation et des circonstances. C'est la raison pour laquelle il faut toujours réaliser une AIPD avant de recourir à la biométrie.

Lorsqu'elles entreprennent une AIPD, les organisations humanitaires doivent tenir compte du fait que différents types de données biométriques peuvent avoir différents niveaux de « sensibilité ». Certaines catégories de données biométriques, tout en étant sensibles pour les raisons exposées plus haut, peuvent être plus ou moins sensibles que d'autres. Les empreintes digitales, par exemple, peuvent être atténuées ou effacées, involontairement (du fait de travaux manuels lourds) ou volontairement, ce qui rend ce type de données moins sensible que d'autres. En revanche, un scan d'iris peut permettre d'extraire des informations très sensibles allant au-delà de l'identification de l'individu. En outre, certaines données biométriques ne peuvent être recueillies et lues qu'avec la participation directe de la personne concernée, comme la reconnaissance par les veines de la paume, ce qui rend ces données moins sensibles que d'autres. D'autres catégories de données

¹³⁴ Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016, Article 4(14).

¹³⁵ Dans l'UE par exemple, les données biométriques sont considérées comme une catégorie particulière de données personnelles : *ibid.*, Article 9.

biométriques, comme les données de l'iris, peuvent être lues à distance, ce qui les rend particulièrement sensibles¹³⁶.

Par conséquent, même lorsque la législation gouvernant le traitement des données personnelles mentionnée plus haut ne s'applique pas, le traitement des données biométriques présente des risques particuliers et exige davantage de précautions. Il faut donc, préalablement au traitement, procéder à un examen approfondi pour déterminer si certaines garanties (mesures de sécurité renforcées par exemple) doivent être mises en place avant, pendant et après son exécution, comme il est expliqué plus loin, ou même s'il est opportun d'utiliser des données biométriques compte tenu des risques potentiels en jeu.

L'analyse de la protection des données présentée dans ce chapitre s'appuie sur les principes énoncés dans la première partie, où ils sont examinés en plus amples détails.

8.2.1 FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

Les organisations humanitaires peuvent traiter des données personnelles sur la base des fondements juridiques suivants¹³⁷ :

- l'intérêt vital de la personne concernée ou d'une autre personne,
- l'intérêt public,
- le consentement,
- l'intérêt légitime de l'organisation,
- l'exécution d'un contrat,
- le respect d'une obligation légale.

Comme il est expliqué au [chapitre 3 : Fondements juridiques du traitement des données personnelles](#), bien que le consentement soit la base juridique privilégiée du traitement des données personnelles, sa validité peut être difficile à prouver en situation humanitaire. Pourtant, les données biométriques sont considérées comme des données sensibles et à ce titre, les responsables du traitement doivent obtenir le consentement des individus. En outre, étant donné que les données biométriques ne peuvent être recueillies que directement auprès des individus concernés, les organisations humanitaires ont généralement la possibilité d'obtenir le consentement à l'utilisation de données biométriques – ce qui n'est pas le cas pour d'autres méthodes de collecte et de traitement des données. Toutefois, elles n'ont pas toujours la possibilité de recueillir un consentement libre, non équivoque, éclairé et documenté au traitement des données biométriques, pour les raisons

¹³⁶ Voir, par exemple : « How Facial Recognition Might Stop the Next Brussels », 22 mars 2016, <http://www.defenseone.com/technology/2016/03/how-facial-recognition-might-stop-next-brussels/126883/>.

¹³⁷ Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

également exposées au [chapitre 3: Fondements juridiques du traitement des données personnelles](#), telles que :

- l'incapacité physique des individus à les communiquer, par exemple dans le cas de patients inconscients (lorsque, par exemple, des données biométriques peuvent être nécessaires pour ouvrir le dossier médical du patient, en association avec un autre pouvoir légitime pour ouvrir le dossier) ;
- le manque de temps et de personnel pour garantir aux patients des conseils appropriés durant les premières phases d'une urgence, où la priorité est d'apporter des soins vitaux ;
- la vulnérabilité des individus ou leur incapacité juridique à donner leur consentement ;
- la haute technicité et l'irréversibilité des données, qui peuvent exposer les individus à des risques difficiles à appréhender ou à envisager au moment où le consentement est donné. Il s'agit en particulier de la possibilité que la science et les technologies connaissent une évolution qui engendre de nouveaux risques non prévus au moment du consentement (par exemple des informations génétiques qui deviennent accessibles à partir de la reconnaissance de l'iris) ;
- aucun choix réel n'est donné quant aux autres moyens d'obtenir de l'assistance ou une protection (par exemple, si votre survie ou celle de votre famille dépend de l'aide humanitaire ou si vous avez besoin de vous enregistrer pour rester légalement dans le pays où vous vous trouvez, vous n'avez guère la possibilité de refuser que l'on collecte vos données biométriques).



Une réfugiée syrienne scanne son iris dans une agence de la Cairo Amman Bank pour accéder à l'assistance mensuelle en espèces, Amman, Jordanie.

Même lorsqu'il est impossible d'obtenir un consentement valable de l'individu, c'est-à-dire de la personne concernée, l'organisation humanitaire peut traiter les données personnelles si elle établit que ce traitement est dans l'intérêt vital de la personne concernée ou d'une autre personne, c'est-à-dire qu'il est nécessaire pour protéger un intérêt essentiel pour la vie, l'intégrité, la santé, la dignité ou la sécurité de la personne concernée ou d'une autre personne.

Dans certains cas, la nature du travail des organisations humanitaires et les conditions d'urgence dans lesquelles elles interviennent dans des conflits armés et dans d'autres situations de violence conduisent à postuler que le traitement des données personnelles est dans l'intérêt vital d'une personne concernée ou d'une autre personne (par exemple, en cas de menaces imminentes contre l'intégrité physique et mentale des personnes concernées).

On pourrait faire valoir que dans des conditions difficiles, en raison de l'efficacité des techniques biométriques pour identifier les individus, l'intérêt vital de la personne concernée ou d'une autre personne peut constituer une autre base juridique plausible du traitement lorsque les organisations humanitaires ne peuvent pas obtenir le consentement des individus. De plus, on peut imaginer une situation dans laquelle la défense de l'intérêt vital des bénéficiaires justifierait l'utilisation de systèmes biométriques. Si, par exemple, les ressources disponibles pour l'action humanitaire sont limitées et si les bénéficiaires potentiels ne reçoivent pas l'assistance essentielle parce que l'aide est frauduleusement apportée en excès à un autre groupe d'individus, les systèmes biométriques peuvent faciliter une bonne affectation des ressources et la prévention des fraudes. D'un autre côté, on peut aussi affirmer que les données biométriques ne sont pas essentielles pour la distribution de l'aide. L'utilisation de données biométriques répond moins à l'intérêt vital des personnes concernées qu'au besoin qu'ont les organisations humanitaires de travailler efficacement et rationnellement, en évitant le risque de duplication et le gaspillage des ressources financières.

En outre, il est important de préciser le cycle de vie des données biométriques. S'il est prévu d'utiliser ces données tout au long de la vie d'un individu, la base juridique de l'intérêt vital de cette personne ne sera sans doute pas applicable, et il faudra obtenir son consentement.

Une dernière considération dans ce domaine a trait à la valeur intrinsèque des données biométriques pour l'identification claire et non équivoque des personnes affectées par une urgence humanitaire et au rôle qu'elles peuvent jouer pour restaurer ou conforter la dignité d'un individu, notamment en lui permettant d'exercer ses droits. De ce point de vue, l'intérêt vital d'une personne concernée pourrait bien être en jeu.

Dans certaines situations, des motifs importants d'intérêt public peuvent être la base juridique du traitement de données biométriques. Ce sera généralement le cas, par exemple, lorsque l'activité en question relève d'un mandat humanitaire établi par le droit national ou international. Ce fondement peut être pertinent dans le cadre de distributions d'aide, où il n'est pas toujours possible d'obtenir le consentement des bénéficiaires. Il faut souligner que si la vie, la sécurité, la dignité et l'intégrité de la personne concernée ou d'autres personnes sont en jeu, l'intérêt vital peut être la base juridique la plus appropriée.

L'intérêt public pourrait être une base juridique appropriée du traitement des données biométriques lorsqu'un mandat d'exécution d'une action humanitaire est établi en droit national, régional ou international et lorsque le consentement ou l'intérêt vital ne s'appliquent pas, comme dans les situations analysées plus haut.

Les organisations humanitaires peuvent également traiter des données personnelles lorsqu'elles y ont un intérêt légitime, sous réserve que les droits et libertés fondamentaux de la personne concernée ne l'emportent pas sur cet intérêt. Cet intérêt légitime peut comprendre le traitement nécessaire pour accroître l'efficacité de l'aide humanitaire apportée et réduire les coûts et les risques de duplication et de fraude. Toutefois, étant donné que les données biométriques peuvent être utilisées à des fins potentiellement intrusives et qu'elles présentent des caractéristiques particulières (évoquées plus haut), on peut se demander si les droits et les libertés d'une personne concernée ne l'emportent pas toujours sur l'intérêt légitime. Pour que l'intérêt légitime du responsable du traitement puisse servir de base juridique, l'AIPD doit d'abord comprendre une analyse approfondie des risques et des ingérences possibles dans les droits et libertés fondamentaux de la personne concernée. C'est particulièrement important s'il existe un risque que des tiers obtiennent un accès non autorisé aux données ou fassent pression sur les organisations humanitaires pour les amener à fournir ces données très sensibles et les utiliser à des fins non exclusivement humanitaires.

8.2.2 TRAITEMENT ÉQUITABLE ET LICITE

En vertu du droit de la protection des données, le traitement des données personnelles doit être licite et équitable¹³⁸. Pour être licite, le traitement doit avoir une base juridique appropriée. L'exigence d'équité est généralement liée à l'information des personnes et à l'utilisation des données. Les organisations humanitaires qui traitent des données biométriques doivent garder à l'esprit que ces principes s'appliquent à tous les stades du traitement.

138 Voir [section 2.5.1 : Principes de licéité, de loyauté et de transparence du traitement](#), et [section 8.2.2 : Traitement équitable et licite](#).

8.2.3 LIMITATION DE(S) LA FINALITÉ(S) ET TRAITEMENT ULTÉRIEUR

Comme expliqué au [chapitre 2: Principes fondamentaux de la protection des données](#), au moment de la collecte des données personnelles, l'organisation humanitaire doit déterminer et exposer les finalités précises du traitement des données. Ces finalités doivent être explicites et légitimes et peuvent comprendre des finalités humanitaires comme la distribution d'aide humanitaire, le rétablissement des liens familiaux, la protection des individus placés en détention, l'assistance médicale ou les activités médico-légales.

Les finalités du traitement doivent être clairement exposées aux individus au moment de la collecte. Les informations biométriques étant utilisées pour l'identification des individus, les finalités du traitement doivent être les finalités initiales de l'identification (l'identification elle-même, le déboursement de l'aide par des biens en nature ou des paiements en espèces, par exemple).

Les données personnelles peuvent être traitées à d'autres fins que celles qui ont été initialement spécifiées au moment de la collecte lorsque le traitement ultérieur est compatible avec ces finalités et, en particulier, lorsqu'il est nécessaire à des fins historiques, statistiques ou scientifiques. Pour déterminer si le traitement ultérieur est compatible avec les finalités de la collecte initiale, les facteurs suivants doivent être pris en compte :

- tout lien entre les finalités de la collecte et celles du traitement ultérieur envisagé ;
- la mesure dans laquelle le traitement ultérieur a un caractère humanitaire ;
- la situation dans laquelle les données personnelles ont été recueillies et, en particulier, la relation entre les personnes concernées et le responsable du traitement, et les attentes éventuelles des personnes concernées ;
- la nature des données personnelles ;
- les conséquences ou risques potentiels du traitement ultérieur envisagé pour les personnes concernées ;
- l'existence de garanties appropriées ;
- les attentes raisonnables des personnes concernées quant à l'utilisation future des données.

EXEMPLE :

Lorsqu'une organisation humanitaire déploie un système d'identification biométrique pour la distribution de l'aide et que les individus concernés y ont consenti, le même système ne peut pas être utilisé pour transmettre les données des participants aux donateurs de l'organisation humanitaire à des fins de référencement croisé, à moins que les participants aient également consenti à cette finalité.

Il convient d'être particulièrement attentif, dans l'examen des facteurs ci-dessus, aux aspects humanitaires de la finalité du traitement.

Comme il est expliqué plus haut¹³⁹, les finalités qui entrent dans la catégorie plus générale des finalités « humanitaires » ont toutes les chances d'être compatibles avec des opérations de traitement ultérieur. Toutefois, ce ne serait pas le cas si de nouveaux risques entrent en jeu ou si le traitement ultérieur engendre, pour les personnes concernées, des risques supérieurs à ses avantages. Cette évaluation dépendrait des circonstances et comprendrait une analyse des risques que le traitement puisse être contraire aux intérêts de la personne à laquelle les informations ont trait ou de sa famille, et qu'il risque notamment de porter atteinte à leur vie, à leur intégrité, à leur dignité, à leur sécurité psychologique ou physique, à leur liberté ou à leur réputation.

Dans le même esprit, le traitement ultérieur pour des finalités non humanitaires (par exemple répression ou sécurité nationale, contrôles de sécurité, gestion des flux migratoires ou demandes d'asile) doit être considéré comme incompatible avec le traitement initial entrepris par l'organisation humanitaire. De même, des finalités qui pourraient être considérées comme humanitaires mais qui engendrent de nouveaux risques pour les individus, comme la gestion des migrations et les demandes d'asile, ou l'identification par les autorités, ne peuvent constituer un traitement ultérieur compatible.

8.2.4 MINIMISATION DES DONNÉES

Les données personnelles traitées doivent être adéquates et utiles aux finalités de la collecte. Cela implique en particulier de ne pas recueillir trop de données et de limiter au minimum nécessaire la durée de conservation des données. Dans l'idéal, la quantité de données personnelles recueillies et traitées doit être limitée à ce qui est nécessaire pour les finalités spécifiées de la collecte et du traitement des données ou d'un traitement ultérieur compatible.

Les données biométriques collectées à des fins d'identification doivent être proportionnées à ces finalités, c'est-à-dire qu'il ne faut collecter et traiter que la quantité de données biométriques nécessaire pour l'identification des individus ; les informations « en surplus » qui ne sont pas utiles à l'identification ne doivent pas être collectées et, si elles le sont, elles doivent être effacées. De même, l'éventail des ensembles de données biométriques collectées doit être limité à ce qui est proportionné (la collecte d'images faciales ou de scans d'iris ne sera peut-être pas considérée comme proportionnée si on utilise déjà des photos et des empreintes digitales pour l'identification).

¹³⁹ Voir [section 8.2.3: Limitation de\(s\) la finalité\(s\) et traitement ultérieur](#).

La compartimentation des données collectées à l'intérieur d'un système biométrique (accès autorisé sur la base du besoin de savoir) pourrait être, pour les organisations humanitaires, un moyen intéressant de répondre aux exigences de minimisation des données.

D'autre part, le principe de minimisation des données doit amener les organisations humanitaires, lorsqu'elles conçoivent un programme impliquant la collecte de données biométriques, à collecter le moins d'identifiants biométriques possible pour atteindre la finalité d'identification pour l'action humanitaire en question.

EXEMPLE :

Pour identifier un bénéficiaire et éviter les fraudes et les duplications, la collecte d'une seule source de données biométriques (comme une empreinte digitale) peut être suffisante ; corrélativement, la collecte d'une combinaison de plusieurs empreintes digitales et d'un scan d'iris peut être disproportionnée et contraire au principe de minimisation des données.

8.2.5 CONSERVATION DES DONNÉES

Les informations biométriques posent des problèmes de sécurité qui peuvent être résolus par la suppression ou la destruction des données après le traitement ou par une politique de conservation des données soigneusement structurée, qui décrit les conditions de la suppression ou de la destruction ou les autres solutions à appliquer, comme l'anonymisation ou les restrictions d'accès. Il faut donc éviter de conserver des données en vue d'un traitement ultérieur, à moins que celui-ci soit clairement défini et nécessaire durant la période de conservation au regard des finalités pour lesquelles les données ont été collectées initialement. Les organisations humanitaires doivent établir leurs politiques internes de conservation des données en fonction du type de données collectées et de l'utilisation qui pourra en être faite.

8.2.6 SÉCURITÉ DES DONNÉES

Étant donné la sensibilité des informations biométriques et les risques d'utilisation abusive en cas d'accès non autorisé consenti ou autrement obtenu¹⁴⁰, il est impératif que l'organisation humanitaire qui détermine les finalités et les moyens du traitement (c'est-à-dire le responsable du traitement) applique des mesures de sécurité adéquates et proportionnées. Le chiffrement ou la compartimentation des informations, par exemple, pourraient constituer des solutions viables à cette fin.

140 Sarah Soliman, « Tracking Refugees With Biometrics: More Questions Than Answers », War on the Rocks Blog, 9 mars 2016 : <https://warontherocks.com/2016/03/tracking-refugees-with-biometrics-more-questions-than-answers/>.

8.3 DROITS DES PERSONNES CONCERNÉES

Les droits des personnes concernées décrits au [chapitre 2: Les principes fondamentaux de la protection des données](#) incluent le droit à l'information, le droit d'accès, le droit de rectification, le droit de suppression et le droit d'opposition.

S'agissant du droit à l'information, il est souvent plus facile pour les responsables du traitement de donner des informations adéquates sur les détails du traitement lorsque des données sont recueillies directement auprès des personnes concernées, comme c'est le cas des données biométriques. Compte tenu des importants risques supplémentaires en jeu, le niveau d'information à fournir si les données sont traitées sur la base du consentement sera élevé. Ces informations doivent comprendre des éléments sur les implications possibles de l'accès de tiers aux données biométriques dans le cadre du traitement requis pour la mise en œuvre du projet biométrique. Au départ, il est possible que l'organisation humanitaire n'envisage pas de donner accès à des tiers ou qu'elle ne connaisse pas les conséquences possibles. Ce peut être le cas, par exemple, en cas de partage des données avec les États d'accueil aux fins du traitement des réinstallations. Ce scénario, non anticipé au moment de la collecte, exigerait de recueillir séparément le consentement après l'enregistrement initial/biométrique.

Une infrastructure adéquate doit être mise en place pour faciliter l'exercice du droit d'accès, du droit d'opposition, du droit de suppression et du droit de rectification lorsqu'on recourt à la biométrie. À cet égard, il est souhaitable de prévoir des procédures de réclamation dans les politiques internes de protection des données et de les appliquer dans le cadre du traitement des données personnelles.

8.4 PARTAGE DE DONNÉES

Le traitement biométrique peut comprendre un partage de données avec des tiers dans les scénarios suivants :

- L'organisation humanitaire fait appel à un sous-traitant pour fournir la technologie biométrique nécessaire à la collecte et au traitement des données. Dans ce cas, une relation de type responsable du traitement/sous-traitant est instaurée.
- L'organisation humanitaire transfère les données à un tiers, qui devient un nouveau responsable du traitement.
- Les autorités du pays d'accueil demandent ou exigent une copie des données biométriques collectées sur leur territoire, soit en masse, soit pour des individus précis.

Il est important de tenir compte des exigences en matière de protection des données avant de procéder au partage et de noter que le « partage » couvre non seulement les situations dans lesquelles les données sont activement transférées à des tiers, mais aussi celles dans lesquelles elles sont simplement rendues accessibles à des tiers. Étant donné la sensibilité des données biométriques, il faut être particulièrement prudent avant de partager des données.

8.5 TRANSFERT INTERNATIONAL DE DONNÉES

Le traitement de données biométriques peut impliquer un transfert de données personnelles vers des parties situées dans différents pays, comme dans le cas du transfert international de données entre différentes organisations humanitaires ou entre des organisations humanitaires et des tiers du secteur public ou privé.

Le droit de la protection des données pose des restrictions aux transferts internationaux de données, et les organisations humanitaires doivent mettre en place des mécanismes conférant une base juridique à ces transferts lorsqu'elles recourent à la biométrie, comme on l'a vu plus haut¹⁴¹. Avant d'entreprendre un transfert international de données, elles doivent déterminer si celui-ci possède un fondement juridique en vertu du droit applicable et de leurs politiques internes. La réalisation d'une AIPD¹⁴² préalable au partage pourrait conforter la licéité de ce traitement du point de vue de la protection des données.

8.6 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Le déploiement de systèmes d'identification biométrique par une organisation humanitaire peut impliquer l'externalisation de travaux à des opérateurs locaux pour la mise en œuvre sur site des projets. Ces technologies très avancées requièrent l'appui de prestataires spécialisés. Les organisations humanitaires peuvent également coopérer entre elles en partageant des bases de données biométriques (voir plus haut). Les autorités étatiques (comme les forces de l'ordre) peuvent faire pression sur les organisations humanitaires pour accéder aux données biométriques que celles-ci détiennent (par exemple en cas de migration ou de déplacement forcé), soit en masse, soit pour des individus particuliers.

Compte tenu de ce qui précède, il est indispensable de déterminer quelles parties définissent effectivement les finalités et les moyens du traitement des données (et sont donc les responsables du traitement) et quelles parties prennent

¹⁴¹ Voir [section 8.2.1: Fondements juridiques du traitement des données personnelles](#).

¹⁴² Voir [section 8.7: Analyses d'impact relatives à la protection des données](#).

simplement leurs instructions auprès des responsables du traitement (et sont donc des sous-traitants). Une fois que les rôles sont clairement définis et que les tâches correspondantes sont attribuées, le transfert international de données entre organisations humanitaires ou entre pays ou vers le secteur public ou privé ne doit intervenir que si des clauses contractuelles appropriées définissant les responsabilités des parties sont signées. Il faut en outre soigneusement déterminer si les sous-traitants engagés sont en mesure de respecter pleinement les exigences de sécurité et de ségrégation. Cette considération est particulièrement importante pour les technologies biométriques, car certains sous-traitants peuvent gérer des travaux pour de multiples responsables du traitement et lorsque des organisations humanitaires et des autorités figurent parmi ces responsables du traitement, le risque d'une ségrégation insuffisante des ensembles de données doit être soigneusement évalué. Réalisées avant le traitement des données biométriques, les AIPD peuvent être un moyen approprié de préciser les rôles des différentes parties intervenant dans le traitement.

8.7 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

Les AIPD sont des outils importants qui garantissent, lors de la conception des projets, que tous les aspects de la réglementation applicable en matière de protection des données et les risques potentiels, soulignés ci-dessus, sont couverts.

Une AIPD doit être effectuée à chaque fois qu'une organisation humanitaire traite des données biométriques. Elle doit préciser les détails et les spécifications du traitement et souligner les risques potentiels et les mesures d'atténuation possibles afin de déterminer s'il convient de collecter des données biométriques et, dans l'affirmative, quelles garanties doivent être mises en place. Soulignons ici que l'AIPD doit précéder le traitement des données biométriques.

PROGRAMMES DE TRANSFERTS MONÉTAIRES

UTILISATION POSSIBLE

SOUTIEN AUX
MARCHÉS LOCAUX

LIBERTÉ
DE CHOIX

TRANSPARENCE
QUANT À L'AIDE
EFFECTIVEMENT
FOURNIE AUX
BÉNÉFICIAIRES

DÉFIS

PLUS DE DONNÉES
PERSONNELLES PAR
RAPPORT À L'AIDE
EN NATURE

OBTENTION D'UN
CONSENTEMENT
ACTIF ET ÉCLAIRÉ

CONSERVATION
DES
DONNÉES

PARTAGE
DE DONNÉES

UTILISATION ULTÉRIEURE
À DES FINS INCOMPATIBLES

CHAPITRE 9

PROGRAMMES DE TRANSFERTS MONÉTAIRES

9.1 INTRODUCTION

Les programmes de transferts monétaires sont des outils prometteurs de soutien aux processus de survie et de relèvement après une urgence humanitaire. Les termes « programmes de transferts monétaires », « aide sous forme d'espèces et de bons », « interventions monétaires » et « aide en espèces » peuvent être employés indifféremment et recouvrent tous les types de transferts monétaires, c'est-à-dire les transferts sous forme de bons et d'espèces, et tous les types de mécanismes de fourniture¹⁴³.

Les transferts monétaires sont très respectueux de la liberté de choix des bénéficiaires et des arbitrages qu'ils doivent opérer. Le monde humanitaire continue d'utiliser divers systèmes d'aide sous forme d'espèces et de bons, qui vont des coupons à échanger contre des produits spécifiques ou contre des services de fournisseurs spécifiques, aux transferts d'espèces conditionnés au respect de certaines exigences par les bénéficiaires, en passant par les transferts sans aucune restriction ni condition qui peuvent être utilisés pour tout ce dont peuvent nécessiter les personnes touchées par une urgence humanitaire¹⁴⁴.

L'assistance monétaire électronique peut revêtir différentes formes, comme l'argent électronique, somme envoyée aux bénéficiaires qu'il est possible de convertir en espèces ou de dépenser sans restrictions (par exemple via un téléphone mobile, des cartes prépayées, des virements bancaires), et les bons électroniques, qui sont envoyés aux bénéficiaires (via des cartes à puce ou des téléphones mobiles) et peuvent être échangés auprès de commerçants agréés contre des articles approuvés, des restrictions aux dépenses étant possibles¹⁴⁵. On utilise parfois aussi de l'argent liquide, ainsi que des bons papier.

Il est largement admis que l'efficacité et l'adéquation de l'aide humanitaire en espèces dépendent de la situation (les individus peuvent-ils obtenir les articles dont ils ont besoin dans une situation donnée?)¹⁴⁶. Bien que des inquiétudes aient

¹⁴³ Voir « Glossary of Cash Transfer Programming (CTP) Terminology » : https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/092017_cash_transfer_programming_terminology_glossary.pdf.

¹⁴⁴ ODI Center for Global Development, *Doing cash differently: How cash transfers can transform humanitarian aid – Report of the High Level Panel on Humanitarian Cash Transfers*, septembre 2015, p. 11 : <https://odi.org/en/publications/doing-cash-differently-how-cash-transfers-can-transform-humanitarian-aid/>.

¹⁴⁵ Commission européenne, *10 common principles for multi-purpose cash-based assistance to respond to humanitarian needs*, mars 2015 : http://ec.europa.eu/echo/files/policies/sectoral/concept_paper_common_top_line_principles_en.pdf; DG ECHO Funding Guidelines, *The use of cash and vouchers in humanitarian crises*, mars 2013 : http://ec.europa.eu/echo/files/policies/sectoral/ECHO_Cash_Vouchers_Guidelines.pdf.

¹⁴⁶ Paul Harvey et Sarah Bailey, *Cash transfer programming and the humanitarian system, Background Note for the High Level Panel on Humanitarian Cash Transfers*, mars 2015 : <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9592.pdf>.

été exprimées au sujet des programmes de transferts monétaires (notamment concernant le risque qu'ils provoquent une inflation sur le marché local), des données probantes montrent que l'aide sous forme d'espèces et de bons est « plus efficace que l'aide en nature¹⁴⁷ ».

Les recherches montrent qu'un recours accru aux transferts monétaires à des fins humanitaires, lorsqu'ils sont appropriés, non assortis de restrictions et effectués sous forme de paiements électroniques chaque fois que possible, offre notamment les avantages suivants¹⁴⁸ :

- donner la liberté de choix et un meilleur contrôle sur leur vie aux personnes affectées par une crise ;
- améliorer l'adéquation du système humanitaire avec les besoins des individus ;
- accroître la transparence de l'aide humanitaire et mieux prévenir les fraudes en montrant la quantité d'aide qui parvient effectivement à la population cible ;
- accroître la redevabilité de l'aide humanitaire, tant envers les populations affectées qu'envers les contribuables des pays donateurs ;
- réduire potentiellement les coûts de fourniture de l'aide humanitaire pour tirer le meilleur parti de budgets limités ;
- soutenir les marchés et les emplois locaux ainsi que les revenus des producteurs locaux ;
- renforcer l'acceptation de l'aide humanitaire par les populations locales ;
- accélérer l'intervention humanitaire et lui conférer plus de flexibilité ;
- accroître l'inclusion financière en connectant les personnes à des systèmes de paiement.

Cependant, il existe aussi des défis et des difficultés. La mise en place d'aides sous forme d'espèces et de bons dans certaines situations d'urgence humanitaire n'est pas toujours une solution optimale (par exemple lorsque les produits et services nécessaires ne sont pas disponibles, lorsque les autorités locales s'opposent à ce type d'aide humanitaire ou lorsqu'il existe un risque d'inflation sur le marché concerné)¹⁴⁹. Les transferts monétaires sont simplement un outil qui permet d'atteindre l'objectif d'un programme ; ils s'inscrivent ainsi souvent dans le cadre de programmes d'assistance humanitaire plus vastes, comprenant des mesures de protection ou des services d'assainissement ou de santé¹⁵⁰. Pour que les programmes de transferts monétaires fonctionnent correctement, les organisations humanitaires doivent traiter des données personnelles, souvent concernant le statut socioéconomique et les vulnérabilités d'individus ou de groupes d'individus. Cela engendre des menaces et des risques d'atteinte à la vie privée inhérents à la collecte et au traitement des données personnelles des bénéficiaires, en particulier au vu des flux de données complexes qu'ils impliquent. L'utilisation de technologies

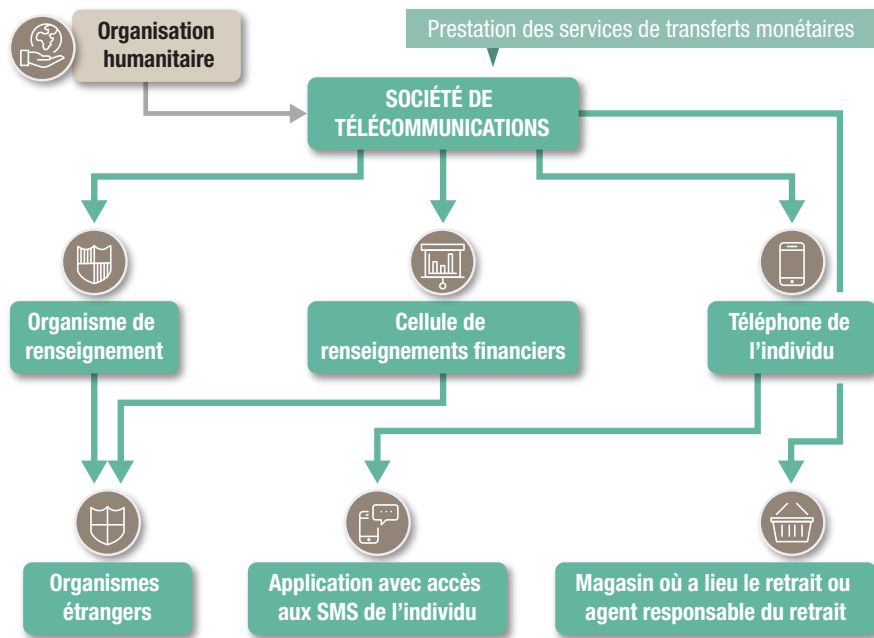
¹⁴⁷ *Ibid.*

¹⁴⁸ ODI et Center for Global Development, 2015, p. 8.

¹⁴⁹ *Ibid.*, p. 11.

¹⁵⁰ *Ibid.*, p. 11.

Comment les données financières mobiles peuvent-elles se retrouver dans les mains d'autres parties ?



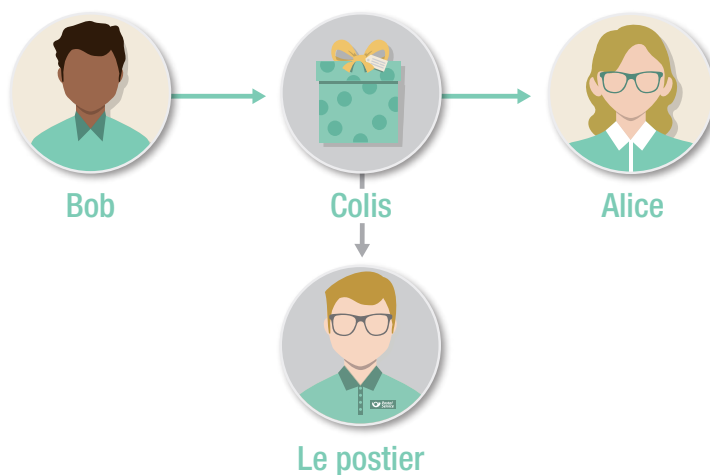
CICR et Privacy International, Section 6: Cash-transfer programmes (CTP), *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 73.

numériques dans le cadre des programmes de transferts monétaires nécessite souvent l'implication de tiers non humanitaires (par exemple, des fournisseurs de réseau de téléphonie mobile national et international, des établissements financiers et des cellules de renseignements financiers). Les organisations humanitaires perdent alors le contrôle des données recueillies et des métadonnées générées par le programme de transferts monétaires et ces données peuvent ensuite être utilisées à des fins non humanitaires (par exemple, dresser le profil de clients potentiels). Elles peuvent également être partagées avec des parties externes en vue de respecter une obligation légale ou en vertu d'accords de partenariat¹⁵¹.

Par ailleurs, une étude menée conjointement par le CICR et Privacy International précise qu'au-delà des données recueillies et traitées sciemment, chaque interaction génère ce que l'on appelle des métadonnées, c'est-à-dire des données sur les

¹⁵¹ CICR et Privacy International, Section 6: Cash-transfer programmes (CTP), dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018 : <https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era>.

Différents types de données et de métadonnées



Le postier peut avoir une idée de ce que contient le colis selon les éléments suivants :



CICR et Privacy International, Section 2: Processing data and metadata, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 33.

données. Ces métadonnées sont la conséquence inévitable de l'interaction avec le système ou service.

Enfin, il est important de souligner que tandis que l'utilisation croissante des technologies numériques et de la connectivité rend « visibles » des personnes auparavant « invisibles » auprès des établissements financiers, ces identités et empreintes numériques peuvent permettre d'inclure des personnes autrefois laissées pour compte dans certains programmes. Cette nouvelle visibilité peut toutefois exposer les bénéficiaires à des risques. Le simple fait qu'ils demandent de l'aide auprès d'une organisation humanitaire peut révéler leur appartenance à un groupe particulier et les exposer à des discriminations. Autrement dit, la visibilité

inévitables découlant de l'engagement numérique peut représenter une menace en situation humanitaire. La visibilité numérique et le profilage peuvent mener à une discrimination financière, ce qui serait contraire à l'objectif initial des programmes de transferts monétaires¹⁵².

9.2 APPLICATION DES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

Les menaces et les risques d'atteinte à la vie privée inhérents à la collecte et à la manipulation des données personnelles des bénéficiaires aux fins des programmes de transferts monétaires peuvent résulter de l'insuffisance des mesures organisationnelles et techniques de sécurité des données. Les organisations humanitaires doivent également tenir compte des répercussions à long terme des données générées, directement ou indirectement, par les programmes de transfert monétaires. Comme les programmes de transferts monétaires utilisent des services et systèmes existants, notamment ceux des banques et des opérateurs de télécommunications, les organisations humanitaires peuvent être tenues de collecter des données auprès des bénéficiaires pour respecter l'identification des clients¹⁵³, l'enregistrement de cartes SIM¹⁵⁴ et d'autres obligations auxquelles ces organismes sont soumis. Les données personnelles collectées aux fins de ces programmes peuvent impliquer divers ensembles de données qui n'auraient peut-être pas été nécessaires pour d'autres formes d'aide humanitaire¹⁵⁵. Ces données sont partagées avec des entités privées pour permettre la distribution de l'aide financière.

En outre, il convient de tenir compte non seulement des données collectées, mais également des données générées, c'est-à-dire des métadonnées découlant des modalités pratiques des programmes de transferts monétaires. La collecte, le partage et la conservation de ces données sont soumis à différentes obligations

¹⁵² CICR et Privacy International, Section 6.1: CTP and financial inclusion: benefits and challenges, dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 68–69.

¹⁵³ L'identification des clients (*Know Your Customer*, KYC) est une procédure permettant aux entreprises de contrôler l'identité de leurs clients afin de respecter la réglementation et la législation en matière de blanchiment d'argent et de corruption. Voir : PwC, *Anti-Money Laundering: Know Your Customer Quick Reference Guide and Global AML Resource Map*, PricewaterhouseCoopers, 2016 : <https://www.pwc.com/gx/en/industries/financial-services/publications/financial-crime-guide-tool-and-global-financial-crime-resource-m.html>.

¹⁵⁴ K. P. Donovan et A. K. Martin, « The rise of African SIM registration: The emerging dynamics of regulatory change », *First Monday*, vol. 19, n° 2 (26 janvier 2014), sec. IV : <http://firstmonday.org/ojs/index.php/fm/article/view/4351>.

¹⁵⁵ Cash Learning Partnership, *Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*, p. 4 : <http://reliefweb.int/sites/reliefweb.int/files/resources/calp-beneficiary-privacy-web.pdf>.

légales et réglementaires. Par exemple, dans le cas de l'argent mobile, ces données comprennent le numéro de téléphone de l'émetteur et du destinataire, la date et l'heure de la transaction financière, le code de transaction, le lieu et le montant de la transaction, le magasin où elle a été effectuée et tout agent impliqué de part et d'autre. Ces données peuvent être utilisées pour déduire d'autres informations et renseignements à des fins de profilage, de ciblage et de surveillance des utilisateurs¹⁵⁶. Par conséquent, les organisations humanitaires doivent connaître les moyens par lesquels les données peuvent être utilisées pour déduire des informations sur les comportements, les mouvements, les appartenances et d'autres caractéristiques des bénéficiaires. Il est possible de déduire des informations sur les bénéficiaires bien après la clôture du programme.

Les organisations humanitaires étant de plus en plus nombreuses à opter pour l'assistance sous forme d'aide directe en espèces, il est indispensable de considérer l'impact du traitement des données personnelles nécessaire pour distribuer cette forme d'aide (par exemple les individus qui reçoivent une aide financière feront-ils l'objet de discriminations?) et les mesures atténuant les risques associés¹⁵⁷.

Les questions de protection des données résultent de la collecte, de la conservation et du recoupement des données qui sont opérés par des responsables du traitement ou des sous-traitants lors des opérations des programmes d'aide en espèces. Les données collectées dans le cadre des programmes de transfert sont souvent relatives aux facteurs et vulnérabilités socioéconomiques. Elles sont utilisées pour cibler l'aide apportée, pour un sous-groupe de personnes touchées (pour la recherche en matière d'évaluation des besoins) ou pour un groupe plus vaste, éventuellement composé de personnes qui ne reçoivent, à terme, aucun transfert monétaire. Les données personnelles suivantes de tous les destinataires sont généralement recueillies dans ce processus : prénom, nom, numéro de téléphone mobile, données d'identification des clients¹⁵⁸, données de géolocalisation ou autres métadonnées téléphoniques et données biométriques. Les organisations humanitaires peuvent également collecter des données relatives aux facteurs ou vulnérabilités socioéconomiques afin de cibler l'assistance apportée. Une fois collectées et enregistrées, ces données peuvent permettre un traitement pour d'autres finalités ou d'autres types de traitement, comme l'analyse de données ou l'exploration de données¹⁵⁹.

¹⁵⁶ CICR et Privacy International, Section 6: Cash-transfer programmes (CTP), dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 73-75.

¹⁵⁷ *Ibid.*, p. 4.

¹⁵⁸ Voir Glossaire et PwC, *Know Your Customer: Quick Reference Guide* : <http://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html>.

¹⁵⁹ Voir [chapitre 6 : Analyse de données et big data](#).

La complexité des flux de données entre les organisations humanitaires et les organisations partenaires apportant de l'aide sous forme d'espèces et de bons soulève aussi des questions de protection des données, qui sont examinées ci-après à la section sur le partage des données¹⁶⁰.

9.3 PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

Les principes fondamentaux de la protection des données sont la référence à respecter dans tout traitement de données personnelles. Ce sont le principe de licéité et de loyauté du traitement, le principe de transparence, le principe de limitation de(s) la finalité(s), le principe de minimisation des données et le principe de qualité des données¹⁶¹.

L'analyse de la protection des données présentée dans ce chapitre s'appuie sur les principes énoncés dans la première partie, où ils sont examinés en plus amples détails.

9.3.1 FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

Les organisations humanitaires peuvent traiter des données personnelles sur la base des fondements juridiques suivants :

- l'intérêt vital de la personne concernée ou d'une autre personne ;
- l'intérêt public, en particulier basé sur le mandat confié à une organisation en vertu du droit national ou international ;
- le consentement ;
- l'intérêt légitime de l'organisation ;
- l'exécution d'un contrat ;
- le respect d'une obligation légale.

Il peut être difficile d'obtenir un consentement éclairé¹⁶² et valable des bénéficiaires des programmes d'aide sous forme d'espèces et de bons en raison de la quantité et de la complexité des informations qu'il faudrait leur donner pour être assuré qu'ils mesurent pleinement les risques et les avantages du traitement. De plus, la simple interaction avec le service génère inévitablement des métadonnées sans que l'utilisateur ait son mot à dire¹⁶³. Comme dans les autres cas où des données personnelles sont recueillies préalablement à l'assistance apportée aux bénéficiaires,

¹⁶⁰ Voir [section 9.5: Partage de données](#).

¹⁶¹ Voir aussi [chapitre 2: Principes fondamentaux de la protection des données](#).

¹⁶² Voir [section 3.2: Consentement](#).

¹⁶³ CICR et Privacy International, Section 6: Cash-transfer programmes (CTP), dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 21.



T. Jump/IRC

Dans la pointe nord du Cameroun, une femme consulte le téléphone dont elle se sert pour recevoir une aide directe en espèces non conditionnelle.

on peut faire valoir qu'à moins qu'une autre méthode d'assistance soit également possible, un individu qui a besoin d'assistance n'a pas vraiment le choix de donner ou de refuser son consentement et, en conséquence, que le consentement ne peut pas être considéré comme valable.

Si le consentement n'est pas possible, une autre base juridique peut être utilisée, comme indiqué ci-après. Les bénéficiaires doivent au minimum être informés individuellement ou collectivement de la nature du programme proposé, de la base juridique du traitement, du type de données collectées, par qui et pourquoi, de la nature de la transmission de données (obligatoire ou volontaire), des sources des données, de la durée de conservation des données, de l'identité des sous-traitants, ainsi que de l'identité de toute autre partie à laquelle seront partagées les données et leurs droits (y compris le droit de recours).

Les organisations humanitaires doivent¹⁶⁴ :

- Aspirer à obtenir le consentement actif et éclairé des bénéficiaires à l'utilisation de leurs données personnelles dans le cadre de l'aide apportée sous forme d'espèces et de bons.
- Ne renoncer au consentement valable et éclairé que lorsqu'il est impossible de l'obtenir ou qu'il est impossible d'obtenir un consentement valable pour d'autres raisons exposées ici. Il est légitime de ne pas solliciter un

¹⁶⁴ Cash Learning Partnership, *Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*, p. 13.

consentement actif et éclairé en cas d'urgence ou lorsqu'au regard des circonstances de la distribution, il n'est pas possible d'obtenir un « consentement actif et éclairé ».

- Si possible, veiller à ce qu'un consentement valable soit donné ou proposer une autre méthode d'assistance aux individus qui se méfient des flux de données ou des parties prenantes intervenant dans le cadre de l'aide apportée sous forme d'espèces et de bons.
- Selon les informations accessibles au public, informer en toute honnêteté les bénéficiaires au sujet des données et métadonnées susceptibles d'être générées, collectées et traitées par des tiers responsables des services et systèmes utilisés par les organisations humanitaires (y compris l'identification des clients pour les banques et l'enregistrement de cartes SIM par les opérateurs de télécommunications).

Étant donné l'efficacité potentielle des opérations sous forme d'espèces en situation de catastrophe et d'urgence et la rapidité de leur déploiement lorsqu'elles sont bien préparées (par exemple, par rapport à l'assistance en nature), les intérêts vitaux de la personne concernée ou d'une autre personne peuvent constituer une autre base juridique plausible du traitement lorsque les organisations humanitaires ne sont pas en mesure d'obtenir le consentement des individus. Cependant, comme toujours avec cette base juridique et comme il est précisé ailleurs dans ce manuel, il convient de réfléchir soigneusement à son utilisation.

L'intérêt public pourrait être une base juridique appropriée du traitement des données dans le cadre d'aides apportées sous forme d'espèces et de bons lorsqu'un mandat d'exécution d'une action humanitaire est établi en droit national, régional ou international et lorsque aucun consentement n'est obtenu et qu'aucun intérêt vital n'est en jeu, comme dans les situations analysées plus haut.

Les organisations humanitaires peuvent également traiter des données personnelles lorsqu'elles y ont un intérêt légitime, sous réserve que les droits et libertés fondamentaux de la personne concernée ne l'emportent pas sur cet intérêt. Cet intérêt légitime peut comprendre le souhait d'accroître l'efficacité de l'aide humanitaire apportée ou de prévenir les fraudes et la duplication de l'aide.

9.3.2 LIMITATION DE(S) LA FINALITÉ(S) ET TRAITEMENT ULTÉRIEUR

Au moment de la collecte des données, l'organisation humanitaire doit déterminer et énoncer les finalités spécifiques du traitement des données¹⁶⁵. Celles-ci doivent être explicites et légitimes et, dans le cadre des programmes de transferts monétaires, impliquer la fourniture d'une aide pour permettre aux populations touchées d'avoir accès aux biens et services dont elles ont besoin.

¹⁶⁵ Voir [section 9.3.1: Fondements juridiques du traitement des données personnelles](#).

Ces finalités doivent être précisées et communiquées aux individus au moment de la collecte.

Les données personnelles peuvent être traitées à d'autres fins que celles qui ont été initialement spécifiées au moment de la collecte lorsque le traitement ultérieur est compatible avec ces finalités et, en particulier, lorsqu'il est nécessaire à des fins historiques, statistiques ou scientifiques. Pour déterminer si le traitement ultérieur est compatible avec les finalités de la collecte initiale, les facteurs suivants doivent être pris en compte :

- les liens éventuels entre les finalités de la collecte initiale et celles du traitement ultérieur envisagé ;
- la situation dans laquelle les données personnelles ont été recueillies et, en particulier, la relation entre les personnes concernées et le responsable du traitement, ainsi que la relation avec le sous-traitant ;
- la nature des données personnelles ;
- les conséquences que le traitement ultérieur envisagé pourrait avoir pour les personnes concernées ;
- l'existence de garanties appropriées ;
- les attentes raisonnables des personnes concernées quant à l'utilisation future des données.

Lors de l'examen des facteurs ci-dessus, il convient d'être particulièrement attentif aux finalités humanitaires du traitement des données.

Il convient également de considérer les autres finalités qui peuvent être en jeu dans le traitement effectué par les sous-traitants commerciaux (établissements financiers et opérateurs de téléphonie mobile, par exemple) ou qui peuvent les intéresser – par exemple, recoupement de listes de bénéficiaires et de listes de personnes désignées, conservation de métadonnées à des fins répressives, profilage des bénéficiaires du point de vue de leur solvabilité, etc.¹⁶⁶ Si les sous-traitants commerciaux étaient obligés ou en mesure de traiter des données personnelles à d'autres fins que la finalité exclusivement humanitaire envisagée, les conséquences seraient les suivantes :

- La qualité de sous-traitants des entités en question pourrait être mise en cause et on pourrait se demander si elles ne sont pas en fait de nouveaux responsables du traitement, qui définissent les moyens et les finalités du traitement.
- Le traitement additionnel peut être incompatible avec la finalité initiale de la collecte et nécessiter une nouvelle base juridique. S'il est possible de trouver une nouvelle base juridique (comme le respect d'une obligation légale de signalement des personnes désignées), les organisations humanitaires doivent réfléchir attentivement à sa compatibilité avec le caractère neutre, impartial et indépendant de l'action humanitaire.

¹⁶⁶ CICR et Privacy International, Section 6: Cash-transfer programmes (CTP), dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018.

Les clauses du contrat de traitement doivent restreindre le plus possible le traitement ultérieur effectué par les sous-traitants.

Dans le cas des programmes de transferts monétaires, les organisations humanitaires doivent connaître les données et métadonnées traitées par les sous-traitants responsables des services et systèmes qu'elles utilisent. Ces données doivent être incluses dans l'AIPD afin d'identifier tout domaine devant être réglementé au moyen de clauses contractuelles.

EXEMPLE :

Un système déployé par une organisation humanitaire pour distribuer de l'aide sous forme d'espèces ou de bons – finalité à laquelle les individus ont consenti – ne peut pas être utilisé pour transmettre les données des participants aux donateurs de ladite organisation à des fins de référencement croisé.

De la même façon, aucune donnée collectée ne peut être utilisée par un établissement financier pour évaluer la solvabilité d'un bénéficiaire et son éligibilité à des services financiers, et ce, même après la fourniture d'une aide par une organisation humanitaire.

9.3.3 MINIMISATION DES DONNÉES

Les informations collectées pour des opérations d'aide directe en espèces doivent être proportionnées à ces finalités, c'est-à-dire qu'il ne faut collecter et traiter que la quantité de données personnelles nécessaire pour identifier les individus ; les informations « en surplus » qui ne sont pas utiles à l'identification ne doivent pas être collectées et, si elles le sont, elles doivent être supprimées.

Étant donné que de multiples données sont collectées dans le cadre d'aides apportées sous forme d'espèces et de bons, il est recommandé de les compartimenter pour satisfaire aux exigences de minimisation des données en autorisant l'accès sur la base du besoin de savoir. En outre, des dispositions contractuelles pourraient être prévues pour interdire tout traitement ultérieur par des entités commerciales.

L'évaluation de l'application du principe de minimisation des données doit également tenir compte des données générées par les sous-traitants dans le cadre du programme, comme les métadonnées de transactions de crédit et les métadonnées du réseau de téléphonie mobile.

En matière de programmes d'aide sous forme d'espèces et de bons, une option possible de l'organisation humanitaire pour limiter les risques pour les personnes concernées consiste, lorsqu'elle le peut, à transférer au prestataire de services commercial (par exemple la banque ou un opérateur de téléphonie mobile) un

identifiant unique (qui ne permet pas à celui-ci d'identifier le bénéficiaire final) accompagné de la somme en espèces à distribuer. Il est toutefois important de réfléchir aux limites de ces approches, car les programmes de ce type dépendent de systèmes rigides opérés par des établissements financiers, des opérateurs de télécommunications et d'autres organismes compétents. De la même façon, il est important de reconnaître les limites des techniques actuelles d'anonymisation et les conséquences en termes de réidentification, en particulier lorsque les données peuvent être corrélées à d'autres sources pour rendre la réidentification possible¹⁶⁷.

9.3.4 CONSERVATION DES DONNÉES

Il est conseillé aux organisations humanitaires de s'assurer que les données des bénéficiaires ne sont pas conservées (par elles-mêmes ou par des sous-traitants) plus longtemps que nécessaire pour atteindre les finalités spécifiques pour lesquelles elles ont été collectées, sauf si leur conservation peut être utile pour renouveler les distributions. Les données personnelles des bénéficiaires qui ont quitté le programme doivent être supprimées par l'organisation, ses sous-traitants et, le cas échéant, les tiers qui ont eu accès aux données. Dans la mesure du possible, l'organisation humanitaire doit vérifier que le prestataire commercial a bien supprimé les données. Une information dont la conservation est jugée nécessaire au terme d'un programme ne doit être conservée que si elle a trait à des données pour lesquelles il y a une finalité légitime, comme d'éventuels programmes futurs, des audits ou des rapports, le suivi et l'évaluation. Dans l'idéal, les données conservées pour ces motifs doivent être agrégées ou anonymisées.

Lorsqu'elles envisagent de conserver des données, les organisations humanitaires doivent également tenir compte des obligations de conservation que le droit interne met à la charge de sous-traitants comme les établissements financiers, les sociétés de cartes de crédit et les opérateurs de téléphonie mobile. Elles doivent être incluses dans les AIPD du programme et dans les politiques en matière de respect de la vie privée.

9.3.5 SÉCURITÉ DES DONNÉES

Pour éviter toute utilisation abusive des données personnelles collectées et traitées dans le cadre de programmes de transferts monétaires, il est indispensable de prendre des mesures de sécurité adéquates et proportionnées. Les organisations humanitaires ont intérêt à instaurer des règles de sécurité techniques et opérationnelles appropriées pour chaque stade de la collecte, de l'utilisation et du transfert des données des bénéficiaires, ainsi que des procédures et des mesures pour protéger les données personnelles des bénéficiaires contre la perte, le vol, les dommages ou la destruction, notamment des systèmes de sauvegarde et des

¹⁶⁷ L. Hardesty, « How hard is it to 'de-anonymize' cellphone data? », MIT News, 27 mars 2013 : <https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data>.

moyens efficaces pour répondre aux atteintes à la sécurité et prévenir les accès non autorisés, la divulgation ou la perte¹⁶⁸.

Il est également conseillé aux organisations humanitaires d'intégrer la protection des données personnelles qu'elles recueillent auprès de bénéficiaires, soit pour leur propre usage, soit pour celui de tiers, dans la conception de chaque programme d'aide sous forme d'espèces ou de bons qu'elles engagent ou mettent en œuvre. Elles doivent donc prévoir des protections de la vie privée dans les processus et mécanismes de mise en œuvre de ces aides. Pour cela, le chiffrement ou la compartimentation des informations peuvent être des solutions viables.

Les organisations humanitaires doivent veiller à se renseigner sur les mesures prises par les éventuels sous-traitants et tiers responsables des systèmes, services et infrastructures qu'elles utilisent, et ce, avant de signer tout accord. Des mesures de sécurité doivent protéger les données personnelles, au repos et en transit, et les infrastructures utilisées pour le traitement contre divers risques, tels que l'utilisation, la divulgation et l'accès illicites ou non autorisés, ainsi que la perte, la destruction ou la détérioration des données. Dans le cadre des vérifications approfondies et des AIDP, les organisations humanitaires doivent se renseigner sur les incidents de sécurité rendus publics dont ont été victimes les sous-traitants et tiers responsables des systèmes, services et infrastructures utilisés; elles doivent également se renseigner sur les mesures prises à la suite de ces incidents pour garantir la sécurité et l'intégrité des données, au repos et en transit, et de l'infrastructure utilisée.

La conservation des données et le transfert international potentiel de données doivent aussi être pris en considération. Pour des réfugiés par exemple, le recours à une banque régionale ayant une succursale ou une installation de stockage dans le pays d'origine des réfugiés peut présenter de graves risques pour la protection des données, car les données peuvent être demandées par les autorités nationales.

Les mesures de sécurité garanties par les sous-traitants doivent être un critère de sélection décisif.

9.4 DROITS DES PERSONNES CONCERNÉES

Le droit à l'information doit être respecté en veillant à informer individuellement ou collectivement les bénéficiaires de la nature du programme proposé, des informations qui sont recueillies, par qui et pourquoi, et de l'identité des sous-traitants. Les organisations humanitaires doivent être transparentes sur l'utilisation qu'elles comptent faire des données personnelles collectées et traitées. Elles doivent

¹⁶⁸ Voir [section 2.8: Sécurité des données et sécurité du traitement](#).

fournir des notices sur le respect de la vie privée qui expliquent l'ensemble des flux de données et la conservation des données envisagés aux bénéficiaires qui souhaitent des informations plus précises.

Une infrastructure et des ressources adéquates doivent être mises en place afin de faciliter l'exercice du droit d'accès, du droit d'opposition, du droit de suppression et du droit de rectification pour tous les programmes d'aide sous forme d'espèces et de bons. À cet égard, il est souhaitable d'intégrer des procédures de réclamation aux pratiques en matière de traitement des données personnelles et aux politiques internes de protection des données.

9.5 PARTAGE DE DONNÉES

Le traitement des données personnelles aux fins des programmes de transferts monétaires peut donner lieu à un partage des données avec des sous-traitants et des tiers lorsque les données ont été collectées et traitées par différents responsables du traitement ou sous-traitants (par exemple, si les organisations humanitaires qui mettent un programme en place externalisent l'identification des individus sur le terrain à des opérateurs sur site). Il est important de tenir compte des exigences de protection des données avant de procéder au partage des données et de noter que le « partage » recouvre non seulement les situations dans lesquelles les données sont activement transférées à des tiers, mais aussi celles dans lesquelles elles sont rendues accessibles (par exemple, partage d'une base de données contenant les données personnelles des bénéficiaires).

Les organisations humanitaires peuvent faire appel à des organisations partenaires pour collecter les données pour leur compte ou à des organisations commerciales (comme des établissements financiers ou des opérateurs de téléphonie mobile) intervenant dans l'exécution de ces programmes. Ces autres organisations peuvent être soumises à des exigences légales et organisationnelles qui les conduisent à partager des données avec des tiers (y compris des autorités de réglementation):

- Obligations d'identification des clients (KYC) imposant de collecter davantage de données personnelles que ce qui est strictement nécessaire pour apporter une assistance.
- Obligations de contrôle des informations d'identification par rapport à des listes de personnes désignées établies par les autorités locales, y compris des entités pouvant être impliquées dans un conflit ou une situation de violence. Ce processus peut faire l'objet d'un suivi par les autorités publiques et peut comporter des obligations de signalement. Cela pose la question de l'inclusion (les bénéficiaires peuvent-ils être exclus d'un programme d'assistance sur la base d'une correspondance trouvée?) et peut compromettre la neutralité et l'indépendance de l'action humanitaire.

- Collecte de données complémentaires dans le cadre du processus, comme des données géolocalisées ou des identifiants téléphoniques uniques et d'autres métadonnées de téléphonie mobile, lorsque des opérateurs de téléphonie mobile interviennent.
- Exigences en matière d'enregistrement de cartes SIM.
- Obligations de conservation incompatibles avec les informations données par les organisations humanitaires au moment de la collecte.
- Autres finalités commerciales comme le profilage des individus du point de vue de la solvabilité ou à des fins publicitaires.
- Autres obligations imposées par la législation nationale.

Les privilèges et immunités sont également très importants en ce qui concerne les programmes de transferts monétaires. À cet égard, les dispositions de la [section 10.9 \(Privilèges et immunités dans le cloud\)](#) doivent être prises en compte pour ces programmes.

9.6 TRANSFERT INTERNATIONAL DE DONNÉES

Le droit de la protection des données pose des restrictions aux transferts internationaux de données ; les organisations humanitaires doivent donc mettre en place des mécanismes leur conférant une base juridique dans le cadre des programmes de transferts monétaires, comme il est expliqué au [chapitre 4 : Transfert international de données](#). Avant d'entreprendre un transfert international de données, elles doivent déterminer si celui-ci possède un fondement juridique en vertu du droit applicable et de leurs politiques internes.

Les services financiers sont fortement interconnectés de sorte que les organisations humanitaires ne peuvent les contrôler. La manière dont les données circulent à l'échelle nationale et internationale dépend de cette interconnexion, ainsi que des lois, réglementations et pratiques nationales. C'est pourquoi les organisations humanitaires doivent discuter des points suivants avec tous les établissements impliqués dans les programmes de transferts monétaires : i) Qui sont leurs partenaires principaux, à l'échelle nationale et internationale ? et ii) Les données des programmes de transferts monétaires peuvent-elles être exclues de tout autre échange d'informations¹⁶⁹ ?

¹⁶⁹ CICR et Privacy International, Section 6: Cash-transfer programmes (CTP), dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 79.

9.7 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Les organisations humanitaires peuvent faire appel à des prestataires de services commerciaux locaux ou internationaux pour le déploiement de leurs programmes d'aide sous forme d'espèces et de bons. Elles peuvent également coopérer entre elles en partageant des bases de données contenant les informations recueillies dans le cadre de ces opérations. Il est donc indispensable de déterminer quelles sont les parties qui définissent effectivement les finalités et les moyens du traitement des données (et sont donc des responsables du traitement) et quelles sont celles qui prennent simplement leurs instructions auprès des responsables du traitement (et sont donc des sous-traitants). Il est possible également que plusieurs parties puissent être considérées comme des responsables du traitement conjoints. Une fois que les rôles ont été clairement définis et les tâches correspondantes attribuées, le partage des données par-delà les frontières, entre des organisations humanitaires ou avec des organismes tiers (publics ou privés) doit être couvert par des dispositions contractuelles appropriées.

Il faut garder à l'esprit que bien que les données personnelles puissent être protégées lorsqu'elles sont conservées dans les systèmes des organisations humanitaires auxquelles le droit international confère des privilèges et des immunités, ces mêmes données peuvent perdre cette protection lorsqu'elles sont transférées à des sous-traitants qui ne bénéficient pas de ces privilèges et immunités. En outre, la législation locale peut imposer aux sous-traitants de partager des données avec l'administration et même leur interdire d'en informer les organisations humanitaires dont émanent les données.

9.8 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

Les analyses d'impact relatives à la protection des données (AIPD) doivent être conçues et adaptées à chaque programme d'aide sous forme d'espèces et de bons. Différents programmes peuvent être conduits d'une organisation à l'autre, mais aussi au sein d'une même organisation. Chaque programme constitue une activité de protection des données distincte, qui doit faire l'objet d'une AIPD. Les AIPD aideront l'organisation humanitaire (a) à déterminer les risques d'atteinte à la vie privée des individus, en particulier ceux qui découlent du flux des données et des parties prenantes ; (b) à déterminer les obligations de conformité de l'organisation en matière de respect de la vie privée et de protection des données ; (c) à protéger la réputation de l'organisation et à donner au public confiance dans le programme et (d) à veiller à ce que l'organisation ne fasse aucun compromis sur la neutralité de son action humanitaire.

Il est recommandé aux organisations humanitaires d'analyser, de documenter et de comprendre le flux de données des bénéficiaires pour chaque programme d'aide qu'elles initient ou mettent en œuvre, soit en interne, soit avec des partenaires, d'identifier les risques encourus et d'élaborer des stratégies d'atténuation des risques. Les problématiques souvent associées aux prestataires de services commerciaux et relatives à la réglementation en matière d'identification des clients (KYC), à l'obligation de signalement aux autorités nationales, au transfert international de données et au stockage potentiel dans le cloud doivent être étudiées et évaluées par rapport aux avantages de l'aide sous forme d'espèces et de bons.

Le Cash Learning Partnership a établi un modèle d'AIPD pour les programmes de transferts monétaires¹⁷⁰.

170 Cash Learning Partnership, *Protecting Beneficiary Privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*, p. 18.



SERVICES CLOUD

UTILISATION POSSIBLE

PUISSANCE DE CALCUL ÉLEVÉE
SUR DE COURTES PÉRIODES

HÉBERGEMENT
DES DONNÉES
EN LIEU SÛR

SOUPLESSE
EN TERMES
D'ACCROISSEMENT
DES CAPACITÉS

FLEXIBILITÉ EN TERMES
DE LOCALISATION

DÉFIS

CONTRÔLE
LIMITÉ SUR
LES SERVICES
CLOUD

INTERCEPTION
D'INFORMATIONS
SENSIBLES

GARANTIE
QUE TOUTES
LES COPIES DE
SAUVEGARDE
SONT SUPPRIMÉES
SUR DEMANDE

ACCÈS POSSIBLE
PAR LES AUTORITÉS

ACCÈS
POSSIBLE
PAR LES
FOURNISSEURS
DE SOLUTIONS
CLOUD

RÉALISATION
D'AUDITS



CHAPITRE 10

SERVICES CLOUD

10.1 INTRODUCTION

La définition la plus courante du cloud computing est celle de l'Institut national américain des normes et de la technologie (National Institute of Standards and Technology, NIST)¹⁷¹, selon laquelle « le cloud computing est un modèle permettant d'accéder partout, aisément et à la demande, par le réseau, à des ressources informatiques configurables mutualisées (par exemple réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement mobilisées et libérées avec un minimum d'effort de gestion ou d'intervention d'un prestataire de services ». Le document du NIST définit trois modèles de service – le SaaS (*Software as a Service*), le PaaS (*Platform as a Service*) et le IaaS (*Infrastructure as a Service*) – et quatre modèles de déploiement – cloud public, privé, communautaire et hybride¹⁷² – même s'il faut garder à l'esprit que de nouveaux modèles apparaissent sans cesse.

Le cloud computing peut faciliter et accélérer la création et le traitement de grandes quantités de données et la production de nouveaux services et applications ; il peut aussi rendre le déploiement plus agile. L'aide humanitaire reposant sur l'information, ce nouveau modèle de traitement des données est devenu un outil utile pour les organisations humanitaires. Il offre plusieurs avantages : accès à une grande puissance de calcul sur de courtes périodes, élasticité et flexibilité en termes de localisation et de flux de données, et réduction des coûts¹⁷³.

Cependant, les services cloud peuvent aussi engendrer des risques et des défis en matière de protection des données et de la vie privée, qui peuvent s'analyser en deux catégories : l'absence de contrôle sur les données d'une part, et l'absence de transparence sur l'opération de traitement elle-même, d'autre part. Pour l'action humanitaire, les risques suivants sont particulièrement importants :

- utilisation des services depuis des sites non protégés ;
- interception d'informations sensibles ;
- failles du système d'authentification ;
- risque que les données soient volées au fournisseur de services cloud, par exemple par des pirates ;
- possibilité d'accès des autorités gouvernementales et des autorités chargées de l'application des lois.

¹⁷¹ US NIST SP 800-145, *The NIST Definition of Cloud Computing*, septembre 2011 : <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

¹⁷² Avis du contrôleur européen de la protection des données relatif à la communication de la Commission intitulée « Exploiter le potentiel de l'informatique en nuage en Europe », 16 novembre 2012, p. 4 : https://edps.europa.eu/sites/edp/files/publication/12-11-16_cloud_computing_fr.pdf.

¹⁷³ D. Schniederjans et K. Özpolat, *An Empirical Examination of Cloud Computing in Humanitarian Logistics*, document de travail : <http://www.cba.uri.edu/research/brownbag/spring2013/documents/DaraS2013329paper.pdf>.

Les implications du cloud computing au regard de la protection des données ont été mises en exergue par la Conférence internationale des commissaires à la protection des données et à la vie privée dans sa résolution sur le sujet, adoptée en 2012 en Uruguay¹⁷⁴.

En outre, les organisations humanitaires auxquelles le droit international confère des privilèges et des immunités doivent savoir que l'externalisation du traitement des données personnelles à un tiers fournisseur de services cloud peut exposer leurs données à un risque de perte de la protection offerte par ces privilèges et immunités. La [section 10.9 \(Privilèges et immunités dans le cloud\)](#) donne de plus amples informations sur les privilèges et immunités dans un environnement cloud.

Les trois modèles de services cloud peuvent être décrits comme suit¹⁷⁵ :

- IaaS (*Infrastructure as a Service*) : un cloud IaaS permet d'accéder aux ressources informatiques brutes d'un service cloud. Au lieu d'acheter le matériel, le client achète l'accès au matériel du fournisseur du service en fonction des capacités dont il a besoin.
- PaaS (*Platform as a Service*) : un cloud PaaS donne accès à une plateforme informatique qui permet aux clients de créer des applications utilisables sur cette plateforme ou sur une autre plateforme similaire. La plateforme peut à son tour être hébergée sur un cloud IaaS.
- SaaS (*Software as a Service*) : un cloud SaaS donne accès à une application complète à laquelle l'utilisateur des services cloud peut accéder via un navigateur ou un autre logiciel. Ce mode d'accès supprime ou réduit la nécessité d'installer le logiciel sur la machine cliente et permet au service de fonctionner sur une plus large gamme d'appareils. Le logiciel peut à son tour être hébergé sur une plateforme ou une infrastructure cloud.

On distingue également différents types d'infrastructure cloud. Un cloud privé est exploité pour une seule organisation ; il peut être géré en interne ou par un tiers et hébergé ou non en interne. Dans un cloud public, les services sont fournis à travers un réseau ouvert au public. Enfin, un cloud hybride est une composition de deux ou plusieurs clouds qui restent des entités distinctes mais sont liés entre eux, ce qui offre les avantages de modèles de déploiement multiples.

Chacun de ces modèles présente des avantages et des inconvénients. Un cloud public est plus accessible, car l'information est stockée hors site et donc disponible en tout lieu via Internet ; il permet d'augmenter rapidement les capacités du serveur et peut permettre de réduire les coûts ; il peut aussi faire régulièrement l'objet de mises à jour et d'améliorations de la sécurité et des performances. Cela étant, comme

¹⁷⁴ http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Cloud-Computing.pdf?mc_phishing_protection_id=28047-br1tehqdu81eaoar3q10.

¹⁷⁵ Information Commissioner's Office, *Guidance on the use of cloud computing*, 2012, p. 5-6 : <https://ico.org.uk/for-the-public/online/cloud-computing/>.

un cloud public nécessite une connexion Internet, il existe un risque de perte de contrôle sur les données en cas de transferts de données non annoncés ou non autorisés d'un système juridique à un autre, d'une fausse suppression des données, de conservation des données après la fin des services, de piratage et d'attaques. Il est difficile de savoir où les données sont conservées dans un cloud public à un moment donné et la suppression n'est presque jamais possible en raison des nombreuses copies de sauvegarde réalisées sans contrôle. À cela s'ajoutent de nombreuses préoccupations relatives à la protection de la vie privée et à la confidentialité, comme le fait que le traitement peut être soumis à des législations différentes qui pourraient imposer un accès non autorisé aux données et la possibilité pour les autorités d'exercer leur juridiction.

Dans un cloud privé/interne, les données sont conservées dans le réseau interne de l'organisation et ne sont donc pas publiquement accessibles. Ce type de cloud offre un environnement plus contrôlé ; il compte un nombre limité d'utilisateurs et engendre ainsi moins de risques de divulgation par des tiers. Un cloud privé peut offrir la même facilité d'utilisation, la même capacité d'évolution et la même flexibilité qu'un cloud public. Ses inconvénients résident dans le coût et le fait qu'il n'offre pas toujours les dernières mises à jour et améliorations en termes de performance et de sécurité.

Avec un cloud hybride, les organisations peuvent déterminer à quelle option recourir en fonction de la classification des informations à stocker. En général, les informations moins sensibles sont envoyées sur un cloud public, tandis que les informations plus sensibles et confidentielles sont conservées sur un cloud privé ou interne. Bien que ce modèle permette de réduire les coûts et offre modularité, sécurité et possibilité de mises à jour/améliorations de la performance, il présente les mêmes risques de perte de contrôle sur les données et de divulgation non autorisée qu'un cloud public.

10.2 RESPONSABILITÉ DANS LE CLOUD

La relation entre le client et le fournisseur de services cloud est du même type que celle qui existe entre le responsable du traitement et le sous-traitant¹⁷⁶. Cependant, il arrive exceptionnellement que le fournisseur de services cloud agisse également comme un responsable du traitement, auquel cas il assume toute la responsabilité (conjointe) du traitement des données et doit respecter toutes les obligations légales de protection des données. Il appartient au client du cloud (c'est-à-dire à l'organisation humanitaire), en tant que responsable du traitement, de s'acquitter des obligations légales qui découlent du droit de la protection des données. En outre, le client du cloud doit sélectionner un fournisseur qui respecte la législation en matière de protection des données.

¹⁷⁶ Voir [section 10.7 : Relation entre le responsable du traitement et le sous-traitant](#).

La notion de responsabilité exprime les obligations de conformité directes que le droit de la protection des données met à la charge des responsables du traitement et des sous-traitants, c'est-à-dire qu'ils doivent pouvoir garantir et démontrer que leurs activités de traitement respectent les obligations légales applicables en adoptant et en appliquant des politiques de protection des données et des notices appropriées.

EXEMPLE :

Lorsqu'une organisation humanitaire passe contrat avec un fournisseur de services cloud en vue de stocker des données personnelles dans le cloud, elle demeure responsable vis-à-vis des personnes concernées de toute atteinte à la protection des données commise par le fournisseur. Il est donc essentiel qu'elle prenne les mesures suivantes avant de stocker des données personnelles dans un cloud :

- réaliser une AIPD portant sur le stockage de données personnelles dans le cloud envisagé et être prête à annuler le projet si les résultats font apparaître des risques indus pour la protection des données des individus ;
- effectuer des vérifications auprès du fournisseur de services cloud afin de s'assurer qu'il prendra les précautions nécessaires et qu'il prend la protection des données au sérieux ;
- discuter ouvertement de la protection des données avec le fournisseur et déterminer s'il semble prêt et apte à honorer ses obligations en matière de protection des données ;
- examiner attentivement le contrat avec le fournisseur avant la signature et s'assurer qu'il prévoit des obligations appropriées en matière de protection des données ;
- pour les organisations humanitaires bénéficiant de privilèges et d'immunités, veiller à ce que ceux-ci soient intégrés comme il se doit à la conception de la solution cloud et respectés.

10.3 APPLICATION DES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

Tous les principes de la protection des données s'appliquent aux services cloud ; il convient ici d'être très attentif à plusieurs aspects qui revêtent une importance toute particulière.

L'analyse de la protection des données présentée dans ce chapitre s'appuie sur les principes énoncés dans la première partie, où ils sont examinés en plus amples détails.

10.3.1 FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

Avant de faire appel à un fournisseur de services cloud, les organisations humanitaires doivent démontrer qu'un des fondements juridiques suivants est présent¹⁷⁷ :

- l'intérêt vital de la personne concernée ou d'une autre personne ;
- l'intérêt public, en particulier basé sur le mandat confié à une organisation en vertu du droit national ou international ;
- le consentement ;
- l'intérêt légitime de l'organisation ;
- l'exécution d'un contrat ;
- le respect d'une obligation légale.

Il est important à cet égard de distinguer le traitement initial des données personnelles effectué par l'organisation humanitaire de leur traitement dans le cloud. L'organisation humanitaire doit s'appuyer sur une base juridique pour pouvoir collecter et traiter les données personnelles, qui peut être l'un des fondements juridiques indiqués au [chapitre 3 : Fondements juridiques du traitement des données personnelles](#). Le traitement dans le cloud doit quant à lui reposer sur une base juridique distincte. Dans chaque situation ou opération humanitaire, il faut évaluer chaque base juridique au cas par cas et déterminer si elle peut être étendue au cloud, soit à titre de base juridique «supplémentaire», soit cumulativement.



Même lorsque l'intérêt vital des individus constitue une base juridique suffisante pour collecter des données personnelles, le placement des données dans le cloud doit lui aussi avoir une base juridique.

¹⁷⁷ Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

EXEMPLE :

Une organisation humanitaire collecte des données personnelles auprès d'individus vulnérables sur la base de leur intérêt vital. Pour accroître l'efficacité de ses services humanitaires, elle souhaite ensuite stocker les données dans un cloud privé et fait appel à cette fin à un fournisseur de services cloud. L'intérêt vital des individus constitue une base juridique suffisante pour collecter les données personnelles, mais le placement des données dans le cloud doit également avoir une base juridique. L'intérêt vital n'est pas forcément une base juridique suffisante pour placer les données dans le cloud puisque ce n'est pas indispensable pour fournir les services humanitaires ; l'objectif est en fait d'accroître l'efficacité de ces services. Une base juridique pouvant justifier le recours à un fournisseur de services cloud pourrait être que cela sert l'intérêt légitime de l'organisation humanitaire et que les droits fondamentaux des personnes dont les données sont traitées ne l'emportent pas sur cet intérêt. Le fait qu'un cloud privé est utilisé conforte cet argument. Une AIPD doit être réalisée pour confirmer la base juridique.

10.3.2 TRAITEMENT ÉQUITABLE ET LICITE

Le traitement des données personnelles doit être licite et équitable. Pour être licite, le traitement doit avoir une base juridique appropriée¹⁷⁸, tandis que l'exigence d'équité est un principe général ordinairement lié à la fourniture d'informations et à l'utilisation des données. Les organisations humanitaires qui utilisent des services cloud doivent garder à l'esprit que ces principes s'appliquent à tous les stades du traitement (collecte, traitement et stockage).

10.3.3 LIMITATION DE(S) LA FINALITÉ(S) ET TRAITEMENT ULTÉRIEUR

Les organisations humanitaires doivent déterminer et exposer les finalités spécifiques du traitement des données personnelles. Ces finalités doivent être précisées et communiquées aux individus au moment de la collecte.

Les finalités humanitaires offrent une large base sur laquelle justifier des opérations de traitement ultérieur. Toutefois, il n'y aura pas de compatibilité si les risques pour les individus concernés l'emportent sur les avantages du traitement ultérieur. Cela dépend de la situation. À titre d'exemple, on conclura à l'incompatibilité lorsque le traitement risque d'être contraire aux intérêts importants de la personne à laquelle les informations ont trait ou de sa famille, notamment lorsqu'il risque de porter atteinte à leur vie, à leur intégrité, à leur dignité, à leur sécurité psychologique ou physique, à leur liberté ou à leur réputation.

178 Voir [section 10.3.1: Fondements juridiques du traitement des données personnelles](#).

Dans les environnements cloud, c'est au client du cloud qu'il revient de déterminer les finalités du traitement avant de collecter les données personnelles auprès de la personne concernée et d'en informer celle-ci. Étant donné qu'il est interdit à un client de services cloud de traiter des données personnelles à d'autres fins que celles prévues initialement, le fournisseur de services cloud ne peut pas unilatéralement décider ou organiser un transfert automatique de données personnelles (et leur traitement) à des centres de données cloud inconnus. Il ne peut pas non plus utiliser les données personnelles pour ses propres finalités (par exemple le marketing, des recherches à d'autres fins ou le profilage).

En outre, tout traitement ultérieur incompatible avec les finalités initiales est également interdit au fournisseur de services cloud et à ses sous-traitants. Or une situation type de services cloud peut aisément impliquer de nombreux sous-traitants. Afin d'atténuer le risque de traitement ultérieur, le contrat entre le fournisseur des services et le client doit prévoir des mesures techniques et organisationnelles et donner des assurances quant à l'enregistrement et à l'audit des opérations de traitement des données personnelles effectuées par les employés du fournisseur ou par ses sous-traitants.

10.3.4 TRANSPARENCE

La transparence est un aspect du traitement équitable et légitime des données personnelles ; elle est aussi étroitement liée à l'information des personnes concernées. Le client du cloud est tenu de fournir des informations précises aux personnes concernées dont les données personnelles ou des données qui les concernent sont collectées – identité et adresse du client du cloud, finalités du traitement, destinataires ou catégories de destinataires des données, y compris les sous-traitants dans la mesure où ces informations sont nécessaires pour garantir l'équité du traitement, et informations sur leurs droits.

La transparence doit être également garantie dans les relations entre le client, le fournisseur de services cloud et les sous-traitants éventuels. Le client ne peut évaluer la licéité du traitement des données personnelles dans le cloud que si le fournisseur l'informe de tous les aspects pertinents. Un responsable du traitement qui envisage de faire appel à un fournisseur de services cloud doit soigneusement analyser les conditions générales du fournisseur et les apprécier du point de vue de la protection des données.

Un autre aspect de la transparence dans le domaine du cloud computing est que le client doit être informé de tous les sous-traitants intervenant dans la fourniture des services cloud, et pas seulement de ceux avec lesquels il a une relation contractuelle directe, ainsi que du lieu d'implantation de tous les centres de données où des données personnelles peuvent être traitées.

10.3.5 CONSERVATION DES DONNÉES

Il est conseillé aux organisations humanitaires de veiller à ce que les données personnelles ne soient pas conservées (par elles-mêmes ou par des sous-traitants) plus longtemps que nécessaire sauf si elles ont des motifs clairs, justifiables et documentés de le faire ; dans le cas contraire, les données détenues par l'organisation et les tiers doivent être détruites. Il est recommandé de supprimer ou de détruire les données après le traitement ou d'établir une politique de conservation des données soigneusement structurée. Lorsque les finalités de la collecte sont atteintes, les données personnelles doivent être supprimées par l'organisation et par tous les tiers qui ont eu accès aux données, à moins que ces derniers aient obtenu le consentement à la conservation des données.

Les données ne doivent être conservées dans le cadre de services cloud que si elles ont trait à une finalité de traitement légitime. Les finalités légitimes à cet égard peuvent être de futurs programmes, le suivi et l'évaluation, tandis que des données anonymisées ou agrégées pourraient être appropriées à des fins de recherche. Conformément au principe de minimisation des données, il ne faut conserver que la quantité minimale de données.

Il appartient au client du cloud de s'assurer que les données personnelles sont effacées dès qu'elles ne sont plus nécessaires. La suppression des données est un aspect crucial pendant la durée d'un contrat de services de cloud computing, mais aussi à sa résiliation. Elle est aussi pertinente en cas de remplacement ou de retrait d'un sous-traitant. Dans ce cas, le client du cloud pourrait demander un certificat de destruction au fournisseur ou un certificat confirmant que les données ont été transférées à un nouveau fournisseur.

Le principe de l'effacement des données s'applique aux données personnelles indépendamment du support de stockage (disques durs ou bandes de sauvegarde, par exemple). Les données personnelles pouvant être conservées simultanément sur plusieurs serveurs répartis sur différents sites, il faut s'assurer que chaque instance est définitivement effacée (les versions antérieures, les fichiers temporaires et même les fragments de fichiers doivent être également supprimés).

L'effacement sécurisé des données personnelles exige que le support de stockage soit détruit ou démagnétisé ou que les données personnelles stockées soient parfaitement effacées. Il convient d'utiliser des logiciels spéciaux qui écrasent les données personnelles à de multiples reprises, conformément à une spécification reconnue. Le client du cloud doit s'assurer que le fournisseur des services veille à l'effacement sécurisé et que le contrat conclu avec celui-ci contient des dispositions claires relatives à l'effacement des données personnelles. Il en va de même des contrats entre les fournisseurs de services cloud et les sous-traitants.

10.4 SÉCURITÉ DES DONNÉES

La sécurité des données peut être assurée par des mesures juridiques, techniques et organisationnelles. Les mesures juridiques peuvent être des dispositions contractuelles, mais aussi des AIPD. Une vision globale doit être adoptée, qui tient compte des phases suivantes d'un contrat de fourniture de services cloud :

- décision d'utiliser ou non des services cloud (AIPD et décision favorable/défavorable de la direction) ;
- procédure d'achat de services cloud, comprenant les vérifications juridiques et techniques effectuées sur les fournisseurs de services cloud potentiels ;
- passation du contrat (prévoir les bonnes dispositions) ;
- exploitation, maintenance et désactivation du service.

Il est recommandé d'élaborer une stratégie complète de protection des données et d'être attentif aux questions de protection des données à toutes les phases du contrat, avant, pendant et après sa conclusion. Elle doit comprendre une évaluation globale du cadre contractuel, notamment le SLA (*Service Level Agreement*) qui définit le niveau de qualité du service et son taux de disponibilité, les clauses générales (telles que le droit applicable, la juridiction compétente ou les avenants au contrat) et le principe général de « parallélisme dans et hors du cloud » (par exemple en termes de durée de conservation des données).

Lorsqu'une organisation humanitaire décide de passer contrat pour des services de cloud computing, elle doit choisir un fournisseur de services capable de donner des garanties suffisantes quant à la sécurité technique et aux mesures organisationnelles gouvernant le traitement envisagé, et veiller à ce que ces mesures soient respectées. En outre, un contrat doit être signé avec le fournisseur, car il faut un acte juridique qui lie le responsable du traitement et le sous-traitant et régit leur relation. Ce contrat doit au minimum établir que le sous-traitant doit suivre les instructions du responsable du traitement et prendre des mesures techniques et organisationnelles assurant une protection adéquate des données personnelles, conformément à la législation applicable en matière de protection des données.

Afin de garantir la sécurité juridique, le contrat entre l'organisation humanitaire et le sous-traitant doit aussi contenir les clauses essentielles de protection des données ci-après :

- Informations sur le lieu d'implantation des centres de données, sur l'identité et la localisation des sous-traitants et sur toute modification ultérieure apportée à la nature du traitement. Ces informations doivent préciser l'objet et la durée des services cloud qui seront fournis par le fournisseur, l'ampleur, les modalités et la finalité du traitement des données effectué par le fournisseur et le type de données personnelles traitées.

- Détails sur les instructions du client du cloud à donner au fournisseur, notamment en ce qui concerne le niveau de service et les pénalités applicables (pénalités financières ou possibilité de poursuivre le fournisseur s'il manque à ses obligations).
- Obligation pour le fournisseur de services d'informer le client en cas de violation des données du client. Notons qu'un incident de sécurité ne constitue pas nécessairement une violation des données.
- Reconnaissance de l'obligation de traiter les données personnelles exclusivement pour les finalités expressément mentionnées et spécifiées et d'effacer les données à la fin du contrat. Les conditions de restitution ou de destruction des données une fois le service rendu, doivent être précisées. En outre, il faut garantir qu'un effacement sécurisé des données sera opéré à la demande du client du cloud.
- Confirmation, dans le cas d'un cloud privé situé hors des locaux du client des services, que les données de l'organisation humanitaire sont conservées sur des serveurs à part.
- Spécification des mesures de sécurité à prendre par le fournisseur de services en fonction des risques découlant du traitement et de la nature des données à protéger.
- Clause de confidentialité liant le fournisseur de services et tous ses employés susceptibles d'accéder aux données. Seules les personnes autorisées peuvent avoir accès aux données.
- Obligation pour le fournisseur de services d'aider le client à faciliter l'exercice du droit d'accès, du droit de rectification et du droit de suppression des données des personnes concernées.
- Le cas échéant, obligation pour le fournisseur de services de respecter les privilèges et immunités du client des services cloud.
- Clause selon laquelle les sous-traitants ultérieurs ne peuvent être sollicités que sur la base du consentement du responsable du traitement (client des services cloud), conformément à une obligation claire du sous-traitant d'informer le responsable du traitement de toute modification projetée à cet égard, le responsable du traitement conservant à tout moment la possibilité de s'opposer à ces modifications ou de résilier le contrat. Le fournisseur de services doit avoir l'obligation de communiquer l'identité des sous-traitants auxquels il fait appel. Il doit être établi que les contrats entre le fournisseur de services et ses sous-traitants reflètent les stipulations du contrat conclu entre le client des services et le fournisseur (les sous-traitants ultérieurs ont les mêmes obligations contractuelles que le fournisseur de services). Il doit être en particulier garanti que le fournisseur de services et ses sous-traitants n'agissent que sur instruction du client. La chaîne de responsabilité doit être clairement indiquée dans le contrat.
- Dispositions selon lesquelles le client des services doit réaliser des audits pendant le contrat et à la fin de celui-ci. Le contrat doit prévoir l'enregistrement et l'audit des opérations de traitement sur les données personnelles effectuées par le fournisseur de services ou les sous-traitants.

- Obligation générale pour le fournisseur de services de donner l'assurance que son organisation interne et ses dispositions en matière de traitement des données (et, le cas échéant, celles de ses sous-traitants ultérieurs) respectent les exigences et les normes légales nationales et internationales applicables.

En ce qui concerne les aspects techniques de la sécurité des données, les organisations humanitaires doivent garder à l'esprit les considérations importantes ci-après¹⁷⁹ :

- **Disponibilité** : « Assurer la disponibilité » signifie garantir un accès fiable et en temps opportun aux données personnelles. La disponibilité dans le cloud peut être menacée par une perte accidentelle de la connexion réseau entre le client et le fournisseur ou par une perte de performances du serveur suite à des actes malveillants tels que les attaques par déni de service (distribué). Les autres risques pour la disponibilité sont les défaillances matérielles accidentelles survenant sur le réseau et dans les systèmes de traitement et de stockage des données dans le cloud, les pannes d'électricité ou d'autres problèmes d'infrastructure. Les responsables du traitement doivent donc vérifier que le fournisseur de services cloud a pris des mesures raisonnables pour gérer les risques d'ingérence telles que des liaisons de sauvegarde par réseau Internet, un stockage redondant et des mécanismes efficaces de sauvegarde des données.
- **Intégrité** : L'intégrité a trait au maintien de la qualité des données, qui ne doivent subir aucune altération malveillante ou accidentelle au cours du traitement, du stockage ou de la transmission. Pour les systèmes informatiques, l'intégrité requiert que les données personnelles traitées sur ces systèmes ne soient pas modifiées. Les modifications peuvent être détectées par des mécanismes d'authentification cryptographique comme les codes d'authentification des messages, les signatures ou les fonctions de hachage cryptographique. Toute atteinte à l'intégrité des systèmes informatiques dans le cloud peut être empêchée ou détectée par des systèmes de détection et de prévention des intrusions. Ces outils de sécurité sont particulièrement importants en environnement réseau ouvert comme celui des clouds.
- **Confidentialité** : Dans un environnement cloud, le chiffrement peut sensiblement contribuer à la confidentialité des données personnelles s'il est appliqué correctement, même s'il ne rend pas les données personnelles irréversiblement anonymes. Grâce à cet outil, le client des services cloud peut s'assurer que les données personnelles dont il est responsable ne sont accessibles qu'aux personnes autorisées possédant la clé appropriée. Le chiffrement des données personnelles doit être utilisé pour toutes les données « en transit » et, lorsque c'est possible, pour les données au repos. Cette règle s'applique en particulier aux responsables du traitement qui prévoient de transférer des données sensibles. Les communications entre le fournisseur de services cloud et le client, et entre les centres de données, doivent aussi être

¹⁷⁹ D'après Groupe de travail « Article 29 », *Avis 05/2012 sur l'informatique en nuage*, 1^{er} juillet 2012, p. 14-17 : https://cnpd.public.lu/content/dam/cnpgd/fr/publications/groupe-art29/wp196_fr.pdf.

chiffrées. Lorsque le chiffrement est la mesure technique choisie pour sécuriser les données, il importe également de garantir la sécurité de la clé. Les autres mesures techniques visant à garantir la confidentialité sont les mécanismes d'autorisation et une authentification forte (par exemple authentification à deux facteurs). Les clauses contractuelles doivent également imposer des obligations de confidentialité aux employés des clients des services cloud, aux fournisseurs de services et aux sous-traitants.

- **Isolement (limitation des finalités)** : L'isolement est une expression du principe de limitation de(s) la finalité(s). Dans les infrastructures cloud, les ressources comme le stockage, la mémoire et les réseaux sont partagées entre de multiples utilisateurs, ce qui engendre de nouveaux risques de divulgation des données et de traitement ultérieur illégitime. L'isolement vise à résoudre ce problème en garantissant que les données ne sont pas utilisées au-delà de leur finalité initiale et en préservant la confidentialité et l'intégrité. Il est assuré par une gouvernance adéquate des droits d'accès aux données personnelles et doit être contrôlé régulièrement. Il convient d'éviter les privilèges excessifs (aucun utilisateur ou administrateur ne doit avoir accès à la totalité du cloud par exemple). Plus généralement, les administrateurs et les utilisateurs ne doivent avoir accès qu'aux informations nécessaires à des finalités légitimes (principe du moindre privilège).
- **Possibilité d'intervention** : Les personnes concernées ont un droit d'accès, un droit de rectification, un droit de suppression, un droit de blocage et un droit d'opposition, qui sont examinés plus loin¹⁸⁰.
- **Portabilité** : Il est très important que les fournisseurs de services cloud utilisent des formats de données et des interfaces de services standards car cela facilite l'interopérabilité et la portabilité entre fournisseurs. Par conséquent, si un client de services cloud décide de changer de fournisseur, l'absence d'interopérabilité peut compliquer, voire empêcher le transfert des données (personnelles) du client au nouveau fournisseur, le client se trouvant alors captif de son fournisseur. Avant de commander un service cloud, le client doit vérifier si le fournisseur garantit la portabilité des données et des services et par quels moyens. La portabilité des données renvoie aussi à la capacité d'une personne concernée à obtenir une copie des données traitées auprès du responsable du traitement dans un format électronique structuré et courant. Pour que ce droit puisse être exercé, il est important qu'il ne subsiste aucune trace des données dans le système d'origine après leur transfert. Techniquement, il doit être possible de vérifier qu'un effacement sécurisé des données a été effectué.

Les autres principes de sécurité informatique que les organisations humanitaires doivent considérer lorsqu'elles passent au cloud sont exposés ci-après¹⁸¹.

¹⁸⁰ Voir [section 10.5 : Droits des personnes concernées](#).

¹⁸¹ Les auteurs remercient ICT Legal Consulting, qui leur a donné l'autorisation d'utiliser les documents sur la sécurité dans le cloud. D'après UK National Cyber Security Centre, *Cloud Security Guidance: Implementing the Cloud Security Principles*, 17 novembre 2018 : <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles>.

10.4.1 PROTECTION DES DONNÉES EN TRANSIT

Les transmissions de données doivent être correctement protégées contre l'interception (« eavesdropping ») et l'altération. Cette règle vaut non seulement pour les connexions entre les sites de l'organisation et l'application cloud, mais aussi pour les chemins de données internes au service et pour les connexions entre l'application et les autres services (interface de programmation applicative, API)¹⁸². Une solution courante consiste à chiffrer le trafic réseau en recourant à un VPN¹⁸³, au protocole TLS (*Transport Layer Security*) ou au chiffrement au niveau de l'application. Il faut veiller à choisir les bons protocoles, à mettre correctement en œuvre le chiffrement et à bien gérer les clés secrètes pour le chiffrement lui-même. Des connexions en fibre optique dédiées peuvent être également employées lorsque les circonstances le permettent.

10.4.2 PROTECTION DES ACTIFS

On ne recourt pas aux mêmes mesures pour protéger les actifs dans un environnement cloud et pour protéger les actifs sur site. Il faut donc considérer plusieurs aspects lorsqu'on évalue une solution cloud.

10.4.2.1 Localisation physique

Il est important de connaître la localisation physique des données stockées pour comprendre quelle législation s'applique, mais aussi les risques de menaces spécifiques comme les coupures de courant et de réseau, les actions commises par des groupes ou organisations hostiles et d'autres menaces propres à chaque pays. Il faut donc obtenir un état détaillé de l'emplacement physique des centres de données et savoir que des données peuvent être échangées entre des centres de données situés en différents lieux à l'insu de l'organisation.

Pour les organisations humanitaires bénéficiant de privilèges et d'immunités, il est également essentiel que le pays d'implantation des centres de données ait l'obligation légale de respecter les privilèges et immunités et qu'il soit connu pour effectivement les respecter.

10.4.2.2 Sécurité des centres de données

Dans le domaine des services cloud, la sécurité physique des centres de données est entièrement contrôlée par le prestataire de services ; c'est pourquoi il est important de bien apprécier la sécurité des sites d'hébergement. Pour cela, on peut vérifier les certifications éventuellement obtenues par le centre de données ou les obligations

¹⁸² API – une interface de programmation applicative est un ensemble normalisé de classes, de méthodes ou de fonctions qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels : https://fr.wikipedia.org/wiki/Interface_de_programmation.

¹⁸³ VPN – un réseau privé virtuel est un système permettant de créer un lien direct entre des ordinateurs distants. Il permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local : https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel.

contractuelles sous-jacentes de la relation entre le fournisseur de services cloud et l'organisation. Le niveau de sécurité garanti doit correspondre au niveau de sécurité requis par l'application à héberger dans le cloud. Une inspection physique pourrait donner d'utiles informations, mais elle est rarement possible dans les environnements cloud.

10.4.2.3 Sécurité des données stockées (données au repos)

Le niveau de sécurité des données stockées dépend du type de service requis et des autres dispositions convenues avec le fournisseur. Néanmoins, on peut raisonnablement supposer que les données seront conservées sur des supports de stockage partagés; le fournisseur de services doit donc clairement préciser le niveau de protection et comment il l'atteint et indiquer les certifications éventuelles par des tiers. Il est toutefois recommandé de ne pas se fier seulement à la sécurité du fournisseur de services pour les données entreposées, au moins pour les plus sensibles, mais d'ajouter d'autres niveaux de protection, comme le chiffrement.

10.4.2.4 Purge des données

Les environnements cloud se caractérisent par de fréquentes opérations de mise à disposition, d'effacement et de migration des ressources; autrement dit, les données et les applications peuvent être aisément déplacées d'un point à l'autre de l'infrastructure partagée. À défaut de gestion appropriée, il y a donc un risque de divulgation des données, car il est probable que les applications d'autres clients seront exécutées sur du matériel précédemment utilisé par des organisations humanitaires. En outre, les données pourraient demeurer indéfiniment dans l'infrastructure cloud. Des mesures doivent être prises pour contrôler cette menace: utiliser des ressources dédiées ou vérifier auprès du fournisseur les mesures instaurées pour supprimer ou autrement purger les données. Le chiffrement, indépendamment du fournisseur de services, pourrait offrir un niveau de protection supplémentaire.

10.4.2.5 Élimination des équipements

L'élimination des équipements est un aspect étroitement lié au point précédent et il convient d'être assuré qu'aucune donnée ou information ne pourra demeurer stockée ni être divulguée après la mise hors service ou l'élimination du matériel. Le fournisseur de services cloud doit garantir qu'il peut satisfaire à cette exigence; à défaut, il convient d'adopter d'autres mesures (chiffrement).

10.4.2.6 Disponibilité

Les services cloud doivent offrir le niveau de disponibilité requis; les contrats de niveau de service (SLA) sont extrêmement importants à cet égard. Le contrat doit être également examiné du point de vue des obligations et des responsabilités. Une vérification des informations accessibles au public, qui peut aider à apprécier la fiabilité réelle du service offert, est recommandée.

10.4.3 SÉGRÉGATION DES UTILISATEURS

Dans un environnement cloud, le fournisseur de services doit garantir la ségrégation des utilisateurs. Cependant, il est important, lorsqu'on évalue un fournisseur, et plus encore lorsque le fournisseur et la technologie sont peu connus, d'évaluer la technologie employée et de recueillir toute information susceptible d'aider à comprendre comment la ségrégation est garantie. Plusieurs facteurs ont une incidence sur la ségrégation, comme le modèle de service, le modèle de déploiement (cloud public ou privé), par exemple. Un test de pénétration peut être utile pour apprécier l'efficacité des mesures de ségrégation, mais seulement jusqu'à un certain point : il n'est valable qu'au moment où le test est réalisé et il ne détecte que les problèmes connus. Il peut être également très utile d'effectuer un contrôle des incidents antérieurs et de leur gestion par le fournisseur.

10.4.4 GOUVERNANCE

Le fournisseur de services doit être doté d'un cadre approprié de gouvernance de la sécurité, car il est à la base du contrôle et de la coordination des mesures de sécurité et de la gestion de l'évolution des menaces et des technologies. Il doit ensuite démontrer qu'il possède les éléments généralement associés à un responsable de niveau C* (par exemple DS, DSI, DT) chargé de la sécurité du cloud, qu'il a correctement mis en œuvre un cadre de gouvernance de la sécurité, que la sécurité et les risques de sécurité sont couverts par la gestion des risques et la gestion financière générales et qu'il respecte la réglementation et la législation. Il convient de déterminer s'il respecte les normes reconnues.

10.4.5 SÉCURITÉ OPÉRATIONNELLE

Le service cloud doit être exploité conformément à de strictes exigences de sécurité, et la sécurité doit être intégrée aux procédures opérationnelles standards. Elle est essentiellement définie par les éléments suivants :

- gestion de la configuration et des modifications pour contrôler ce qui est dans l'environnement de production et les modifications apportées, effectuer les tests requis et recevoir une autorisation en bonne et due forme avant d'effectuer des modifications ;
- gestion des vulnérabilités pour évaluer, détecter et corriger les failles de sécurité pouvant survenir dans les services et l'infrastructure ;
- suivi, pour détecter les anomalies, les attaques et les actes non autorisés susceptibles de compromettre la sécurité des services ;
- gestion des incidents : en cas d'incident, le fournisseur de services doit être capable de prendre les mesures adéquates pour atténuer, maîtriser et corriger le problème. Cette obligation comprend les communications et les rapports adressés aux clients et aux forces de l'ordre.

10.4.6 PERSONNEL

Le fournisseur de services cloud doit avoir pris des mesures pour évaluer la fiabilité du personnel intervenant dans la gestion des services. Une vérification appropriée des antécédents doit être effectuée pour toute fonction sensible ou dotée de privilèges. Les opérateurs doivent être formés et ils doivent comprendre et reconnaître leurs responsabilités.

10.4.7 DÉVELOPPEMENT

En général, les fournisseurs de services développent une grande partie de leur infrastructure. Ils doivent respecter les meilleures pratiques et les normes sectorielles afin que les menaces soient évaluées au cours du développement; des lignes directrices pour la sécurisation de la conception, du codage, des tests et du déploiement doivent être en place.

10.4.8 CHAÎNE D'APPROVISIONNEMENT

Les fournisseurs de services cloud recourent souvent à des produits et services tiers pour intégrer ou gérer les services qu'ils proposent. Or une faiblesse dans la chaîne d'approvisionnement peut compromettre la sécurité de l'ensemble du service et des applications cloud. Le fournisseur doit expliquer comment il sélectionne les fournisseurs tiers, la procédure d'agrément des services et produits, les modalités de gestion des risques de sécurité, les modalités de vérification de l'attitude des prestataires en matière de sécurité ainsi que les modalités de contrôle des pièces détachées, des mises à jour et d'autres changements. Cette procédure est d'autant plus importante que les services cloud peuvent être superposés et que d'autres prestataires peuvent intervenir en aval de la chaîne. Dans la mesure du possible, il convient de contrôler les fournisseurs ou de conclure des contrats interdisant au fournisseur de services cloud de faire appel à des fournisseurs tiers qui ne sont pas acceptables pour l'organisation.

10.4.9 GESTION DES UTILISATEURS

En fonction du service offert, la procédure d'autorisation peut être en partie gérée par le fournisseur de services cloud. Cette procédure doit être évaluée pour vérifier qu'elle est conforme aux meilleures pratiques, à la réglementation et aux besoins de l'organisation, afin de garantir un accès sécurisé aux interfaces de gestion. Ces interfaces permettent d'effectuer des actions qui, dans une certaine mesure, peuvent être considérées équivalentes aux actions physiques accomplies dans un centre de données traditionnel; elles doivent donc être soigneusement protégées. Les accès doivent être attribués avec le plus grand soin afin de garantir une gestion appropriée des rôles et des privilèges.

10.4.10 IDENTITÉ ET AUTHENTIFICATION

Comme pour la gestion des utilisateurs, l'accès à toute interface de service doit être strictement protégé. L'application des procédures d'identification et d'autorisation doit être évaluée pour s'assurer qu'elle répond aux besoins de sécurité de l'organisation. Exemples de méthodes : authentification à deux facteurs, utilisation de certificats clients TLS, systèmes à signature unique, etc. Les méthodes adoptées doivent être à jour conformément aux évolutions en matière de sécurité et à la complexité croissante des menaces.

10.4.11 INTERFACES EXTERNES

Lorsque les interfaces de gestion sont exposées, la surface d'attaque offerte aux entités hostiles se trouve accrue. Il convient donc d'évaluer la sécurité de ces interfaces par rapport à cette menace et la disponibilité de solutions telles que des réseaux privés ou des mesures équivalentes pour accéder aux interfaces privées.

10.4.12 ADMINISTRATION DES SERVICES

L'architecture et la gestion des systèmes d'administration doivent être soigneusement pensées et mises en œuvre car ces systèmes sont très exposés aux attaques. Une description de la gestion des systèmes d'administration et des procédures peut donc être utile pour évaluer la politique de sécurité du fournisseur de services.

10.4.13 AUDITS

Le fournisseur de services doit communiquer les résultats d'audits indépendants à l'organisation ou autoriser celle-ci à demander une évaluation ou un audit indépendant. Les données d'audit concernant les services (performances, durée d'indisponibilité, incidents de sécurité, etc.) doivent pouvoir être examinées.

10.4.14 UTILISATION DES SERVICES

L'organisation doit bien comprendre les interactions avec le service cloud : interfaces, échanges de données, procédure d'autorisation pour les utilisateurs, administration, charges de travail et tout autre aspect susceptible d'influencer le service, considéré comme la somme des activités du cloud et de l'organisation. Une évaluation précise des flux de données, des procédures et des architectures doit être réalisée préalablement à la mise en œuvre d'une solution cloud. Des procédures appropriées doivent être conçues et appliquées, le personnel doit être formé et les opérateurs doivent posséder les connaissances requises de la solution cloud, de son utilisation et de la relation avec l'organisation, et posséder d'autres informations liées à une bonne utilisation et à une gestion appropriée de la solution cloud.

10.5 DROITS DES PERSONNES CONCERNÉES

Les personnes concernées ont également un droit d'accès, de rectification, de suppression et d'opposition en ce qui concerne leurs données personnelles traitées dans le cloud¹⁸⁴. L'organisation humanitaire doit vérifier que le fournisseur n'élève pas d'obstacles techniques et organisationnels à l'exercice de ces droits, même lorsque les données font l'objet d'un traitement ultérieur par des sous-traitants. Le contrat qui lie le client au fournisseur doit exiger que ce dernier facilite l'exercice des droits des personnes concernées et qu'il veille à ce que l'exercice de ces droits soit protégé en ce qui concerne ses sous-traitants éventuels.

10.6 TRANSFERT INTERNATIONAL DE DONNÉES

Les services cloud impliquent par nature un transfert international de données personnelles vers diverses parties situées dans différents pays. La législation relative à la protection des données limite le transfert international de données ; les organisations humanitaires doivent donc s'assurer que l'utilisation de services cloud est conforme aux lois auxquelles elles sont éventuellement soumises et à leurs propres politiques internes. Cela signifie par exemple que tout contrat conclu avec un fournisseur de services cloud doit préciser comment le fournisseur respecte les exigences légales relatives au transfert international de données (par exemple au moyen de clauses contractuelles avec ses entités et avec ses sous-traitants). La réalisation d'une AIPD¹⁸⁵ préalablement au transfert international de données pourrait conforter la licéité de ce traitement du point de vue de la protection des données.

10.7 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Comme l'explique la section 4.5¹⁸⁶, la relation entre une organisation humanitaire qui place des données personnelles dans le cloud et le fournisseur de services cloud qu'elle charge contractuellement de le faire est une relation du même type que celle qui existe entre le responsable du traitement et le sous-traitant. Cependant, dans la pratique, ces fonctions peuvent être plus difficiles à catégoriser qu'il n'y paraît à première vue car cela dépendra de la latitude laissée au fournisseur, qui doit être définie dans le contrat entre le fournisseur et le client. L'essentiel est que ces incertitudes n'affectent pas les droits des personnes concernées, c'est-à-dire que les organisations humanitaires doivent être aussi transparentes que possible sur l'usage qu'elles font des services cloud et ne pas laisser les fournisseurs léser les personnes concernées.

¹⁸⁴ Voir [section 2.11: Droits des personnes concernées](#).

¹⁸⁵ Voir [section 10.8: Analyses d'impact relatives à la protection des données](#).

¹⁸⁶ Voir [section 4.5: Relation entre le responsable du traitement et le sous-traitant](#).

Lorsqu'une organisation humanitaire recourt à des services cloud, le fournisseur de ces services fait souvent appel à des sous-traitants ultérieurs. Le contrat avec le fournisseur doit préciser que le recours à des sous-traitants ultérieurs n'est possible que si le responsable du traitement (c'est-à-dire l'organisation humanitaire) y a consenti. Il doit être clairement précisé que le sous-traitant (le fournisseur de services cloud) doit informer le responsable du traitement de toute modification à cet égard, ce dernier conservant la possibilité de s'opposer à ces modifications ou de résilier le contrat.

10.8 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

Les AIPD sont des outils importants lors de la conception des projets pour s'assurer que tous les aspects de la réglementation applicable en matière de protection des données et les risques sont couverts. À chaque fois qu'on envisage de recourir à des services cloud, il est indispensable d'effectuer des AIPD adaptées à ces configurations¹⁸⁷. Les AIPD doivent analyser les détails et les spécifications du traitement, mais elles doivent aussi examiner les risques qu'il comporte et les mesures d'atténuation. Sur ce point, il est important de souligner qu'elles doivent être réalisées avant toute utilisation de services cloud.

10.9 PRIVILÈGES ET IMMUNITÉS DANS LE CLOUD

Au-delà des considérations qui précèdent, les organisations humanitaires bénéficiant de privilèges et d'immunités doivent également tenir compte du fait que le placement de données dans le cloud peut compromettre la protection apportée par ces privilèges et immunités sauf si des mesures juridiques, techniques et organisationnelles appropriées sont instaurées. Cette considération est essentielle, d'autant que dans une situation d'urgence humanitaire, les privilèges et immunités d'une organisation humanitaire peuvent être la première ligne de protection des données personnelles des individus vulnérables, notamment en situation de conflit ou dans d'autres situations de violence.

Les organisations humanitaires doivent étudier l'opportunité de prendre les mesures juridiques, organisationnelles et techniques suggérées ci-après pour assurer une protection adéquate de leurs privilèges et immunités dans un environnement cloud.

10.9.1 MESURES JURIDIQUES

- Les données doivent être exclusivement hébergées et traitées par des sous-traitants externes établis dans des États où les privilèges et immunités de l'organisation sont officiellement reconnus par des accords relatifs aux statuts

¹⁸⁷ Voir [chapitre 5 : Analyses d'impact relatives à la protection des données](#).

qui reconnaissent d'une part, l'inviolabilité des dossiers, des archives, de la correspondance et des communications quel que soit le lieu de conservation des données et l'entité qui les conserve, et, d'autre part, l'immunité à l'égard de toute forme de procédure judiciaire. Idéalement, cette protection juridique doit être confortée par un historique de respect constant de ces privilèges et immunités.

- Les sous-traitants et sous-traitants ultérieurs doivent être contractuellement tenus d'informer toute autorité souhaitant accéder aux données que celles-ci sont protégées par les privilèges et immunités d'une organisation humanitaire ; de rejeter toute demande d'accès émanant des autorités, aussi bien informelle, administrative que judiciaire, et de rediriger celle-ci vers l'organisation humanitaire ; d'informer immédiatement l'organisation humanitaire de toute demande d'accès à ses données, qu'elle soit informelle, administrative ou judiciaire, de l'identité de l'autorité demandeuse et du statut de la demande ; et d'aider l'organisation humanitaire à transmettre les informations et les documents dont l'organisation humanitaire peut avoir besoin dans une procédure informelle, administrative ou judiciaire pour faire valoir ses privilèges et immunités sur les données en question.

10.9.2 MESURES ORGANISATIONNELLES

- Les données de l'organisation humanitaire doivent être conservées sur des serveurs distincts et être séparées des données des autres clients des sous-traitants et sous-traitants ultérieurs.
- Les serveurs qui hébergent les données des organisations humanitaires doivent être clairement marqués de l'emblème de l'organisation et porter l'indication « Legally Privileged Information » (Informations confidentielles et protégées).
- Dans la mesure du possible, l'accès aux serveurs qui hébergent les données des organisations humanitaires ne doit être possible qu'avec l'autorisation des sous-traitants et de l'organisation humanitaire.
- Le personnel du sous-traitant et des sous-traitants ultérieurs doit être correctement informé du statut protégé des données et formé à la procédure à suivre en cas de demande d'accès émanant de tiers.

10.9.3 MESURES TECHNIQUES

- Les données hébergées dans un environnement cloud doivent être chiffrées, et seule l'organisation humanitaire doit posséder les clés de chiffrement.
- Si la solution cloud envisagée est un SaaS et si les sous-traitants et les sous-traitants ultérieurs ont besoin de gérer le service proposé, des dispositions doivent être prises pour garantir qu'ils pourront accéder au système pour le gérer, effectuer des mises à jour, corriger les bogues et assurer le support utilisateurs sans jamais avoir accès à des données non chiffrées.

APPLICATIONS MOBILES DE MESSAGERIE

UTILISATION POSSIBLE



DÉFIS

NÉCESSITÉ DE DÉFINIR
DES ORIENTATIONS CLAIRES
CONCERNANT LE TRAITEMENT
PAR LES ORGANISATIONS
HUMANITAIRES DES
DONNÉES ISSUES
D'APPLICATIONS
DE MESSAGERIE



CHAPITRE 11

APPLICATIONS MOBILES DE MESSAGERIE

11.1 INTRODUCTION¹⁸⁸

Dans leur travail quotidien, les organisations humanitaires recourent à de multiples canaux de communication, comprenant des moyens d'échange d'informations formels (radio et télévision, par exemple), informels, non officiels et directs. Pour employer les canaux de communication les plus adaptés à chaque situation, elles doivent comprendre la culture et les besoins de la société touchée par une crise et ses moyens de communication.

De ce point de vue, dans les lieux où les applications mobiles de messagerie sont très répandues, leur déploiement par les organisations humanitaires est particulièrement intéressant car elles permettent de communiquer immédiatement avec les personnes affectées par une crise ou par un conflit et contribuent à une coordination efficace des tâches et actions internes. Ce type de technologie peut renforcer l'efficacité de l'action humanitaire et permettre de toucher des populations dans des lieux reculés ou inaccessibles. Cependant, les applications mobiles de messagerie sont souvent employées sans vraiment tenir compte des risques relatifs à la protection des données personnelles.



A. Wiegmann/REUTERS

Des migrants rechargent leurs téléphones mobiles à une borne wifi dans un camp de fortune près de la gare ferroviaire de San Giovanni, à Côte, Italie (août 2016).

188 Ce chapitre s'inspire du rapport *Humanitarian Futures for Messaging Apps*, établi par le CICR, The Engine Room et Block Party en janvier 2017 : <https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html>.

Bien qu'elles offrent de formidables fonctionnalités, les applications mobiles de messagerie peuvent présenter d'importants risques pour la protection des données. Il semble qu'en pratique, les organisations humanitaires les déploient lorsqu'elles le jugent utile, sans suivre de procédure formelle reposant sur une analyse des risques et des considérations de viabilité et de gestion à long terme. Ce qui prime alors, ce sont leurs besoins pressants d'information et de communication. Dans la mesure où cette approche ne comporte pas d'analyse des risques, elle est contraire aux principes directeurs des organisations humanitaires, tels que la responsabilité, le bien-fondé, le principe « ne pas nuire » et le devoir de diligence. Comme pour tout autre canal de communication, l'adoption d'applications mobiles de messagerie exige une analyse attentive des avantages qu'elles offrent et des risques qu'elles comportent. Les questions à prendre en compte dans cette analyse dépendent des circonstances propres à une situation. À titre d'exemple, les préoccupations relatives à la sécurité des données personnelles d'individus dans une situation de violence politique peuvent être très différentes des préoccupations de sécurité en cas de catastrophe naturelle.

Les applications mobiles de messagerie installées sur des téléphones cellulaires ou sur d'autres appareils intelligents peuvent présenter des risques d'atteinte au droit des individus à la protection de leurs données personnelles. En effet, ces applications permettent non seulement d'échanger des données entre utilisateurs, mais aussi de traiter, d'agréger et de générer des quantités massives de données (métadonnées, données de localisation et contacts, par exemple). Certaines autorités de protection des données considèrent que les risques pour la protection des données personnelles résultent d'une combinaison des facteurs suivants : 1) méconnaissance de la part des utilisateurs des données qu'ils traitent effectivement sur un appareil intelligent, 2) absence de consentement des utilisateurs, 3) mesures de sécurité insuffisantes et 4) possibilité de traitement ultérieur¹⁸⁹.

Conformément à l'impératif de « proximité numérique », selon lequel les organisations humanitaires doivent s'efforcer d'être numériquement présentes là où sont les bénéficiaires (tout comme elles essaient de l'être physiquement), les organisations humanitaires tendent à déployer des applications mobiles de messagerie qui sont connues et utilisées dans une société donnée au moment de l'urgence humanitaire, comme WhatsApp, Facebook Messenger, Snapchat, Viber, Telegram ou LINE. Ces plateformes propriétaires sont de gros prestataires de services qui ne souhaitent pas nécessairement personnaliser leurs applications pour répondre aux besoins des organisations humanitaires. En même temps, le déploiement d'une plateforme de communication moins connue risque d'exclure des personnes que l'organisation cherche à aider.

189 Voir Groupe de travail « Article 29 » sur la protection des données, *Avis 02/2013 sur les applications destinées aux dispositifs intelligents*, 27 février 2013 : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp202_fr.pdf.

Le recours aux applications mobiles de messagerie peut aussi conduire à un traitement ultérieur des données collectées, y compris des données personnelles. Ces applications permettent de collecter des informations en ligne et peuvent aussi offrir de nouveaux moyens d'analyser les données disponibles. Autrement dit, les données et les métadonnées collectées via ces applications peuvent aider à recouper des informations de manière inédite. De ce fait, et compte tenu de la probabilité d'un traitement ultérieur des données personnelles, il est important de tenir compte de la finalité pour laquelle une application de messagerie est utilisée et des entités avec lesquelles les données collectées seront partagées. Les organisations humanitaires peuvent être alors amenées à constater qu'il leur est impossible d'affirmer de manière certaine que les utilisateurs peuvent effacer ou supprimer les données déjà soumises car cela supposerait de négocier avec de nombreuses parties.

Les applications mobiles de messagerie ont été principalement conçues pour les communications privées entre des individus ou de petits groupes. Les organisations humanitaires pourraient se servir de ce type de fonctionnalité pour donner des conseils de base ou s'informer auprès des bénéficiaires sur des incidents, un conflit en cours ou des besoins précis. Cependant, ces applications peuvent être également utilisées dans l'action humanitaire pour « diffuser » du contenu à de nombreux contacts ou followers. Lorsque les utilisateurs sont très nombreux notamment, ces applications peuvent fonctionner comme un canal de communication unidirectionnel (par exemple pour annoncer l'heure et le lieu de distribution de l'aide humanitaire ou un changement des horaires d'ouverture d'une clinique locale).

11.1.1 LES APPLICATIONS MOBILES DE MESSAGERIE DANS L'AIDE HUMANITAIRE

Une application mobile de messagerie est un logiciel qui permet d'envoyer et de recevoir des informations sur un téléphone mobile ou sur un autre appareil portable intelligent. La facilité de fonctionnement des applications mobiles a joué pour beaucoup dans leur popularité, dans leur acceptation par le public et dans la croissance continue de la demande. Il y a essentiellement trois différences entre les communications par application mobile de messagerie et les communications qui empruntent des réseaux de téléphonie mobile¹⁹⁰ :

- Les applications mobiles de messagerie émettent et reçoivent des données via une connexion Internet wifi ou une connexion données mobile (contrairement aux messages SMS, qui sont transmis sur les réseaux de téléphone traditionnels).
- Elles peuvent émettre ou recevoir un bien plus large éventail de données qu'il n'est possible de le faire par SMS ou même par MMS, le successeur multimédia du SMS. Au fil du temps, les applications mobiles de messagerie ont développé davantage de similitudes que de différences et, outre les appels voix et le texte,

¹⁹⁰ CICR, The Engine Room et Block Party, *Humanitarian Futures for Messaging Apps*, janvier 2017.

leurs utilisateurs peuvent aussi envoyer et recevoir les types d'informations suivants : fichiers, y compris des photos, images et (parfois) documents, enregistrements audio, y compris les enregistrements vocaux qui fonctionnent comme un message de messagerie vocale, données de localisation basées sur le capteur GPS du téléphone, appels vidéo live (dans certaines applications) et émoticônes (représentations pictographiques d'émotions ou d'objets).

- Elles peuvent transmettre du contenu chiffré de bout en bout. Cependant, elles peuvent aussi générer et conserver de grandes quantités de métadonnées – non chiffrées.

Les organisations humanitaires ont adopté les applications mobiles de messagerie pour les raisons suivantes¹⁹¹ :

- cibler une audience (membres du personnel ou bénéficiaires) utilisant déjà des applications mobiles de messagerie ;
- réduire les coûts de communication ;
- maintenir un contact fiable avec des personnes (personnel ou bénéficiaires) en déplacement ;
- communiquer avec des personnes dans des environnements où les autres moyens de communication ne sont pas disponibles ;
- augmenter la vitesse de communication ;
- améliorer la sécurité des communications numériques par rapport aux moyens de communication existants (lorsque ces applications offrent un chiffrement du contenu de bout en bout) ;
- faciliter la collecte ou la diffusion d'informations dans des zones difficiles d'accès, reculées ou inaccessibles ;
- accélérer la collecte des données ou accroître l'efficacité ;
- améliorer la coordination entre les bureaux.

Compte tenu de ces considérations, on distingue deux domaines d'analyse du point de vue de la protection des données :

- le traitement de données personnelles via les applications mobiles de messagerie elles-mêmes ;
- le traitement de données personnelles collectées par les organisations humanitaires via ces applications.

Ces deux domaines sont traités ci-après.

¹⁹¹ Pour une explication plus détaillée des raisons de l'adoption d'applications mobiles de messagerie dans l'action humanitaire, voir *Humanitarian Futures for Messaging Apps*, CICR, The Engine Room et Block Party, janvier 2017.

11.2 APPLICATION DES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

L'analyse de la protection des données présentée dans ce chapitre s'appuie sur les principes énoncés dans la première partie, où ils sont examinés en plus amples détails.

11.2.1 TRAITEMENT DES DONNÉES PERSONNELLES VIA LES APPLICATIONS MOBILES DE MESSAGERIE

Pour communiquer par messagerie mobile avec des individus dans une situation d'urgence humanitaire, les organisations humanitaires doivent, le plus souvent, installer et utiliser des applications déjà employées par la majorité de la population. La plupart du temps, les individus, c'est-à-dire les bénéficiaires, ont déjà téléchargé et installé ces applications et consenti à leurs conditions en matière de protection des données.

Toutefois, en communiquant avec les bénéficiaires par messagerie mobile, une organisation humanitaire peut inciter ceux-ci à croire, directement ou indirectement, que ces moyens de communication sont sûrs et qu'ils ne s'exposent à aucun préjudice lorsqu'ils communiquent avec elle. Il est donc important, indépendamment du consentement initial au traitement de leurs données personnelles donné par les bénéficiaires au fournisseur de l'application, que l'organisation humanitaire analyse les implications de cette utilisation afin que leurs échanges n'aient aucune conséquence néfaste inattendue. Il est recommandé pour cela de réaliser une AIPD, qui tiendra compte des considérations exposées ci-dessous. L'AIPD peut conclure que certaines catégories de données seulement peuvent être collectées ou communiquées par une certaine application ou qu'une application peut être utilisée dans certaines circonstances seulement et pas dans d'autres. Il est possible aussi que l'utilisation d'une application particulièrement répandue ne convienne pas à l'organisation humanitaire et que celle-ci ne souhaite s'en servir que pour informer des individus qu'elle a l'intention de communiquer par le biais d'une autre application, plus sûre. Lors de l'évaluation, il faut également tenir compte du fait que les applications mobiles de messagerie développent et modifient leurs fonctionnalités très rapidement et que rien ne garantit qu'une fonctionnalité offerte par une application sera indéfiniment disponible ou que les utilisateurs exécutent des logiciels à jour, en particulier dans les pays où le chiffrement est limité par la loi. De même, les politiques et déclarations des entreprises sur l'utilisation des données, la sécurité et la vie privée peuvent être revues ultérieurement. Il sera souvent impossible pour les organisations de voir les détails techniques du code sous-jacent, et donc d'effectuer une évaluation approfondie des effets de ces modifications sur la sécurité et la vie privée des utilisateurs. Les organisations qui font appel à des prestataires tiers pour gérer ou traiter les informations doivent aussi être prêtes à assumer la responsabilité de ces

risques. Des modifications apportées aux fonctionnalités de l'application peuvent nécessiter une révision de l'AIPD.

Il faut également souligner la différence entre les communications uni- et bidirectionnelles avec les bénéficiaires via des applications de messagerie car les communications bidirectionnelles comportent des risques bien plus élevés (des données personnelles potentiellement plus nombreuses peuvent être transférées) et posent aussi la question de la gestion/viabilité à long terme par rapport aux attentes.

11.2.1.1 Menaces potentielles

La protection des données et le respect de la vie privée sont des préoccupations présentes dans tous les domaines d'action des organisations humanitaires ; celles-ci doivent donc évaluer les risques lorsqu'elles envisagent de déployer une application mobile de messagerie. La préoccupation principale est le risque que des tiers aient accès aux données collectées par les organisations humanitaires pour des finalités contraires à la neutralité, à l'impartialité et à l'indépendance du travail humanitaire (par exemple, autorités locales, forces de l'ordre, groupes mus par divers intérêts ou entités privées).

Ces tiers peuvent être :

- des entités situées dans le pays d'origine des réfugiés, notamment des groupes armés et des autorités, qui peuvent souhaiter identifier des groupes ou des individus afin de leur nuire ou de les cibler ;
- des entités intervenant dans la politique de migration ou la sécurité, qui souhaitent comprendre et prévoir les tendances et les flux de déplacement ;
- des entités intervenant dans la surveillance aux fins de la sécurité nationale ;
- des parties hostiles qui souhaitent cibler et attaquer des organisations humanitaires et les personnes qu'elles aident ;
- des entités commerciales qui souhaitent effectuer un profilage comportemental de groupes précis, ce qui peut entraîner des discriminations¹⁹².

Les préoccupations dans ce domaine ont été reconnues et confirmées par la Conférence internationale des commissaires à la protection des données et à la vie privée, dans sa Résolution sur la protection des données personnelles et l'action humanitaire internationale :

« Les organisations humanitaires qui ne bénéficient pas des Privilèges et Immunités peuvent faire l'objet de pressions pour fournir des données collectées à des fins humanitaires à des autorités qui souhaitent utiliser ces données pour d'autres fins que celles pour lesquelles elles ont été originellement collectées (par exemple le contrôle des flux migratoires et la lutte contre le terrorisme).

192 Maria Xynou et Chris Walker, « Why we still recommend Signal over WhatsApp », 23 mai 2016 : <https://securityinabox.org/en/blog/why-we-still-recommend-signal-over-whatsapp/>.

Le risque de détournement de finalité peut avoir un impact considérable sur le droit à la protection des données des réfugiés et sur leur sécurité, ainsi que sur l'action humanitaire en général¹⁹³. >

11.2.2 QUELS TYPES DE DONNÉES LES APPLICATIONS MOBILES DE MESSAGERIE COLLECTENT-ELLES OU CONSERVENT-ELLES ?

Il existe trois protocoles principaux dans les domaines de la messagerie mobile et du chiffrement : le protocole Signal, MTProto et iMessage¹⁹⁴ :

1. Le protocole Signal (anciennement Axolotl et TextSecure) est utilisé par les applications suivantes : Signal Messenger développée par Open Whisper Systems, WhatsApp détenue par Facebook, Facebook Messenger (dans les conversations secrètes), Google Allo (en mode « navigation privée »), Skype (dans les conversations privées depuis mi-2018) et Viber (mise en œuvre propriétaire et modifiée).
2. Le protocole MTProto a été développé par Telegram qui l'utilise encore aujourd'hui (dans les discussions secrètes).
3. Le protocole iMessage a été développé par Apple qui l'utilise aujourd'hui dans sa messagerie instantanée (iMessage).

Chacun de ces protocoles de messagerie génère et traite différents types de données, et protège également le contenu des messages et les métadonnées à des degrés divers.

Contenu des messages : Bien que certains grands éditeurs d'applications mobiles de messagerie déclarent que leur application garantit un chiffrement de bout en bout, ce qui signifie qu'elles sont incapables de décrypter ou de lire le contenu des messages, d'autres applications très répandues comme Facebook Messenger stockent le contenu de tous les messages sur leurs serveurs. Notons que dans certaines applications, le chiffrement de bout en bout est seulement proposé en option (c'est le cas de Telegram, LINE et Facebook Messenger). Dès lors, si les utilisateurs ne savent pas qu'ils doivent activer cette fonctionnalité dans leurs paramètres, toutes les données de messages seront envoyées non chiffrées. Les communications avec la plupart des bots sur des services comme Telegram ne sont pas chiffrées de bout en bout. Il est important de souligner que bien que le contenu soit protégé, les métadonnées ne bénéficient pas forcément des mêmes garanties (voir la partie « Métadonnées » ci-dessous)¹⁹⁵.

¹⁹³ ICDPPC, Résolution sur la protection des données personnelles et l'action humanitaire internationale, Amsterdam, 2015 : https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2015/11/resolution_sur_laprotectiondesdonneespersonnellesetlactionhumani.pdf.download.pdf/resolution_sur_laprotectiondesdonneespersonnellesetlactionhumani.pdf.

¹⁹⁴ CICR et Privacy International, Section 6: Cash-transfer programmes (CTP), dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 50.

¹⁹⁵ Lucy Handley, « Sheryl Sandberg: WhatsApp metadata informs governments about terrorism in spite of encryption », CNBC, 31 juillet 2017 : <https://finance.yahoo.com/news/sheryl-sandberg-whatsapp-metadata-informs-112540721.html>.

Informations des utilisateurs : Lorsque les utilisateurs souscrivent à une application mobile, ils doivent donner des informations les concernant (allant du numéro de téléphone pour la plupart des applications, à des images, au nom et à l'adresse mail dans le cas de WeChat et Facebook Messenger). L'enregistrement de la carte SIM est obligatoire dans de nombreux pays ; l'obligation de donner un numéro de téléphone imposée par l'application peut alors empêcher une utilisation anonyme de l'application. Dans certains pays d'Amérique latine, les utilisateurs ont également l'obligation d'enregistrer le numéro de leur appareil¹⁹⁶. De nombreuses applications accèdent automatiquement à la liste des contacts téléphoniques d'un utilisateur à la souscription pour trouver les autres contacts qui ont déjà souscrit à l'application. Dans certains cas, les applications peuvent stocker ces données séparément (WhatsApp, par exemple, a confirmé en juin 2016 qu'elle conserve les listes de contacts)¹⁹⁷. Dans certains cas, des informations sur les groupes auxquels l'utilisateur appartient peuvent être également enregistrées.

Métadonnées : En fonction de leurs conditions d'utilisation, les applications de messagerie collectent diverses quantités de métadonnées, y compris les sites et informations accessibles depuis l'application. Les métadonnées potentiellement générées à partir d'un message comprennent, par exemple, le numéro IMEI (identité internationale d'équipement mobile)/IMSI (identité internationale d'abonné mobile), le numéro de téléphone de l'émetteur, le numéro de téléphone du destinataire, la taille du message, les données de localisation, les données relatives au temps, les adresses IP, le modèle du matériel et des informations sur le navigateur Web¹⁹⁸. De nombreux éditeurs d'applications déclarent que ces données sont conservées sur leurs serveurs, mais ils précisent rarement la durée de conservation des données ou si les métadonnées sont chiffrées et comment (même parmi les applications qui affirment avoir mis en place un chiffrement de bout en bout). Alors que certaines applications de messagerie sur ordinateurs individuels proposent de masquer les métadonnées en utilisant les services cachés de Tor (logiciel qui permet la navigation anonyme)¹⁹⁹, les principales applications

¹⁹⁶ GSMA, *Mandatory registration of prepaid SIM cards: Addressing challenges through best practice*, avril 2016 : www.gsma.com/publicpolicy/wp-content/uploads/2016/04/Mandatory-SIM-Registration.pdf.

¹⁹⁷ Micah Lee, « Battle of the secure messaging apps: How Signal beats WhatsApp », The Intercept, 22 juin 2016 : <https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>.

¹⁹⁸ CICR et Privacy International, Section 6: Cash-transfer programmes (CTP), dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 60.

¹⁹⁹ Les applications suivantes utilisent les services cachés de Tor (logiciel conçu pour permettre les communications anonymes) : Guardian Project, *What is Orbot?* : <https://guardianproject.info/apps/orbot/> ; Security in a Box, *Guide to Orbot* : <https://securityinabox.org/en/guide/orbot/android> ; Tor Project, *Tor Messenger Beta: Chat over Tor, Easily*, 29 octobre 2015 : <https://blog.torproject.org/blog/tor-messenger-beta-chat-over-tor-easily> ; Joseph Cox, 'Ricochet', *the Messenger That Beats Metadata*, *Passes Security Audit*, 17 février 2016 : <http://motherboard.vice.com/read/ricochet-encrypted-messenger-tackles-metadata-problem-head-on>.

mobiles de messagerie disponibles aujourd'hui n'offrent pas cette possibilité. Les applications mobiles les plus respectueuses de la vie privée, comme Signal²⁰⁰, visent simplement à collecter le moins possible de métadonnées.

Données déduites : Même avec le chiffrement de bout en bout d'un contenu, il est possible de déduire de nombreuses informations à partir des métadonnées générées par les messages :

Des chercheurs du MIT et de l'Université catholique de Louvain, en Belgique, ont analysé les données de 1,5 million d'utilisateurs de téléphones mobiles dans un petit pays européen sur une période de 15 mois ; ils ont découvert que, avec une résolution temporelle et spatiale relativement faible, quatre points de repère suffisent à identifier de manière unique 95 % de ces utilisateurs.

Autrement dit, pour extraire l'intégralité des informations de localisation d'une seule personne à partir d'un ensemble de données « anonymisées » de plus d'un million de personnes, vous n'auriez qu'à la placer quatre fois par an à une centaine de mètres d'une antenne-relais de téléphonie mobile pendant une heure. Quelques publications sur Twitter révéleraient probablement toutes les informations nécessaires, si elles contiennent des informations spécifiques sur la localisation de la personne²⁰¹.

Partage de données avec des fournisseurs tiers : Les éditeurs d'applications mobiles de messagerie déclarent fréquemment qu'ils partagent les données personnelles des utilisateurs avec d'autres entreprises dont les services permettent le fonctionnement de l'application. Cependant, il est rare qu'ils déclarent avec quelles entreprises ils travaillent, quels services elles fournissent, à quelles données elles ont accès ou comment les données sont traitées et stockées. Twilio, un fournisseur tiers qui travaille avec certains éditeurs d'applications mobiles de messagerie, produit des rapports de transparence succincts dans lesquels il indique avoir reçu 376 demandes de données émanant d'agences internationales au premier semestre 2016 contre 46 sur la même période en 2015²⁰².

Preuve de l'installation d'une application mobile sur le téléphone d'un utilisateur :

En ayant accès à l'appareil d'un individu, les autorités pourraient trouver des preuves physiques de l'installation d'une application mobile de messagerie. Il serait aussi possible d'avoir cette information par d'autres moyens – par exemple les utilisateurs doivent généralement associer une adresse mail à leur smartphone pour télécharger une application mobile, ce qui crée un lien potentiellement traçable entre l'application mobile et d'autres activités en ligne.

200 Signal, « Grand jury subpoena for Signal user data, Eastern District of Virginia », 4 octobre 2016 : <https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/>.

201 L. Hardesty, « How hard is it to 'de-anonymize' cellphone data? », MIT News, 27 mars 2013 : <https://newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data>.

202 Voir Twilio, *Transparency Policy* : <https://www.twilio.com/legal/transparency>.

11.2.3 COMMENT D'AUTRES PARTIES PEUVENT-ELLES ACCÉDER À DES DONNÉES PARTAGÉES SUR DES APPLICATIONS MOBILES DE MESSAGERIE ?

D'autres parties peuvent accéder aux données transmises via des applications mobiles de messagerie, notamment par les moyens suivants :

- Un éditeur d'applications mobiles de messagerie (ou un fournisseur tiers qui accède aux informations personnelles des utilisateurs de l'application) divulgue le contenu de messages ou les métadonnées qu'il conserve sur ses serveurs à la demande d'une autorité du pays où ces données sont stockées.
- Une autre partie obtient un accès illicite ou caché au contenu de messages ou aux métadonnées conservées sur les serveurs d'un éditeur d'applications (par piratage) ou accède à ces informations au cours de leur transit entre les deux acteurs (attaque appelée « man-in-the-middle » ou « attaque de l'intercepteur »). À titre d'exemple, des tests effectués fin 2013 par le Citizen Lab de l'Université de Toronto ont montré que l'application mobile de messagerie LINE ne chiffrait pas le contenu envoyé sur les connexions 3G alors que le contenu envoyé en wifi était chiffré²⁰³.
- Lorsqu'un appareil (par exemple un téléphone mobile ou un ordinateur) est saisi, l'utilisation d'outils judiciaires peut permettre d'accéder aux métadonnées, y compris au contenu et aux données que l'utilisateur pense avoir supprimés²⁰⁴. Des outils d'extraction de données peuvent être utilisés pour télécharger des données à partir de téléphones mobiles, notamment :
 - les contacts ;
 - les données d'appel (qui nous appelons, quand et combien de temps dure l'appel) ;
 - les messages texte ;
 - les fichiers sauvegardés (photos, vidéos, fichiers audio, documents, etc.) ;
 - les données d'application (les applications que nous utilisons et les données stockées sur celles-ci) ;
 - les informations de localisation ;
 - les connexions au réseau wifi (qui peuvent révéler les lieux où nous nous sommes connectés au wifi, comme notre lieu de travail et les endroits où nous nous sommes rendus).

²⁰³ Les réseaux 3G sont chiffrés par défaut, mais seulement au niveau du fournisseur du réseau, ce qui implique que les fournisseurs d'accès Internet et les sociétés de télécommunications peuvent décrypter les informations envoyées sur ces réseaux. Citizen Lab, *Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications*, novembre 2013 : <https://citizenlab.ca/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/> ; J. Russell, « Thailand's Government Claims It Can Monitor The Country's 30M Line Users » : <https://techcrunch.com/2014/12/23/thailand-line-monitoring-claim/>.

²⁰⁴ CICR et Privacy International, Section 5.3: Other metadata, dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018.

Certains outils d'extraction de données des téléphones mobiles peuvent également accéder aux données stockées, non pas sur nos téléphones, mais dans le cloud, ou aux données dont nous ne connaissons pas l'existence ou auxquelles nous n'avons pas accès, c'est-à-dire les données supprimées²⁰⁵.

- Des parties accèdent au contenu des applications mobiles de messagerie par d'autres méthodes secrètes, par exemple en ayant accès aux codes de connexion SMS envoyés aux utilisateurs lorsqu'ils souscrivent à une application en redirigeant le trafic sur les réseaux conventionnels de téléphonie mobile²⁰⁶ ou en incitant les utilisateurs à installer un logiciel malveillant (malware) sur leur téléphone, qui donne accès à l'appareil et aux données qui y sont enregistrées²⁰⁷.
- Un individu est contraint de remettre son téléphone. Le chiffrement de bout en bout ne chiffre que les données en transit, pas celles qui sont enregistrées sur l'appareil de l'utilisateur. Si une partie accède physiquement à un téléphone ou à un ordinateur ayant accès à un compte d'application mobile de messagerie (par exemple en obligeant l'utilisateur à le déverrouiller), elle peut prendre connaissance du contenu des messages et des détails des applications installées sur l'appareil. Dans certains pays, les autorités considèrent que le seul fait d'installer des applications mobiles comme WhatsApp est un indicateur de comportement subversif²⁰⁸. Signal, Telegram et SnapChat proposent toutes des messages qui s'autodétruisent, c'est-à-dire qu'ils ne sont visibles sur le téléphone de l'émetteur et du destinataire que pendant une durée limitée avant d'être automatiquement effacés.
- Un éditeur d'applications mobiles de messagerie laisse une autorité accéder directement au contenu ou aux données transmis sur l'application en intégrant une fonctionnalité secrète dans son code (appelée « porte dérobée »). Certains pays auraient ainsi menacé de condamner à des amendes les éditeurs d'applications qui n'introduisaient pas de portes dérobées dans leur code,

205 Mobile Phone Extraction, explicatif élaboré par Privacy International et Liberty dans le cadre de l'action commune « Neighbourhood Watch: How policing surveillance technology impacts your rights », disponible à l'adresse : <https://privacyinternational.org/neighbourhood-watched>.

206 Frederic Jacobs, « How Russia Works on Intercepting Messaging Apps », 30 avril 2016 : <https://www.bellingcat.com/news/2016/04/30/russia-telegram-hack/> ; Thaddeus T. Grugg, « Operational Telegram », 18 novembre 2015 : <https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a#.f1vg48cli>.

207 Voir, par exemple, Iran Threats, « Malware posing as human rights organizations and commercial software targeting Iranians, foreign policy institutions and Middle Eastern countries », 1^{er} septembre 2016 : <https://iranthreats.github.io/resources/human-rights-impersonation-malware/>.

208 Electronic Frontier Foundation, « Your Apps, Please? China Shows how Surveillance Leads to Intimidation and Software Censorship », janvier 2016 : <https://www.eff.org/deeplinks/2016/01/china-shows-how-backdoors-lead-software-censorship> ; Maria Xynou et Chris Walker, « Why we still recommend Signal over WhatsApp », 23 mai 2016.

citant en particulier WhatsApp, Telegram et Viber²⁰⁹. D'autres entreprises ont déclaré publiquement avoir refusé d'accéder à la demande d'organismes gouvernementaux de créer des portes dérobées²¹⁰. En outre, les organismes de renseignement tentent aujourd'hui encore d'autoriser la création de portes dérobées pour leur permettre d'accéder au contenu chiffré²¹¹.

- Si le groupe est « public » (c'est-à-dire que tout le monde peut le rejoindre, sans invitation), il est possible d'accéder à ces données ; de plus, dans une messagerie de groupe, telle que WhatsApp, chaque membre du groupe peut extraire le nom sous lequel les autres membres se sont inscrits, leur numéro de téléphone et les messages qu'ils ont envoyés²¹².
- Les protections utilisées sur les applications de messagerie ont aussi été compromises par des failles du SS7, soit des protocoles de télécommunications sous-jacents²¹³. Ces failles permettent aux individus d'usurper un numéro de téléphone, de créer une copie du compte sur l'application de messagerie et d'envoyer et de recevoir tous les messages liés à ce numéro, et ce, sans que l'utilisateur ne s'en rende compte²¹⁴.

209 Patrick Howell O'Neill, « Russian bill requires encryption backdoors in all messenger apps », 20 juin 2016 : <http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb/>.

210 Jon Russell, « Tim Cook Says Apple Won't Create Universal iPhone Backdoor For FBI », 17 février 2016 : <https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/> ; Max Eddy, « What It's Like When The FBI Asks You To Backdoor Your Software », 8 janvier 2014 : <http://securitywatch.pcmag.com/security/319544-what-it-s-like-when-the-fbi-asks-you-to-backdoor-your-software>.

211 Pour en savoir plus, voir : Privacy International, « Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages », 29 mai 2019. Disponible à l'adresse : <https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages>.

212 V. Wadhwa, « WhatsApp Public Groups Can Leave User Data Vulnerable to Scraping », VentureBeat, 3 avril 2018 : <https://venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping/>.

213 Aujourd'hui, le réseau téléphonique public commuté (RTPC, soit l'ensemble des réseaux téléphoniques à commutation de circuits opérés au niveau local, régional ou national) utilise un système de signalisation appelé Signalling System N° 7 (« SS7 »). Le système SS7 est également la base de la téléphonie mobile ; on l'utilise pour acheminer les appels, envoyer/recevoir des SMS et pour d'autres services mobiles. Pour une présentation plus détaillée, voir : CICR et Privacy International, Section 5: Telecommunications and messaging, dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018.

214 Vijay, « How To Hack WhatsApp Using SS7 Flaw », TechWorm (blog), 2 juin 2016 : <https://www.techworm.net/2016/06/how-to-hack-whatsapp-using-ss7-flaw.html> ; John Leyden, « SS7 Spookery on the Cheap Allows Hackers to Impersonate Mobile Chat Subscribers », The Register, 10 mai 2016, édition en ligne, sec. Security : https://www.theregister.com/2016/05/10/ss7_mobile_chat_hack/?ma=1504742415001.

11.2.4 FONCTIONNALITÉS DES APPLICATIONS MOBILES DE MESSAGERIE LIÉES AU RESPECT DE LA VIE PRIVÉE ET À LA SÉCURITÉ

Les fonctionnalités suivantes doivent être recherchées lorsqu'on choisit une application mobile de messagerie pour échanger des informations en situation humanitaire.

11.2.4.1 Anonymat autorisé/pas d'exigence d'authentification de l'identité

Permettre aux utilisateurs de communiquer anonymement via une application mobile de messagerie protège leur vie privée, alors qu'exiger des noms réels, des adresses mail et des identités authentifiées accroît le risque que les individus soient surveillés et ciblés. Moins un utilisateur doit donner d'informations pour utiliser une application mobile de messagerie, moins il y aura d'informations accessibles à des tiers.

11.2.4.2 Pas de conservation du contenu des messages

La vie privée des utilisateurs est mieux respectée lorsque le contenu des messages est envoyé à un appareil et supprimé des serveurs de l'éditeur de l'application une fois le message lu. Des applications mobiles de messagerie comme Telegram, WhatsApp, Viber et Signal déclarent ne pas stocker systématiquement les messages et effacer le contenu des messages sur leurs serveurs dès leur réception par le(s) destinataire(s). Cependant, des entreprises telles que Skype conservent le contenu des messages sur leurs serveurs après que l'utilisateur a lu le message, sans préciser la durée de conservation maximale au terme de laquelle les données seront effacées.

11.2.4.3 Chiffrement de bout en bout

Le chiffrement de bout en bout restreint la capacité de tiers comme des gouvernements ou des adversaires à intercepter les communications entre des organisations humanitaires et leurs bénéficiaires et à voir le contenu des messages. Dans ce cas, même si une entreprise conserve les données de contenu, celles-ci seront chiffrées et ne seront donc pas lisibles pour l'entreprise ou un autre tiers cherchant à y accéder. Le chiffrement restreint ainsi le type et la quantité de données lisibles que les éditeurs d'applications peuvent être forcés de divulguer. Dans l'idéal, il doit être déployé par défaut dans les conversations individuelles et collectives. Des ressources en ligne évaluent le niveau de sécurité des applications²¹⁵.

11.2.4.4 Propriété des données

Il est essentiel que les utilisateurs d'applications mobiles de messagerie soient considérés comme les propriétaires légaux de leurs données personnellement identifiables et du contenu de leurs messages. De cette façon, les éditeurs ne

²¹⁵ Electronic Frontier Foundation, *Secure Messaging Scorecard* : <https://www EFF.org/pages/secure-messaging-scorecard>.

peuvent pas utiliser ces données à des fins commerciales ou à d'autres fins sans le consentement explicite de l'utilisateur. Cet aspect est traité par la législation nationale de certains pays et peut être également régi par les conditions générales de l'application.

11.2.4.5 Non-conservation ou conservation minimale des métadonnées

Moins les applications mobiles de messagerie conservent de métadonnées sur leurs serveurs, moins elles ont de données à divulguer sous la contrainte à des gouvernements ou à vendre à des intérêts commerciaux. Les applications telles que Signal et Telegram prétendent ne conserver aucune métadonnée sur leurs utilisateurs bien que l'affirmation de Telegram soit contestée²¹⁶, alors que la plupart des applications examinées déclarent collecter les numéros des contacts, les journaux d'activité sur l'application et les données de localisation.

11.2.4.6 Code de l'application mobile de messagerie en open source

Lorsque le code qui sous-tend une application mobile de messagerie est ouvert, l'application peut être examinée par des tiers indépendants pour vérifier qu'elle ne présente pas de vulnérabilité aux menaces de sécurité ni de fonctions de surveillance cachées comme les portes dérobées. Idéalement, une application mobile de messagerie publiera toute sa base de code : Signal et Wire sont totalement ouvertes, tandis que Telegram et Threema ne publient qu'une partie de leur code²¹⁷.

11.2.4.7 L'entreprise examine soigneusement les demandes de divulgation émanant des forces de l'ordre

Il est indispensable que l'éditeur de l'application mobile de messagerie contrôle rigoureusement les demandes de données utilisateurs émanant des forces de l'ordre et qu'il y réponde avec modération. Dans l'idéal, il donnera des informations sur son comportement à cet égard en publiant des rapports de transparence régulièrement actualisés détaillant les demandes reçues, leur pays d'origine et les types d'informations fournies. Au moment où nous écrivons, Microsoft²¹⁸ et Facebook²¹⁹ publient régulièrement des rapports de transparence indiquant le nombre de demandes reçues et quelle quantité de données elles transmettent aux forces de l'ordre, tandis que l'entreprise Open Whisper Systems (l'éditeur de Signal) publie une description plus détaillée des demandes peu nombreuses qu'elle reçoit²²⁰.

²¹⁶ Jeremy Seth Davis, « Telegram metadata allows for 'stalking anyone' », 30 juillet 2015 : <https://www.scmagazine.com/home/security-news/telegram-metadata-allows-for-stalking-anyone/>.

²¹⁷ Pour plus d'informations à ce sujet, voir Lorenzo Franceschi-Bicchieri, « Wickr: Can the Snapchat for Grown-Ups Save You From Spies? », 4 mars 2013 : <http://mashable.com/2013/03/04/wickr/#3EwYsDKZ5kqh>.

²¹⁸ Microsoft, *Law Enforcement Requests Report* : <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>.

²¹⁹ Facebook, *Government Requests for User Data* : <https://govtrequests.facebook.com/about/>.

²²⁰ Open Whisper Systems, *Government Requests*, « Grand jury subpoena for Signal user data, Eastern District of Virginia » : <https://whispersystems.org/bigbrother>.

En outre, il est important de déterminer si une entité qui fournit une application mobile de messagerie est située dans un pays où le gouvernement a d'importants pouvoirs de surveillance ou un historique de contournement régulier des contraintes légales encadrant la surveillance²²¹.

11.2.4.8 Partage limité de données personnelles avec des tiers

Bien que les applications mobiles de messagerie aient besoin de partager certaines données avec des tiers (en général celles qui jouent un rôle technique dans le traitement des données) pour faciliter la livraison de leurs services, il est de la plus haute importance que les entreprises ne partagent pas les données personnelles et qu'elles ne partagent que des données minimales désidentifiées lorsque cela s'avère strictement nécessaire. Les organisations doivent choisir une application mobile de messagerie qui ne partage aucune donnée avec les tiers outre ce qui est strictement nécessaire au fonctionnement technique du service – et en demander confirmation aux éditeurs avant de poursuivre.

11.2.4.9 Restriction de l'accès via le système d'exploitation, le logiciel ou les correctifs de sécurité spécifiques de l'appareil

De nouvelles versions des systèmes d'exploitation des téléphones mobiles intègrent également des fonctions de sécurité supplémentaires, par exemple pour interdire aux applications d'accéder aux données stockées ailleurs sur l'appareil. Les utilisateurs peuvent également choisir de délivrer des autorisations individuelles ou d'autoriser le chiffrement intégral de l'appareil. Cependant, il est peu probable de trouver ces nouveaux appareils et systèmes d'exploitation dans des zones où interviennent les organisations humanitaires. Des tiers non autorisés pourraient alors accéder aux données stockées, ainsi qu'aux métadonnées générées via les applications de messagerie, à l'aide des différents moyens décrits plus haut (section 11.2.3)²²².

11.2.5 TRAITEMENT DE DONNÉES PERSONNELLES RECUEILLIES PAR DES APPLICATIONS MOBILES DE MESSAGERIE

Une fois que les bénéficiaires entrent en communication avec les organisations humanitaires par le biais d'applications mobiles de messagerie, les organisations humanitaires auront besoin de collecter, très probablement de stocker sur d'autres plateformes, d'agréger et d'analyser les informations fournies.

Il est indispensable que ce traitement respecte également les principes de protection des données énoncés dans la première partie de ce manuel. Quelques principes propres aux données collectées par des applications mobiles de messagerie, sont examinés ci-après.

²²¹ Sources intéressantes pour des recherches complémentaires : <https://www.digcit.org/fr/index.html> ; <https://privacyinternational.org/advocacy> ; <https://advox.globalvoices.org/> ; et <https://www.eff.org/deeplinks>.

²²² CICR et Privacy International, Section 5.3: Other metadata, dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018, p. 61–62.

Communiquer avec des communautés en situation humanitaire implique toujours de négocier un ensemble de questions complexes, comme les suivantes :

- Les individus ont-ils besoin de donner à une organisation humanitaire « l'autorisation » d'ajouter leurs données à un groupe ou circuit ?
- Comment un individu peut-il choisir de ne pas recevoir le contenu ? Cette procédure est-elle bien expliquée dès le départ ?
- Comment les personnes peuvent-elles être informées sur les tiers avec lesquels leurs données personnelles sont partagées ?
- Si des demandes d'aide qui ne relèvent pas du mandat de l'organisation humanitaire sont partagées avec une autre organisation humanitaire, des protocoles de partage des données ont-ils été clairement définis ?
- Comment les personnes savent-elles combien de temps leurs données seront conservées et pour quelles finalités ?
- Comment communiquer sur toutes ces questions pour que même des personnes peu familières avec la technologie puissent les comprendre aisément ?

Travailler avec des applications mobiles de messagerie ajoute un niveau de complexité à toutes ces questions.

Les AIPD des organisations humanitaires doivent préciser les divers protocoles et le degré auquel chacun d'eux protège le contenu et les métadonnées. Ce faisant, elles pourront évaluer les options et décider laquelle est la plus adaptée à une finalité donnée (par exemple, le partage d'informations sensibles), analyser le contexte dans le lequel le protocole sera utilisé (par exemple, un contexte juridique et politique), ainsi que définir le profil des bénéficiaires.

11.3 FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

Les organisations humanitaires peuvent traiter des données personnelles recueillies par des applications mobiles de messagerie sur un ou plusieurs des fondements juridiques suivants²²³ :

- l'intérêt vital de la personne concernée ou d'une autre personne ;
- l'intérêt public, en particulier basé sur le mandat confié à une organisation en vertu du droit national ou international ;
- le consentement ;
- l'intérêt légitime de l'organisation ;
- l'exécution d'un contrat ;
- le respect d'une obligation légale.

²²³ Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

Dans la plupart des cas, le traitement des données personnelles collectées par le biais d'applications mobiles de messagerie peut se fonder sur le consentement, l'intérêt vital ou l'intérêt public. Si les individus ont déjà communiqué avec une organisation humanitaire par le biais d'une application mobile de messagerie ou lui ont donné leur numéro de téléphone, on peut considérer qu'ils ont donné leur consentement pour recevoir des messages. Le consentement doit toutefois être éclairé et il est essentiel que les organisations humanitaires donnent les informations pertinentes concernant la finalité, la conservation ou le partage des données collectées, etc., comme l'explique la section correspondante de ce manuel²²⁴.

Hormis le consentement, on peut considérer que les messages concernant des urgences humanitaires relèvent de l'intérêt vital des personnes concernées ou de l'intérêt public. Ces fondements juridiques exigent aussi que les individus soient informés, ce qui peut être fait en leur envoyant un lien vers la notice d'information dans un message adressé via l'application mobile de messagerie.

11.4 CONSERVATION DES DONNÉES

Les organisations humanitaires doivent préciser dans leurs notices d'information et dans leurs politiques de protection des données la durée de conservation envisagée pour les données qu'elles collectent.

Certaines données saisies dans la plupart des applications mobiles de messagerie sont conservées et stockées par des tiers (éditeurs des applications de messagerie), qui partagent eux-mêmes une partie de ces données avec d'autres – prestataires de services permettant l'exécution de l'application ou sociétés mères (comme pour Facebook et WhatsApp). L'organisation humanitaire doit donc également souligner dans sa notice d'information que les données fournies par le biais de l'application mobile seront également conservées par l'éditeur de l'application et par les tiers intervenant sous sa responsabilité, et qu'elles seront gouvernées par leurs politiques de protection des données.

Les organisations humanitaires doivent également envisager de se doter d'une politique de conservation relative aux échanges d'informations ou « conversations » et de supprimer régulièrement l'historique des conservations afin de garantir la minimisation des données.

²²⁴ Voir [chapitre 2 : Principes fondamentaux de la protection des données](#).

11.5 DROITS DE RECTIFICATION ET DE SUPPRESSION

Conformément à la première partie de ce manuel, les organisations humanitaires doivent prévoir des mécanismes facilitant l'exercice effectif des droits des personnes concernées et en informer celles-ci dans leurs politiques de protection des données.

Cette obligation ne pose peut-être pas problème pour les données extraites des applications mobiles de messagerie par les organisations humanitaires, mais il peut être difficile de déclarer avec confiance que les applications permettent aux utilisateurs de détruire ou supprimer les données qu'ils ont déjà soumises, car cela impliquerait des négociations avec de multiples parties (qui ne sont pas toutes transparentes sur les données détenues). Il est recommandé de le préciser également dans la politique de protection des données.

11.6 MINIMISATION DES DONNÉES

Étant donné le peu de contrôle qu'ont les organisations humanitaires sur les données collectées par les applications mobiles de messagerie, celles qui souhaitent utiliser ces applications doivent s'efforcer de minimiser la quantité d'informations qui leur est soumise. Des travaux de recherche ciblés sur les États-Unis ont également constaté qu'en général, les utilisateurs n'ont pas connaissance des implications, pour leur vie privée, de l'installation d'une application mobile de messagerie et du partage de données qu'elle entraîne²²⁵. Par conséquent, les organisations humanitaires devraient mettre en place des mesures destinées à inciter les personnes touchées par les crises à partager les données personnelles absolument indispensables à la fourniture d'aide humanitaire.

²²⁵ P. G. Kelley *et al.*, « A Conundrum of Permissions: Installing Applications on an Android Smartphone », dans *Financial Cryptography and Data Security*, vol. 7398, Springer, Berlin, Heidelberg, 2012 : http://dx.doi.org/10.1007%2F978-3-642-34638-5_6.

EXEMPLE :

Dans la perspective des élections municipales en Afrique du Sud en août 2016, la fondation sans but lucratif Africa's Voices Foundation s'est associée à Livity Africa pour évaluer l'impact de *Voting is Power*, une campagne encourageant les jeunes à voter et à faire connaître les questions qu'ils jugeaient importantes²²⁶.

À cette fin, ces deux organisations ont effectué des enquêtes en ligne auprès de jeunes (par mail et via WhatsApp et Facebook Messenger) et publié des billets sur les réseaux sociaux. WhatsApp et Messenger ont été sélectionnées en raison de leur popularité auprès des jeunes (476 personnes ont été contactées via Facebook Messenger et 46 via WhatsApp). Africa's Voices Foundation estimait que l'utilisation de groupes WhatsApp encourageait les conversations qui produiraient des informations particulièrement utiles. Le responsable Impact et Communications, Rainbow Wilcox, a déclaré : « Les données qu'il est possible de collecter [via WhatsApp] sont riches, authentiques et apportent un éclairage sur les croyances et les comportements socioculturels ».

La fondation craignait toutefois que l'utilisation de Facebook Messenger et de WhatsApp porte atteinte à la vie privée. « Nous avons sollicité un consentement éclairé et stocké les données de façon sécurisée, mais il nous est impossible de contrôler l'utilisation des données sur ces plateformes », a déclaré Claudia Abreu Lopes, Directrice de la Recherche et de l'Innovation. « C'était problématique parce que nous demandions des informations personnelles comme le vote et les données démographiques. Nous avons décidé de ne pas renouveler cette expérience si les risques pour la vie privée ne sont pas bien mesurés au préalable ».

Comme il est suggéré plus haut, il est recommandé que les organisations humanitaires envisagent également de se doter de politiques prévoyant la suppression régulière des conversations après extraction des données nécessaires.

11.7 LIMITATION DE(S) LA FINALITÉ(S) ET TRAITEMENT ULTÉRIEUR

Le plus souvent, les données recueillies via des applications mobiles de messagerie seront extraites et analysées par des organisations humanitaires sur d'autres plateformes. Dans le cadre de leurs politiques de protection des données à communiquer aux personnes concernées, les organisations humanitaires doivent aussi indiquer clairement les finalités du traitement.

²²⁶ Africa's Voices, Case Study: Livity South Africa : https://issuu.com/africasvoices/docs/africa_s_voices_report_for_livity_a.

Cela peut être particulièrement difficile compte tenu de la souplesse d'utilisation et de l'immédiateté des communications qui caractérisent ces solutions, car il est probable qu'une personne concernée soulèvera plusieurs questions au cours d'une conversation, chaque question nécessitant une ou plusieurs actions de suivi. Compte tenu de ce qui précède et de la compatibilité des finalités humanitaires, une finalité générale d'assistance et de protection humanitaire devrait être suffisante.

Là encore, comme le traitement par applications mobiles de messagerie échappe au contrôle des organisations humanitaires, celles-ci doivent également mentionner, dans leur politique de protection des données, que conformément à cette politique, ces applications peuvent traiter des données pour d'autres finalités.

11.8 GESTION, ANALYSE ET VÉRIFICATION DES DONNÉES

Il est difficile d'exploiter les données traitées par des applications mobiles de messagerie dans l'action humanitaire. Un plus grand nombre de personnes peut désormais collecter et partager de plus gros volumes de données avec les organisations, mais il en résulte que celles-ci doivent s'assurer qu'elles peuvent gérer, analyser et vérifier les données collectées.

La création d'un flux de travail pour gérer et analyser les informations reçues peut poser des difficultés. Il n'y a pas d'interopérabilité entre les systèmes utilisés par les applications mobiles de messagerie et les systèmes de gestion des informations ou bases de données existantes ; pour les organisations humanitaires, la transcription manuelle de messages dans des tableurs est souvent le seul moyen d'analyser les données pour une prise de décision efficace.

La vérification des informations reçues par des applications mobiles de messagerie pose également des difficultés. Ce problème se pose dans de nombreux circuits de communication en ligne²²⁷, mais pour les applications mobiles de messagerie, la vérification est compliquée par la vitesse à laquelle les informations peuvent être envoyées, ainsi que par le volume des messages et les types de données qui peuvent être envoyés. Les médias d'information et les défenseurs des droits humains ont tenté de surmonter ces défis en travaillant ensemble pour produire des ressources

²²⁷ The Engine Room, « Verification of social media: The case of UNHCR on Twitter » : <https://responsibledata.io/reflection-stories/social-media-verification/>.

et des lignes directrices sur cette question, dont certaines peuvent être utiles aux organisations humanitaires²²⁸.

Les organisations humanitaires effectuent un traitement ultérieur lorsque les données personnelles collectées via des applications mobiles de messagerie sont gérées, analysées et vérifiées. Par conséquent, elles doivent s'assurer que les opérations de traitement ultérieur des données personnelles sont compatibles avec les finalités initiales de la collecte.

11.9 PROTECTION DES DONNÉES DÈS LA CONCEPTION

Si les organisations humanitaires ont l'intention de développer une application mobile de messagerie, elles doivent envisager de mettre en œuvre le principe de protection des données dès la conception, qui exige de développer des systèmes et des services respectueux de la vie privée, tant pour les solutions techniques que pour les mesures organisationnelles. Une AIPD permet une mise en œuvre concrète de ce principe. L'architecture client-serveur utilisée pour stocker des données doit aussi respecter le principe de protection des données dès la conception.

Lorsqu'elle décide de développer sa propre plateforme ou application, une organisation humanitaire doit prendre en compte certains éléments. Tout d'abord, la promotion de l'utilisation de l'application auprès des bénéficiaires de l'organisation s'annonce complexe. Ensuite, les opérations de maintenance et de sécurité de l'application engendrent des coûts récurrents, car après la conception, tous les logiciels doivent être régulièrement mis à jour en raison de l'émergence de nouvelles vulnérabilités. Une organisation humanitaire devra alors évaluer si elle dispose des capacités et de l'expertise en interne pour développer et maintenir une application ou plateforme de ce type²²⁹.

228 Voir, par exemple, Craig Silverman (éd.), *Guide de vérification*, Centre européen de journalisme : http://verificationhandbook.com/book_fr/; The Engine Room, Benetech et Amnesty International, *DatNav: New Guide to navigate and integrate digital data in human rights research*, 2016 : <https://www.theengineroom.org/datnav-digital-data-in-human-rights-research/>; Réseau de partenaires de First Draft News : https://fr.firstdraftnews.org/?_ga=2.111650308.1280992218.1593244700-895816878.1593244700.

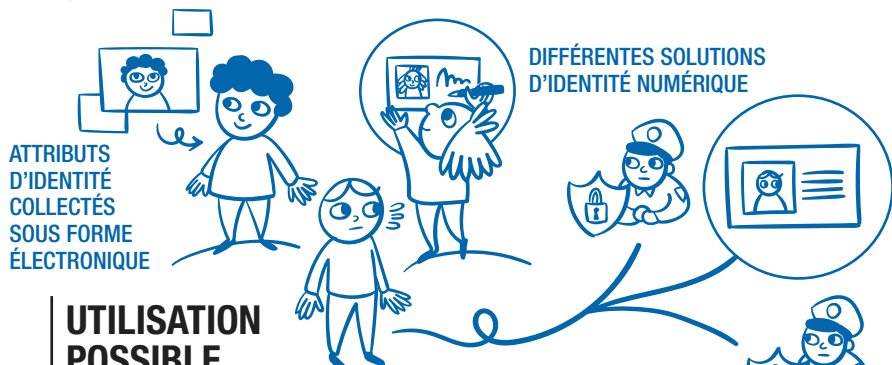
229 CICR et Privacy International, Section 5.4: Outsourcing, contracting, and using third parties, dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018.

11.10 TRANSFERT INTERNATIONAL DE DONNÉES

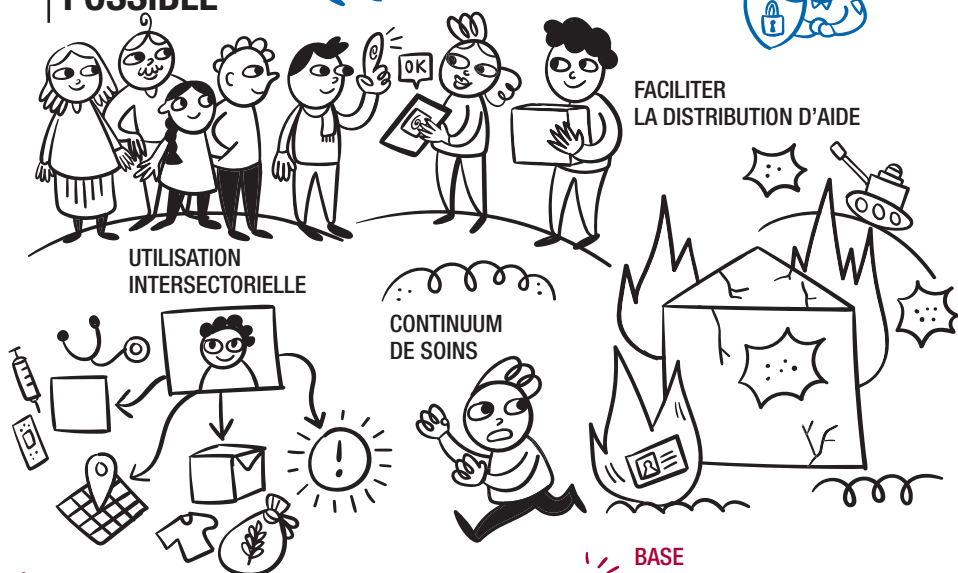
Il est également important de savoir que certains services convergent et peuvent se chevaucher du point de vue des entités intervenant et des modes de fonctionnement utilisés. En pratique, cela signifie que les activités de traitement des données des réseaux sociaux et des applications de messagerie ne doivent ni ne peuvent être considérées comme deux activités distinctes. Les applications de messagerie sont souvent liées aux réseaux sociaux de manière directe (par exemple, Facebook Messenger) ou indirecte, lorsqu'elles appartiennent au même groupe d'entreprises (par exemple, Facebook détient WhatsApp). Les services peuvent alors partager des données pour diverses finalités²³⁰.

230 CICR et Privacy International, Section 4.1: Messaging apps and social media, dans *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, octobre 2018.

IDENTITÉ NUMÉRIQUE



UTILISATION POSSIBLE



DÉFIS



CHAPITRE 12

IDENTITÉ NUMÉRIQUE²³¹

²³¹ Les auteurs souhaitent remercier Aiden Slaven (ID2020), Giulio Coppi (Norwegian Refugee Council) et Robert Riemann (Contrôleur européen de la protection des données) pour leur aide à la rédaction de ce chapitre.

12.1 INTRODUCTION

Chaque être humain a une identité. Le droit à l'identité est incontestable et il est reconnu dans les déclarations et conventions internationales²³². Toutefois, tous les êtres humains ne disposent pas de moyens pour prouver leur identité. S'il est vrai que tout individu devrait être en mesure de prouver qui il est grâce à un outil d'identité²³³, la question de la forme d'un tel outil est sujette à controverse. Il n'en demeure pas moins que, quelle que soit sa forme – document, carte, jeton, application mobile ou autre –, cet outil doit être produit et géré. Les mandats des organisations internationales encadrent leur action, notamment sur les questions d'identité numérique, comme nous le verrons dans ce chapitre.

Dans la plupart des cas, les organisations humanitaires doivent utiliser des systèmes de gestion de l'identité pour atteindre les objectifs d'un programme (par exemple un système de gestion des bénéficiaires conçu pour assurer la fourniture d'une aide aux individus ciblés)²³⁴. Certaines organisations ont participé à des initiatives visant à développer des systèmes de gestion de l'identité qui vont au-delà des simples objectifs d'un programme et qui, en pratique, fournissent une identité juridique²³⁵ (parfois sous forme numérique) à ceux qui n'ont pas de document d'identité et qui risquent dès lors de devenir « invisibles, sous-estimés et laissés pour compte²³⁶ ». Cependant, un outil d'identité conçu et déployé à l'origine pour atteindre les objectifs d'un programme peut parfois évoluer vers une utilisation plus large (par exemple pour prouver l'identité juridique d'une personne).

²³² Voir, par exemple : Déclaration universelle des droits de l'homme, Article 6, et Convention relative aux droits de l'enfant des Nations Unies, Article 7.

²³³ Voir Objectifs de développement durable, Objectif 16.9 : « D'ici à 2030, garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances » : <https://www.un.org/sustainabledevelopment/fr/peace-justice/>.

²³⁴ USAID, *Identity in a Digital Age: Infrastructure for Inclusive Development*, 2017, p. 1 : https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf.

²³⁵ Tout au long de ce chapitre, le terme « identité juridique » se base sur la définition opérationnelle des Nations Unies : « L'identité juridique s'entend des caractéristiques fondamentales de l'identité d'une personne (nom, sexe, lieu et date de naissance, par exemple) conférée après sa naissance à partir de l'enregistrement et de la délivrance d'un certificat par une autorité habilitée de l'état civil. En l'absence d'enregistrement des naissances, l'identité juridique peut être conférée par une autorité d'identification légalement reconnue. Ce système devrait être relié au système de l'état civil dans le cadre d'une approche intégrée de l'identité juridique de la naissance à la mort. L'identité juridique est retirée par la délivrance d'un certificat de décès par l'autorité de l'état civil lors de l'enregistrement du décès. Pour ce qui est des réfugiés, il incombe au premier chef aux États membres de leur délivrer la preuve de leur identité juridique. La délivrance d'une preuve de l'identité juridique aux réfugiés peut également être gérée par une autorité internationalement reconnue et habilitée. » Programme des Nations Unies pour l'identité juridique : <https://unstats.un.org/legal-identity-agenda/>.

²³⁶ USAID, 2017, p. 1.

Ce chapitre analyse les implications que la mise en place d'un système de gestion de l'identité numérique des bénéficiaires a en termes de protection des données. L'analyse couvre, entre autres, les modalités de collecte et de stockage des données par les organisations humanitaires dans un système de ce type et la manière dont ces organisations gèrent les informations sur les participants, utilisateurs et bénéficiaires.

Avant tout, il convient de souligner qu'il n'existe aucune définition universelle du terme « identité numérique », bien que l'on convienne généralement qu'elle désigne « un ensemble d'attributs d'identité collectés et stockés sous forme électronique qui décrit de manière unique une personne dans un contexte donné et est utilisé lors de transactions électroniques²³⁷ ». L'identité numérique est toutefois un concept pourvu de multiples facettes, ce qui signifie qu'elle est liée à plusieurs autres notions essentielles telles que l'identification, l'identité fonctionnelle, l'identité fondamentale et l'identité personnelle²³⁸. Puisque ces termes sont utilisés tout au long de ce chapitre, le tableau ci-dessous donne une explication simplifiée de chacun d'eux.

Terme	Objectifs	Caractéristiques typiques	Cas pratique
Identité fonctionnelle	Permet à un service spécifique (fonction) d'authentifier les participants.	Contextuelle, reproduction des informations.	Chaque individu peut avoir plusieurs identités fonctionnelles pouvant être transnationales, comme un numéro d'étudiant, un numéro d'électeur ou un numéro associé à un programme de distribution alimentaire.
Identité fondamentale (identité juridique)	Fournit une identité juridique à une vaste population en tant que bien public, sans être liée à un service spécifique. Elle permet aux individus de prouver qui ils sont. L'organisme qui délivre cette identité est considéré comme une source fiable d'identité, parfois désignée comme source d'identité faisant autorité.	Génère une identité juridique qui peut être reprise par d'autres entités. Dans son champ d'application, chaque personne ne peut avoir qu'une seule identité de ce type. Cependant, la même personne peut avoir plusieurs identités juridiques (par exemple, si plusieurs passeports sont délivrés par différents pays).	Généralement délivrée par le gouvernement pour l'ensemble de la population d'un pays ²³⁹ , par exemple, un numéro de sécurité sociale, un certificat de naissance ou un numéro Aadhaar (en Inde, numéro à 16 chiffres qui permet d'identifier de manière unique les habitants en fonction de leurs données biométriques et démographiques).

²³⁷ Groupe de la Banque mondiale, GSMA et Secure Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, 2016, p. 11: <https://www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation/>.

²³⁸ J. Donner, « The difference between digital identity, identification, and ID: Caribou Digital's style guide for talking about identity in a digital age », 19 décembre 2018 : <https://medium.com/caribou-digitalthe-difference-between-digital-identity-identification-and-id-41580bbb7563>.

²³⁹ USAID, 2017, p. 12.

Terme	Objectifs	Caractéristiques typiques	Cas pratique
Identité conceptuelle (identité personnelle) ²⁴⁰	Définit l'identité d'un individu par rapport aux autres au sein d'une structure sociale donnée, tout en déterminant la manière dont il se voit et celle dont il est perçu par la société dans laquelle il se trouve.	Intangible, variable et fortement définie par la perception personnelle et sociale.	Définit les attributs (tels que l'origine ethnique, la sexualité, la religion ou l'orientation politique) selon la manière dont les individus se définissent eux-mêmes et celle dont les autres les définissent au sein de leur société.

Au vu de ces différents types d'identité, il est important que les organisations humanitaires précisent d'emblée si elles souhaitent obtenir l'identité fonctionnelle ou fondamentale des bénéficiaires, car ce choix affecte la conception du système d'identité et les processus de gestion associés (par exemple, collaboration avec un tiers ou liens vers d'autres systèmes existants). Les restrictions juridiques orienteront souvent les décisions relatives à la conception du système d'identité.

12.1.1 AUTHENTIFICATION, IDENTIFICATION ET VÉRIFICATION : QUI ÊTES-VOUS ET COMMENT POUVEZ-VOUS LE PROUVER ?

Les organisations humanitaires n'ont pas toujours besoin de connaître l'identité juridique d'une personne. Par exemple, c'est le cas lorsque la finalité de l'interaction est d'apporter de l'aide. Par conséquent, avant de développer un système d'identité numérique, les organisations humanitaires doivent déterminer quelles informations elles souhaitent recueillir auprès des bénéficiaires pour un programme humanitaire spécifique. Dès lors, il est important de bien faire la différence entre authentification, identification et vérification.

L'identification répond à la question suivante : « Qui êtes-vous ? » Cependant, lors de la mise en place d'un système de gestion de l'identité, les organisations doivent d'abord se poser cette question : « Que dois-je savoir sur cette personne pour pouvoir lui apporter une aide ou une protection ? » Dans certains cas, savoir qui est la personne peut néanmoins être important. Par exemple, lorsque des mineurs non accompagnés sont réunis avec leurs parents, il est essentiel de vérifier que les parents en question sont bien ceux qu'ils prétendent être. Mais souvent, si ce n'est dans la plupart des cas, il est suffisant de savoir que la personne satisfait à certains critères ou possède un ensemble d'attributs spécifiques pour pouvoir bénéficier d'un service (par exemple, elle peut prouver qu'elle a moins de 12 ans pour se faire vacciner). On appelle aussi cette démarche authentification : être en mesure de prouver que nous sommes ceux que nous prétendons être.

²⁴⁰ Ce chapitre ne traitera pas de l'identité conceptuelle, celle-ci ne pouvant pas être incluse dans un système d'identité.

Même lorsque seule l'authentification est nécessaire, il incombe aux organisations humanitaires de mettre en place un processus de vérification lors de l'enregistrement des bénéficiaires dans le système de gestion de l'identité. La vérification désigne donc l'action qui consiste à vérifier l'identification d'une personne (comme confirmer le nom d'une personne sur son document d'identité) ou certains de ses attributs d'identité (comme vérifier auprès du chef communautaire que la personne est bien membre de la communauté bénéficiaire de l'aide). Lors de l'utilisation d'un système d'authentification simple pour assurer la fourniture de l'aide aux personnes concernées, il peut être utile de s'assurer, au moment de l'enregistrement, que les personnes devant recevoir l'aide sont bien celles qui ont été enregistrées. Il convient toutefois de souligner que la vérification est inutile pour certains services d'aide, par exemple lorsqu'une organisation humanitaire rend des informations disponibles sur une plateforme en ligne où tout le monde peut s'enregistrer.

Lorsque les organisations humanitaires inscrivent et enregistrent des bénéficiaires, certaines données les concernant devront être recueillies et stockées dans le système de gestion de l'identité. Comme on le verra ci-après, le choix des attributs à enregistrer et pour quelle(s) finalité(s) est une décision clé du point de vue de la protection des données. En effet, seuls les attributs nécessaires aux fins de l'activité (par exemple garantir la fourniture d'une aide) doivent être collectés. Ainsi, une organisation n'aura la plupart du temps pas besoin d'enregistrer une copie d'un document d'identité pour attester qu'une personne enregistrée est bien mineure. Une fois enregistré, le bénéficiaire peut recevoir un document établissant son identité (attestation, carte, code pin ou certificat numérique) qu'il peut gérer et auquel il peut accéder sur un appareil mobile. Une vérification supplémentaire n'est alors pas nécessaire au moment de la fourniture de l'aide, puisque le bénéficiaire dispose déjà d'une preuve qu'il a droit au service en question.

12.1.2 IDENTITÉ NUMÉRIQUE

L'identité numérique est un ensemble d'attributs stockés sous forme électronique qui décrit de manière unique une personne dans un contexte donné (voir les différents types d'identité décrits précédemment : identité fonctionnelle, fondamentale et conceptuelle). Dans certains cas, les individus peuvent avoir plus d'une identité numérique (potentiellement des centaines), correspondant chacune à une identité fonctionnelle. Ce type de système permettrait aux bénéficiaires d'avoir accès à des services, à une assistance ou à une protection sans qu'ils n'aient à démontrer leur identité juridique, de la même manière qu'un modèle d'accès avec nom d'utilisateur et mot de passe ou qu'un système de jetons.

Il arrive également que les organisations doivent être en mesure de différencier des individus avec un haut degré de certitude, et qu'elles ne disposent que d'une identité numérique pour chaque personne. Dans ces scénarios, le système d'identité leur permettrait de relier une identité numérique à une personne physique, l'objectif étant de faciliter la différenciation entre les individus, par exemple, lorsque l'organisation apporte une aide personnalisée (comme des soins

de santé). Pourtant, même lorsqu'un lien de ce type est nécessaire, l'organisation n'a pas forcément besoin d'obtenir des documents attestant l'identité juridique des bénéficiaires. Ainsi, le nom des individus pourrait suffire pour s'enregistrer, sans qu'il soit nécessaire de confirmer que le nom donné correspond bien à celui de l'identité juridique (par exemple via une vérification du certificat de naissance ou autre document d'identité).

Enfin, il peut arriver que les organisations humanitaires aient besoin d'un système qui leur permette aussi d'établir et de vérifier l'identité juridique des individus. Cette situation est très similaire au cas précédent, si ce n'est qu'un document attestant l'identité juridique sera requis pour identifier formellement la personne en question.

En résumé, lors de la mise en place d'un système de gestion de l'identité numérique, les organisations internationales devraient suivre les étapes suivantes :

- Tout d'abord, l'organisation détermine quelles informations elle doit connaître au sujet des personnes concernées pour mettre en œuvre un programme humanitaire spécifique. Ce choix déterminera si une identification est nécessaire ou si une authentification seule suffit. Du point de vue de la protection des données, la dernière option doit être privilégiée autant que possible.
- Ensuite, l'organisation détermine si une identité fonctionnelle ou fondamentale est nécessaire en fonction des besoins du programme, tout en gardant à l'esprit que seule une poignée d'organisations humanitaires disposent d'un mandat pour établir ou gérer des identités fondamentales, et ce, uniquement à des fins spécifiques.
- Enfin, l'organisation élabore un processus de vérification pour contrôler les informations fournies au moment de l'inscription. Selon le système d'identité choisi, ce processus peut n'impliquer aucune formalité spécifique, intégrer certaines vérifications ou nécessiter un document juridique faisant autorité. Il incombe également à l'organisation de déterminer si elle doit conserver ou non les informations examinées lors de la phase de vérification.

12.1.3 CONCEPTION ET GOUVERNANCE DU SYSTÈME

Une fois que les objectifs sont clairs pour l'organisation humanitaire (authentification, identification et vérification), celle-ci doit décider comment devra être conçu le système d'identité numérique pour atteindre les finalités prévues, et qui en assurera la gouvernance. L'organisation (ou autre organisme) peut contrôler le système de manière centralisée, ou décentralisée en partageant le contrôle entre plusieurs parties²⁴¹. Certaines initiatives actuelles visent à permettre

²⁴¹ La différence entre une architecture décentralisée et distribuée et un système d'identité fédéré est détaillée dans les ouvrages de référence. Même s'il s'agit d'un point important, il dépasse la portée de ce chapitre et ne sera donc pas abordé ici. Pour une description détaillée de l'identité décentralisée, voir : Digital Identity Foundation (<https://identity.foundation/>), World Wide Web Consortium (<https://w3c-ccg.github.io/did-spec/>) et Forum économique mondial (http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf).

aux individus de contrôler leurs propres systèmes d'identité en déterminant qui peut accéder à leurs informations d'identité et à quel moment. En ce sens, la structure de gouvernance est parfois influencée par le lieu où sont hébergées les données. Par exemple, lorsque plusieurs parties accèdent au même système, une plateforme partagée est nécessaire. De la même façon, lorsque des efforts sont déployés pour donner le contrôle aux individus, il est possible de les autoriser à stocker leurs informations sur leurs propres appareils ou à utiliser un fournisseur de services de leur choix.

L'arbre de décision suivant résume les questions auxquelles devraient répondre les organisations humanitaires et les facteurs qu'elles devraient prendre en compte lorsqu'elles évaluent la possibilité de mettre en œuvre d'un système d'identité :

1. Type de système d'identité

- L'authentification est-elle suffisante ou avez-vous besoin d'identifier réellement les bénéficiaires ?
- Comptez-vous générer des identités fonctionnelles ou fondamentales ? N'oubliez pas : seules certaines organisations disposent d'un mandat pour générer des identités fondamentales.
- Avez-vous besoin de vérifier les informations fournies lors de l'inscription ? Si non, un système sans vérification est-il acceptable ? Si oui, la vérification requiert-elle un document formel attestant l'identité juridique, ou une forme plus simple de vérification est-elle acceptable ? Avez-vous besoin de conserver les informations examinées lors du processus de vérification ?

2. Conception

- Quelles informations doivent être stockées ? Par qui ? Et où ?
- À noter que la vérification d'un attribut spécifique (comme la nationalité, pour déterminer si la personne peut être incluse dans un programme humanitaire) ne signifie pas que cette information doit être stockée dans le système d'identité. Le système peut simplement confirmer que la personne dispose de l'attribut en question, sans détails supplémentaires.
- Dans certains cas, la vérification peut même être inutile. Par exemple, c'est le cas d'un service numérique largement accessible pour lequel il est possible de créer librement un compte sans divulguer aucune information personnelle, ou lorsque la simple présence d'un individu dans un lieu où se trouvent des personnes déplacées lui donne le droit d'accéder à l'aide (par exemple lorsque des cartes sont distribuées sans que des informations soient collectées).
- De quelle manière les données seront-elles contrôlées et gérées ? Qui a besoin d'accéder aux informations, à quel moment et pour quelles finalités ?

12.1.4 IDENTITÉ NUMÉRIQUE DANS LE SECTEUR HUMANITAIRE : SCÉNARIOS POSSIBLES

Les quatre scénarios suivants mettent en lumière les interactions entre différents systèmes d'identité numérique dans le secteur humanitaire.

Scénario 1 – Une organisation humanitaire délivre un justificatif d'identité (par exemple, une carte ou un document d'enregistrement) au bénéficiaire enregistré pour l'aide. Dans ce scénario, le bénéficiaire (une personne concernée, au sens du glossaire figurant au début du présent ouvrage) utilise une identité fonctionnelle, qui lui permet de recevoir l'aide. Dans certaines situations, un système d'identification de ce type pourrait toutefois être accepté comme preuve de l'identité du bénéficiaire ; autrement dit, il pourrait faire office d'identité fondamentale (voir scénario 4). Cela dit, dans le cadre de certains programmes humanitaires, l'authentification des individus suffit pour prouver qu'ils sont en droit d'accéder légitimement à certains services d'aide ; l'identification n'est alors pas nécessaire.

Scénario 2 – Une organisation humanitaire offre plusieurs services aux bénéficiaires. En vue de fournir ces services, chaque unité de l'organisation doit pouvoir accéder à une partie des données collectées auprès des bénéficiaires. Par exemple, pour fournir une aide en nature, une unité peut avoir besoin d'accéder à l'historique de l'aide déjà reçue par le bénéficiaire. En revanche, une autre unité peut avoir besoin d'accéder au dossier médical de la personne pour lui offrir des soins de suivi, et une troisième unité peut, quant à elle, avoir besoin de connaître certaines informations sur l'individu pour l'aider à rétablir le contact avec sa famille.

Scénario 3 – Plusieurs organisations humanitaires offrent de multiples services aux bénéficiaires via un système d'identité unifié. Dans le cadre d'une solution partagée de ce type, chaque organisation peut accéder aux données dans la mesure où celles-ci sont nécessaires et pertinentes pour la prestation de ses services. Ce scénario nécessite donc de procéder à l'authentification et l'identification des individus. L'interopérabilité entre les différents organismes et organisations impliqués peut s'avérer bénéfique, le système servant de portail unique pour l'aide humanitaire. Il s'agirait alors d'appliquer le principe « une fois pour toutes²⁴² » dans l'action humanitaire pour faciliter la prestation de services physiques ou numériques directement aux bénéficiaires par le biais de plateformes en ligne ou à travers l'échange d'informations ou de documents (automatiquement ou

²⁴² Le principe « une fois pour toutes » implique que les individus ne fournissent leurs informations personnelles aux autorités qu'une seule fois, après quoi les ministères peuvent échanger ces informations, sur demande ou avec le consentement des personnes concernées, aux fins d'exercer leurs missions d'intérêt public, évitant ainsi de devoir les collecter à nouveau.

sur demande) entre différentes organisations humanitaires²⁴³. Les organisations devront néanmoins tenir compte de divers facteurs en optant pour ces solutions. Par exemple, elles doivent identifier le cadre de gouvernance applicable et veiller à définir précisément les rôles des parties associées au système (responsables du traitement et sous-traitants). Cela dit, puisqu'une ségrégation adéquate de l'accès aux données peut être complexe d'un point de vue technique, il n'est pas rare que des violations de données se produisent dans le cadre des solutions commerciales unifiées. De même, en raison des relations complexes qui existent entre les organisations, il peut être difficile dans un système unifié de s'assurer que les données sont utilisées uniquement aux fins pour lesquelles elles ont été collectées. De plus, des systèmes complexes de ce type peuvent de fait conduire à l'exclusion de certains groupes qui ne disposent pas forcément des compétences numériques nécessaires à l'utilisation de ces outils.

Scénario 4 – Dans certains contextes, les organisations humanitaires peuvent délivrer des documents d'identité fonctionnelle aux bénéficiaires, tels que des cartes d'enregistrement, qui permettent aux personnes concernées d'accéder aux services. Ces documents peuvent finalement servir d'identité fondamentale pour les autorités ou les établissements financiers qui les acceptent comme preuve d'identité.

EXEMPLE :

En Jordanie et en Égypte, deux pays qui accueillent un grand nombre de réfugiés, les autorités locales exigent un passeport valide ou une pièce d'identification délivrée par le gouvernement (comme une carte de service du ministère de l'Intérieur jordanien pour les réfugiés et les demandeurs d'asile) afin de satisfaire aux exigences d'enregistrement des cartes SIM et de connaissance des clients (KYC – *Know Your Customer*). Le Haut Commissariat des Nations Unies pour les réfugiés soutient que ses propres documents d'identification devraient également être acceptés, car ils sont parfois les seules formes d'identification dont disposent les demandeurs d'asile et les réfugiés.

12.1.5 IDENTITÉ NUMÉRIQUE EN TANT QU'IDENTITÉ FONDAMENTALE

De nombreuses initiatives visent aujourd'hui à développer des systèmes d'identité numérique qui servent d'identité fondamentale aux personnes qui ne disposent d'aucun document d'identité.

²⁴³ Voir : Contrôleur européen de la protection des données (CEPD), Avis n° 8/2017 – Avis du CEPD sur la proposition de règlement établissant un portail numérique unique et sur le principe « une fois pour toutes », 1^{er} août 2017 : https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_fr.pdf.

Ces initiatives s'inspirent du fait que les personnes qui ne peuvent prouver leur identité rencontrent des difficultés pour faire valoir leurs droits, accéder à des services publics et revendiquer des prestations ou des aides sur la base de leur âge, de leur nationalité, des circonstances ou de tout autre attribut d'identité ou de statut²⁴⁴. Par ailleurs, la preuve d'identité étant désormais un prérequis pour accéder à de nombreux services, l'absence d'identité est un obstacle majeur à la participation à la vie politique, sociale et économique. Par exemple, les fournisseurs de services privés exigent souvent une preuve d'identité pour satisfaire aux exigences juridiques en vigueur ou dans le cadre de leurs processus de diligence raisonnable (connaissance du client, lutte contre les fraudes et l'usurpation d'identité, et réduction des risques et coûts de transaction, notamment). Les systèmes d'identité numérique pourraient être un moyen d'aider les personnes dans le besoin qui n'ont pas de document d'identité. Toutefois, comme mentionné plus haut, très peu d'organisations humanitaires disposent du mandat nécessaire, et donc d'une base légitime, pour développer et déployer des systèmes de ce type.

Il est important de préciser que les programmes d'identité numérique ne se limitent pas à certaines technologies ou à certains systèmes spécifiques. Ils peuvent être élaborés à l'aide de plusieurs technologies ou d'une combinaison de solutions. Les technologies fréquemment associées à l'identité numérique sont notamment les suivantes :

- **Biométrie**²⁴⁵ : l'inscription de bénéficiaires dans des programmes d'identité numérique dans le secteur humanitaire peut comprendre l'utilisation de données biométriques, telles que les empreintes digitales ou les scans de l'iris.
- **Blockchain**²⁴⁶ : une blockchain est une solution possible pour permettre aux individus qui ont un accès limité aux technologies et infrastructures numériques de démontrer leur identité²⁴⁷. Malgré son potentiel prometteur, il faut toutefois tenir dûment compte des défis posés par la technologie des blockchains.
- **Analyse de données**²⁴⁸ : il est possible de créer des identités numériques à partir d'attributs comportementaux numériques (processus également appelé identification algorithmique) sans utiliser d'identifiants officiels. L'activité en ligne d'une personne (utilisation des médias sociaux, historique de navigation, achats en ligne, historique des appels, etc.) pourrait être utilisée pour vérifier

²⁴⁴ G. Verdirame et al., *Rights in Exile: Janus-Faced Humanitarianism*, Berghahn Books, New York, 2005, p. 59–63 : <https://www.berghahnbooks.com/title/VerdirameRights>.

²⁴⁵ Voir [chapitre 8 : Biométrie](#).

²⁴⁶ Voir [chapitre 14 : Blockchain](#).

²⁴⁷ A. Beduschi et al., *Building Digital Identities: The challenges, risks and opportunities of collecting behavioural attributes for new digital identity systems*, University of Exeter et Coalition, 2017, p. 15–16, p. 26 : https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Buiding_Digital_Identities_with_Behavioural_Attributes.pdf.

²⁴⁸ Voir [chapitre 6 : Analyse de données et big data pour les problématiques relatives au recours à l'analyse de données](#).

son identité²⁴⁹. Bien que le potentiel des systèmes d'identité basés sur le profil de la personne ne soit pas encore pleinement exploité, cette approche n'en suscite pas moins des préoccupations en termes de protection des données²⁵⁰.

12.2 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

Une AIPD vise à identifier, évaluer et gérer l'impact qu'aura sur les personnes concernées et leurs données personnelles un projet, une politique, un programme ou une autre initiative impliquant le traitement de ces données. Elle doit permettre d'identifier les mesures à prendre afin de minimiser les risques pour les droits et libertés des individus et doit être effectuée tout au long du cycle de vie d'un projet ou d'une initiative. Compte tenu des grandes quantités de données qui sont traitées par les systèmes d'identité numérique, et des risques et préjudices pouvant en résulter pour les personnes concernées, les organisations humanitaires devraient effectuer une AIPD avant et pendant la mise en œuvre du système et du programme. En outre, le processus d'AIPD devrait analyser non seulement la conformité aux exigences de protection des données, mais également les répercussions potentiellement néfastes du système sur divers droits fondamentaux, ainsi que les conséquences éthiques et sociales du traitement des données²⁵¹.

L'utilisation de systèmes d'identité pour diverses finalités humanitaires, dont certaines ne sont pas toujours définies d'emblée, comporte le risque d'un détournement d'usage. C'est le cas lorsque les organisations humanitaires font un usage abusif des données des bénéficiaires, volontairement ou non, en utilisant les systèmes d'identité à des fins autres que celles initialement prévues. Par ailleurs, des gouvernements et des groupes armés non étatiques peu respectueux des droits humains pourraient accéder à ces systèmes ainsi qu'à d'autres pour identifier des ennemis ou des opposants, ou pour cibler ou dresser le profil de certains groupes en fonction de leur origine ethnique, leur opinion politique, leur nationalité ou d'autres caractéristiques. Ils pourraient ensuite utiliser ces informations pour contrôler et discriminer ces individus ou groupes et leur nuire de différentes manières ; par exemple, ils pourraient les empêcher d'avoir accès à des aides et services essentiels, les priver de liberté et du droit à un procès équitable, ou même leur faire subir des atrocités (comme le génocide rwandais et les persécutions perpétrées par l'Allemagne nazie, où l'identification et le profilage ont joué un rôle essentiel).

²⁴⁹ A. Beduschi *et al.*, 2017, p. 8.

²⁵⁰ Par exemple, les comptes fantômes de Facebook. Voir : R. Brandom, « Shadow profiles are the biggest flaw in Facebook's privacy defense », 11 avril 2018 : <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy>.

²⁵¹ A. Mantelero, « AI and Big Data: A blueprint for a human rights, social and ethical impact assessment », *Computer Law & Security Review*, vol. 34, n° 4, août 2018, p. 754-772, p. 755 : <https://doi.org/10.1016/j.clsr.2018.05.017>.

12.3 PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT

La protection des données dès la conception et par défaut est une pratique qui doit être intégrée tout au long du cycle de vie des applications qui traitent des données personnelles²⁵². Elle consiste à concevoir une opération, un programme ou une solution de traitement de manière à intégrer d'emblée les principes clés de la protection des données et à offrir à la personne concernée la meilleure protection possible pour ses données. En ce sens, les principes clés de la protection des données sont :

- licéité, équité et transparence ;
- limitation de la finalité ;
- minimisation des données ;
- exactitude ;
- limitation du stockage (conservation limitée) ;
- intégrité et confidentialité (sécurité) ;
- responsabilité.

Lors de la conception d'un système d'identité, les organisations humanitaires devraient donc commencer par analyser leurs besoins, puis déterminer si un système d'identité est nécessaire et proportionné pour résoudre le problème identifié. Si une organisation estime qu'un système d'identité est nécessaire, elle devrait réfléchir attentivement au type de système qui répond au mieux à ses besoins et qui est le plus adapté aux circonstances spécifiques. Ce faisant, l'organisation pourra appliquer les principes de minimisation des données et de proportionnalité, comme expliqué à la section 12.6.

La protection des données dès la conception exige aussi que l'organisation élabore des systèmes de manière à ce que les personnes concernées puissent exercer plus facilement leurs droits (voir section 12.5). Par exemple, dans un système d'identité numérique, les personnes concernées devraient, par défaut, avoir accès aux notes d'information, à toutes les informations relatives à leur identité et au registre indiquant qui a accédé à leurs données et à quelles fins.

²⁵² L. Jasmontaite *et al.*, « Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR », *European Data Protection Law Review*, vol. 4, n° 2, 2018 : <https://edpl.lexxion.eu/article/EDPL/2018/2/0>.

12.4 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Les systèmes d'identité numérique peuvent impliquer divers organismes et entités, notamment des organisations humanitaires, des gouvernements et des entités commerciales, telles que des banques, des fournisseurs de systèmes de paiement, des fournisseurs de réseau et des sociétés spécialisées dans la biométrie. Il peut dès lors être complexe d'établir quelles parties doivent être considérées comme responsables du traitement et lesquelles doivent être considérées comme sous-traitants. De même, il peut être difficile de délimiter les obligations et responsabilités des parties. Pour contrer ce problème, un système d'identité numérique doit être conçu de manière à identifier clairement les parties prenantes, leurs responsabilités et obligations ainsi que les flux et catégories de données que chacune utilise et à quelles fins. Lorsqu'une organisation humanitaire détermine les modalités et les finalités d'un programme d'identification, elle agit en tant que responsable du traitement et est ainsi responsable de toute violation, de toute utilisation abusive et de tout autre préjudice pouvant résulter du programme. Si une responsabilité conjointe est établie ou si un sous-traitant traite des données personnelles uniquement pour le compte du responsable du traitement, il est de bonne pratique de définir les responsabilités des parties dans un accord écrit.

12.5 DROITS DES PERSONNES CONCERNÉES

Diverses initiatives se penchent actuellement sur la possibilité de développer des systèmes d'identité numérique contrôlés par les personnes concernées. L'objectif est de donner le contrôle aux individus pour leur permettre de stocker les données d'identité sur leurs propres appareils sans référentiel central et, au besoin, de fournir des identifiants à ceux qui doivent vérifier les données²⁵³. Comme nous l'avons évoqué plus haut, il faudrait pour cela élaborer un système dans lequel les bénéficiaires stockent leurs informations personnelles sur leurs propres appareils ou sur un autre support de stockage de leur choix, et dans lequel ils sont en mesure de décider à quel moment partager ces informations avec les organisations et organismes engagés dans l'action humanitaire. Certaines initiatives portant sur des systèmes d'identité fonctionnelle ou fondamentale visent elles aussi à donner le contrôle aux individus, là encore en leur permettant de stocker leurs données personnelles sur leurs appareils et de les partager avec d'autres entités lorsqu'ils le souhaitent. Quant à savoir si un transfert du contrôle aurait effectivement lieu dans la pratique, la question fait débat. Lors de la mise en œuvre de telles initiatives, il est important de veiller à ce que les individus connaissent leurs droits et les risques

253 M. Pisa and M. Juden, *Blockchain and Economic Development: Hype vs. Reality*, Center for Global Development, Washington, D.C., 2017, p. 25 : https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf.

liés au stockage de ces informations sur leurs appareils personnels, et qu'ils soient suffisamment équipés pour pouvoir utiliser ces outils de manière sécurisée.

EXEMPLE :

L'Alliance ID2020 a été fondée avec l'objectif d'influencer le développement d'identités numériques « responsables », en vertu desquelles les individus contrôlent entièrement leur identité et peuvent choisir quelles données partager et avec qui. Selon l'Alliance, « la plupart des données personnelles sont aujourd'hui stockées dans des silos. Plus vous stockez de données dans des silos, moins vous serez à même de les contrôler ». Pour résoudre ce problème, l'Alliance déclare que les individus « doivent garder le contrôle sur leurs propres identités numériques, y compris les modalités de collecte, d'utilisation et de partage des données personnelles²⁵⁴ ».

Bien que ces initiatives ne soient pas encore très fréquentes, les organisations humanitaires peuvent accorder plus de contrôle aux bénéficiaires et leur permettre d'accéder à leurs données au moyen d'identifiants ; ils pourront ainsi avoir accès à toutes les informations concernant leur identité et, le cas échéant, à leur profil personnel créé par l'organisation en question. Les avantages et risques potentiels associés à cette solution doivent encore être étudiés afin de déterminer si elle pourrait fonctionner en pratique et si elle donnerait véritablement le contrôle aux individus. En théorie, cependant, un système de ce type pourrait informer automatiquement les bénéficiaires si un tiers accédait à leurs données ou si une activité de traitement était lancée. Il permettrait aussi aux bénéficiaires de mettre à jour leur consentement, lorsque ce dernier constitue le fondement juridique du traitement, et de recevoir des informations à jour concernant le traitement. Grâce à davantage de contrôle, les bénéficiaires pourraient exercer directement leurs droits en tant que personnes concernées via un profil ou une plateforme en ligne. Par ailleurs, au cas où les bénéficiaires ne sauraient pas se servir des outils numériques, ou n'auraient pas accès à la technologie nécessaire, les organisations humanitaires doivent proposer une alternative pour leur permettre de faire valoir leurs droits sur leurs données personnelles.

12.5.1 DROIT D'ACCÈS

Les bénéficiaires sont en droit d'exiger l'accès aux informations relatives au traitement de leurs données et à leurs données en cours de traitement²⁵⁵. Bien que ce droit puisse être limité dans certaines circonstances, les organisations humanitaires, agissant en tant que responsables du traitement, doivent répondre à ces demandes en faisant savoir aux bénéficiaires si leurs données sont traitées et, le cas échéant,

²⁵⁴ Toutes les citations proviennent du site de l'organisation ID2020 : <https://id2020.org>.

²⁵⁵ Voir [section 2.11.2 : Droit d'accès](#).

en leur donnant accès aux données en question. En pratique, il peut toutefois être difficile de faire valoir ce droit dans le cadre de programmes d'identité numérique, en raison des difficultés qu'il y a souvent à vérifier que la personne ayant demandé l'accès aux informations est bien autorisée à les recevoir, en particulier lorsque la demande a été soumise sous forme électronique (scénario le plus probable lorsqu'il est question d'identité numérique). Si ce problème concerne de nombreux autres systèmes numériques, il est important d'en tenir compte dans le cas de l'identité numérique. Les organisations humanitaires devraient par conséquent prendre des mesures pour garantir le respect des droits des personnes concernées, et ce, avant de concevoir un système d'identité numérique et de décider de sa mise en œuvre éventuelle.

Un autre défi lié au respect des droits des personnes concernées dans le cadre des programmes d'identité numérique tient au fait que plusieurs unités au sein d'une même organisation peuvent détenir différents éléments d'information sur la personne concernée. Il peut par conséquent s'avérer compliqué de rassembler toutes ces informations pour répondre à une demande, voire inutile, car les bénéficiaires demandent souvent l'accès à une catégorie spécifique de données ou aux données relatives à un programme particulier, et non pas à l'ensemble des données les concernant détenues par l'organisation. Les organisations devraient donc en discuter avec les personnes concernées, de sorte à comprendre les spécificités de la demande et éviter ainsi tout effort superflu. Elles devraient tenir compte de cette problématique dans les réflexions qu'elles mènent au stade de la conception du système d'identité numérique afin de pouvoir anticiper les problèmes de ce type et trouver des moyens de les éviter. Un système d'accès par identifiant, tel que celui mentionné plus haut, permettrait aux bénéficiaires d'accéder à leur profil à tout moment, de vérifier quelles informations les concernant sont conservées et à quelles fins elles sont utilisées.

12.5.2 DROITS DE RECTIFICATION ET DE SUPPRESSION

Les bénéficiaires doivent pouvoir rectifier les données incorrectes les concernant et, dans certains cas, exiger la suppression de leurs données. Ils peuvent le faire directement, par exemple en se connectant à leur compte (comme envisagé ci-dessus). Lorsque les bénéficiaires ne contrôlent pas leurs données, l'exercice de leurs droits peut cependant s'avérer complexe, surtout lorsqu'il s'agit d'évaluer et de confirmer l'identité d'une personne qui demande la rectification ou la suppression de ses données. Pour résoudre ce problème, les organisations humanitaires doivent mettre en œuvre un système de vérification qui respecte le principe de minimisation et ne collecte pas de données personnelles inutiles. Là encore, la connexion des bénéficiaires à leur propre compte pourrait être une solution.

12.6 APPLICATION DES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

Bien que cette section donne une vue d'ensemble des préoccupations que peut susciter l'utilisation de systèmes d'identité numérique en termes de protection des données, chaque cas doit être examiné en détail et de manière individuelle, en tenant compte de la technologie utilisée et du type d'identification requis pour atteindre les objectifs du programme. Chaque programme aura des exigences différentes. De la même façon, chaque technologie aura des implications différentes en termes de protection des données.

12.6.1 FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

Les organisations humanitaires doivent traiter des données personnelles pour pouvoir établir ou vérifier l'identité d'un bénéficiaire. Ces opérations de traitement peuvent reposer sur un ou plusieurs fondements juridiques. Par exemple, dans les scénarios 2 et 3, une organisation humanitaire devra identifier un fondement juridique distinct pour chaque activité de traitement, comme l'intérêt vital pour le traitement de données médicales et le consentement pour le traitement de données personnelles à des fins de rétablissement des liens familiaux.

Pour ce qui est du consentement, il est important de reconnaître que les bénéficiaires ne sont parfois pas en position de le donner de manière valable²⁵⁶. Le consentement est une manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée donne son accord au traitement de données personnelles la concernant. De même, bien que les organisations humanitaires puissent invoquer l'intérêt public comme base juridique d'un programme fournissant des justificatifs d'identité officiels, l'impossibilité d'obtenir le consentement peut faire naître un sentiment de méfiance chez les bénéficiaires. Ces derniers peuvent penser que, puisqu'ils n'ont pas leur mot à dire sur le traitement de leurs données personnelles, leurs droits sont restreints. C'est particulièrement vrai lorsque les données en question concernent leur identité, qui fait partie intégrante de la vie d'une personne.

12.6.2 LIMITATION DE(S) LA FINALITÉ(S) ET TRAITEMENT ULTÉRIEUR

Les données personnelles doivent être collectées pour des finalités spécifiques, explicites et légitimes, et le traitement ultérieur ne doit être entrepris que lorsque celui-ci est compatible avec les finalités initiales²⁵⁷. À cet égard, il est important d'évaluer si les données personnelles collectées auprès d'une personne concernée en vue de lui fournir des justificatifs d'identité numérique dans le cadre d'un

²⁵⁶ Voir [section 3.2: Consentement](#).

²⁵⁷ Voir [chapitre 2: Principes fondamentaux de la protection des données](#).

programme humanitaire spécifique (par exemple dans le but d'établir l'identité des bénéficiaires) pourraient être traitées ultérieurement dans le cadre d'un autre programme (par exemple pour la fourniture d'une aide ou de services). Les organisations humanitaires devraient tenir compte des facteurs suivants lors de l'application du principe de limitation des finalités²⁵⁸ :

- la compatibilité entre les finalités initiales et ultérieures ;
- le contexte dans lequel les données sont collectées, notamment la relation entre l'individu et le responsable du traitement ;
- la nature des données ;
- les conséquences possibles pour les bénéficiaires ;
- l'existence de garanties appropriées (notamment de garanties en matière de sécurité des données, telles que le chiffrement ou la pseudonymisation).

Comme les systèmes d'identité numérique peuvent avoir plusieurs utilisations, chacune avec leur propre finalité, les organisations doivent préciser clairement toutes les finalités d'une opération de traitement donnée. En cas de modification ou de précision ultérieure de ces finalités, elles devront en informer les personnes concernées.

12.6.3 PROPORTIONNALITÉ

Le principe de proportionnalité exige l'utilisation des moyens de traitement les moins intrusifs pour atteindre les finalités prévues du traitement. Il est utile de rappeler que certaines activités humanitaires, telles que la fourniture d'aide, n'exigent parfois des bénéficiaires que la preuve qu'ils sont bien en droit d'en bénéficier (authentification), tandis que d'autres exigent une preuve de l'identité fondamentale ou « officielle » (vérification). C'est pourquoi les organisations humanitaires, agissant en tant que responsables du traitement, devraient déterminer quelles activités nécessitent une identification et lesquelles n'en ont pas besoin. En limitant le traitement à l'authentification des bénéficiaires en droit d'accéder aux services, les organisations pourraient éviter un traitement ultérieur des données, accidentel ou involontaire, ou la collecte d'informations inutiles, puisque les identités juridiques des bénéficiaires ne seraient pas collectées ni stockées par l'organisation. Lorsqu'une authentification ou identification est nécessaire, les organisations devraient par ailleurs tenir compte du volume et du type de données dont elles ont besoin. Par exemple, pour ce qui est des données biométriques, elles devraient traiter le moins de données possible (une empreinte digitale au lieu de dix).

²⁵⁸ CEPD, 2017, p. 11-12.

12.6.4 MINIMISATION DES DONNÉES

Les organisations humanitaires ne doivent collecter et traiter que la quantité minimale de données nécessaire pour atteindre l'objectif du traitement. Elles doivent donc être parfaitement au clair sur les informations dont elles ont vraiment besoin avant de mettre en œuvre un système d'identification traitant des données personnelles. Si une organisation estime qu'il est suffisant de démontrer son droit à recevoir une aide (authentification), elle n'a pas à collecter ou traiter d'informations d'identité de quelque manière que ce soit.

12.6.5 SÉCURITÉ DES DONNÉES

Les systèmes d'identité numérique, tels que celui envisagé dans le scénario 3, peuvent permettre aux bénéficiaires de stocker leurs données personnelles sur leurs propres appareils. Il en va de même pour les initiatives visant à fournir un justificatif d'identité aux individus qui ne disposent d'aucun document d'identité. Dans ce cas, des organisations ou individus malveillants pourraient, en théorie, accéder à ces informations en parvenant à contourner les dispositifs de sécurité de l'appareil ou en contraignant physiquement les bénéficiaires à leur remettre leurs appareils.

Il arrive également, comme mentionné dans les scénarios 1 et 2, que les organisations humanitaires stockent des données personnelles dans leurs propres bases de données dans le cadre d'un programme d'identité numérique. Or ces bases de données peuvent devenir la cible d'organisations ou d'individus malveillants. Les organisations humanitaires doivent donc s'assurer que leurs systèmes d'identité numérique préservent la confidentialité, la disponibilité et l'intégrité des données et, ce faisant, qu'elles protègent de manière adéquate les données contre tout usage abusif, toute violation et tout recours en responsabilité²⁵⁹. Par ailleurs, la nature sensible de certains types de données personnelles nécessitera généralement un très haut niveau de sécurité. Des techniques de chiffrement telles que les systèmes de partage de secret (ou de secret réparti) peuvent aider à augmenter la sécurité. Dans ces systèmes, les données sont chiffrées et la clé est partagée entre plusieurs parties (par exemple, différentes organisations humanitaires, comme l'envisage le scénario 3) qui devront collaborer pour déchiffrer les données, évitant ainsi d'avoir un point unique de défaillance. Dans ce cas, la clé peut aisément être détruite au besoin, car la suppression d'un certain nombre de fragments (le nombre varie d'un système à un autre) empêche toute utilisation future des données.

Lors de la mise en œuvre de programmes d'identité numérique, les organisations humanitaires devraient également tenir compte des mesures de sécurité adoptées par les partenaires éventuels. Ainsi, si les informations sur les bénéficiaires sont partagées avec d'autres organisations ou organismes, il est essentiel de mettre en place des mesures de sécurité pour les protéger et éviter les conséquences néfastes que pourrait avoir une violation de ces données.

²⁵⁹ USAID, 2017, p. 25.

12.6.6 CONSERVATION DE DONNÉES

Les données personnelles ne devraient pas être conservées plus longtemps que ce qui est nécessaire à la finalité du traitement. Lorsque la finalité principale du traitement est d'apporter une aide humanitaire sous forme de nourriture, d'abris ou de soins médicaux, les données personnelles ne devraient être conservées que pour la durée nécessaire à la fourniture de cette assistance. Toutefois, la situation est plus complexe pour les programmes d'identité numérique visant à fournir des justificatifs d'identité aux bénéficiaires qui ne disposent d'aucun document d'identité, car ceux-ci peuvent souhaiter continuer à utiliser ce justificatif (qui remplace un document d'identité ou fait office de document d'identité) toute leur vie et mettre à jour leur statut ou situation au fil des années. Dans ce cas, la définition d'une durée de conservation appropriée pour les données peut s'avérer complexe. Les organisations humanitaires devraient toutefois indiquer une durée de conservation initiale correspondant à la finalité initiale pour laquelle les données sont collectées. Une fois cette période écoulée, les organisations participant à ce type de programmes devraient évaluer régulièrement s'il est encore nécessaire de conserver ces données. Une autre option serait d'autoriser les bénéficiaires à décider par eux-mêmes de la conservation ou non de leurs données.

12.7 TRANSFERT INTERNATIONAL DE DONNÉES

Selon la solution technique et la conception choisie, les données traitées dans les systèmes d'identité numérique peuvent couramment traverser les frontières. Dans le scénario 3 évoqué plus haut, plusieurs organisations partagent des informations entre elles, ou les bénéficiaires eux-mêmes partagent leurs données avec plusieurs organisations en même temps. Ce transfert international de données soulève des questions de protection des données²⁶⁰. Bien que certaines juridictions aient adopté des dispositions en matière de protection (comme l'établissement de clauses contractuelles), les organisations humanitaires utilisant des programmes d'identité numérique peuvent éprouver des difficultés à mettre en œuvre ces dispositions dans la pratique, le système pouvant impliquer plusieurs parties situées à différents endroits. En règle générale, il est conseillé aux organisations humanitaires de prendre toutes les mesures possibles pour faire en sorte que tout transfert de données personnelles à un tiers (et tout transfert ultérieur) ne diminue pas le niveau de protection des droits des individus. Les organisations étant responsables de tous les transferts de données qu'elles effectuent, elles sont également tenues responsables si des données sont partagées de manière illicite avec d'autres organisations que celles envisagées dans ce scénario. Le consentement des bénéficiaires pourrait cependant constituer, dans certains cas, une base juridique appropriée pour le transfert de données par les organisations. Comme mentionné plus haut, on peut cependant se demander si les bénéficiaires sont toujours en mesure de donner un consentement valable²⁶¹. Si tel n'est pas le cas, une autre base juridique doit être identifiée.

²⁶⁰ Voir [chapitre 4 : Transfert international de données](#).

²⁶¹ Voir [section 3.2 : Consentement](#).

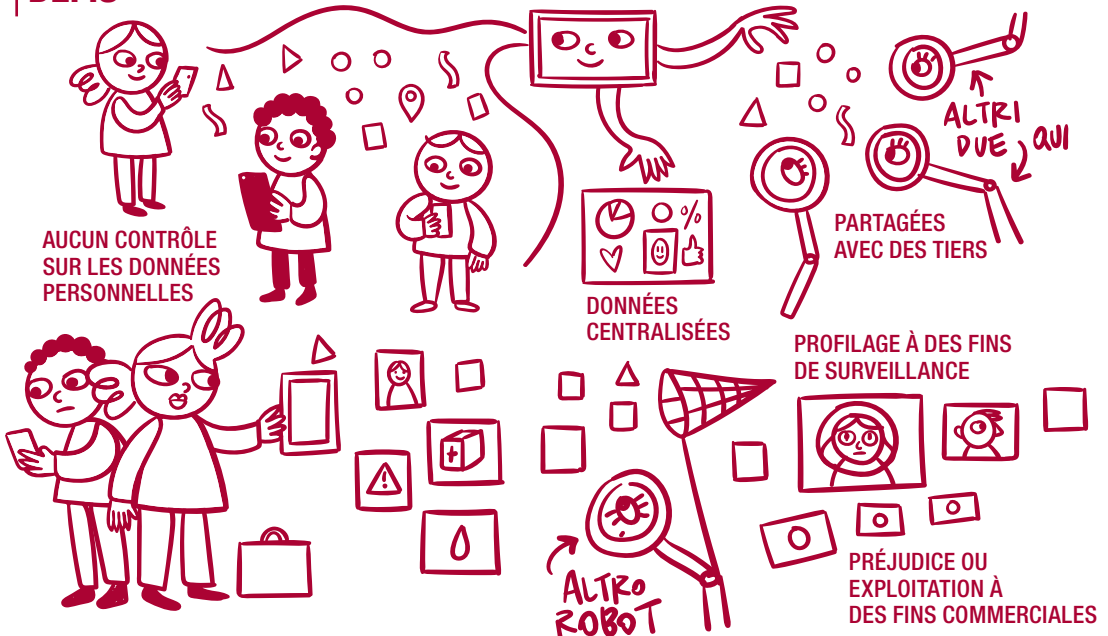
MÉDIAS SOCIAUX



UTILISATION POSSIBLE



DÉFIS



CHAPITRE 13

MÉDIAS SOCIAUX^{262, 263}

262 Ce chapitre est consacré à l'utilisation des médias sociaux par les organisations humanitaires pour communiquer avec les bénéficiaires et les impliquer davantage dans leurs programmes. Pour plus d'informations sur l'utilisation des médias sociaux en vue d'identifier les crises et améliorer les interventions humanitaires, consultez le [chapitre 6 : Analyse de données et big data](#). Pour en savoir plus sur les applications de messagerie, consultez le [chapitre 11 : Applications mobiles de messagerie](#).

263 Les auteurs souhaitent remercier Nicolas de Bouville (Facebook) pour sa participation à la rédaction de ce chapitre.

13.1 INTRODUCTION

13.1.1 MÉDIAS SOCIAUX DANS LE SECTEUR HUMANITAIRE

Les organisations humanitaires utilisent les médias sociaux de différentes manières pour communiquer avec leurs bénéficiaires. En situation d'urgence, par exemple, les médias sociaux peuvent permettre d'informer les personnes de l'existence de lieux sûrs ou de zones où l'aide est distribuée. Les organisations humanitaires peuvent aussi utiliser les médias sociaux pour faire de la sensibilisation (par exemple concernant les besoins humanitaires découlant des migrations), pour encourager les bénéficiaires à échanger des informations pertinentes dans une situation d'urgence ou pour fournir des renseignements en matière de santé et d'accès à des soins médicaux.

Cette interaction avec les bénéficiaires n'est toutefois pas sans risques. Lorsque les individus consultent les messages publics ou privés que les organisations humanitaires publient sur les médias sociaux, lorsqu'ils y répondent, ou lorsqu'ils rejoignent des groupes publics ou privés créés par ces organisations, ils partagent de nombreuses données avec la plateforme en question. Les organisations humanitaires et les bénéficiaires peuvent communiquer via les médias sociaux sans nécessairement avoir pleinement conscience qu'ils génèrent à la fois des données et des métadonnées (ensemble de données qui décrit d'autres données et donne des informations sur celles-ci²⁶⁴) qui peuvent être collectées par les plateformes des médias sociaux et utilisées pour dresser le profil d'un individu et définir ses caractéristiques, comme les principaux traits de son identité, ses réseaux, ses points de vue et opinions, ses préférences et ses appartenances à divers groupes. De même, les organisations et les bénéficiaires peuvent ne pas avoir conscience des conséquences et des risques liés au traitement de leurs données personnelles.

Bien que les individus puissent interagir avec les organisations humanitaires de manière informelle, comme s'il s'agissait d'une conversation privée, la conception et le fonctionnement des plateformes de ces médias sociaux peuvent en réalité permettre à des tiers de potentiellement suivre, collecter, conserver et analyser leurs échanges. Ces tiers comprennent non seulement des fournisseurs de médias sociaux, mais aussi des entreprises, des organismes chargés de l'application des lois, de l'immigration et du contrôle des frontières ainsi que les gouvernements, qui utilisent des techniques de renseignement en sources ouvertes et des outils sophistiqués de surveillance des médias sociaux. Les données, y compris les images partagées sur les médias sociaux, peuvent être analysées de différentes manières – depuis la reconnaissance d'images et de visages, jusqu'à l'identification

²⁶⁴ Pour en savoir plus sur les métadonnées, voir : CICR et Privacy International, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, 2018 : <https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf>.

de sentiments et d'émotions²⁶⁵ – qui reposent souvent sur des algorithmes opaques et l'apprentissage automatique²⁶⁶. Ce type de profilage rend encore plus obscure la manière dont les échanges sur les médias sociaux et leur utilisation exposent en réalité leurs utilisateurs. La prise de décisions fondées sur ce type de profilage peut avoir de graves conséquences pour un individu, car cette opacité augmente les risques découlant de l'accès inégal aux données et à la justice, comme l'impossibilité de remettre en question des hypothèses erronées qui influencent ou déterminent les processus décisionnels et les résultats.

Bien que les médias sociaux puissent faciliter le travail des organisations humanitaires, l'utilisation de ces plateformes peut aussi conduire à une perte de contrôle sur les données générées et partagées et poser des risques à moyen ou long terme. Ces risques doivent être évalués à l'aide de procédures et d'évaluations transparentes (voir section 13.2 ci-dessous sur les analyses d'impact relatives à la protection des données).

Voici quelques exemples d'utilisation des médias sociaux par les organisations humanitaires comme moyen de communication avec les bénéficiaires²⁶⁷:

- **Meilleure gestion des situations d'urgence grâce à la réduction de l'impact des catastrophes, à leur anticipation et à une meilleure préparation, et renforcement de la capacité à se relever**: au Bangladesh, la création d'une plateforme de coordination nationale a permis aux organisations humanitaires, de concert avec le gouvernement, de diffuser sur les médias sociaux des messages facilement compréhensibles qui ont permis aux populations de mieux se préparer aux catastrophes.
- **Amélioration de la distribution de l'assistance**: en 2016, le CICR a multiplié par deux le volume de nourriture contenu dans les colis alimentaires distribués en Syrie, les conditions de sécurité dans le pays ayant provoqué un allongement des intervalles entre les distributions alimentaires. Les bénéficiaires ont été informés de ce changement dans une courte vidéo partagée sur la page Facebook du CICR. À travers l'espace réservé aux commentaires, les bénéficiaires ont également pu réagir à la vidéo et expliquer leurs besoins (par exemple demander des cartons plus résistants pour que la nourriture contenue ne soit pas endommagée lors du transport). Le CICR a ensuite répondu aux commentaires, en expliquant comment il comptait satisfaire à certaines demandes, et pourquoi il ne pouvait satisfaire à d'autres.

²⁶⁵ Voir par exemple : F.M. Plaza-del-Arco *et al.*, « Improved emotion recognition in Spanish social media through incorporation of lexical knowledge », 27 septembre 2019 : <https://www.sciencedirect.com/science/article/pii/S0167739X1931163X>.

²⁶⁶ Voir [chapitre 16 : Intelligence artificielle et apprentissage automatique](#).

²⁶⁷ Exemples tirés de l'article suivant : T. Lüge, « Comment utiliser les médias sociaux pour communiquer avec les personnes touchées par une situation de crise : Un petit guide sur l'utilisation des médias sociaux dans les organisations humanitaires », CICR, IFRC et OCHA, 2017 : <https://www.icrc.org/fr/document/comment-utiliser-les-medias-sociaux-pour-communiquer-avec-les-personnes-touchees-par-une>.

- **Amélioration de l'efficacité des services :** la Croix-Rouge du Kenya suit activement les médias sociaux pour récolter des informations sur les accidents de la route et envoyer des ambulances sur les lieux où ils se produisent. En conséquence, les Kényans signalent fréquemment les accidents de la route à la Croix-Rouge via ces mêmes réseaux.
- **Fourniture d'« informations comme forme d'aide » et promotion de la santé :** MSF et d'autres ONG utilisent les médias sociaux pour fournir des informations et des conseils de santé aux bénéficiaires.

Bien que les plateformes de médias sociaux offrent un vaste éventail de possibilités, leur utilisation peut parfois poser des risques pour les bénéficiaires et soulever d'importantes questions de responsabilité pour les organisations humanitaires. Ce chapitre traitera de la manière dont sont générées les données sur les médias sociaux, puis des principales préoccupations en matière de protection des données.

13.1.2 MÉDIAS SOCIAUX ET DONNÉES

13.1.2.1 Quelles données sont générées sur les médias sociaux et de quelle manière ?

Les plateformes des médias sociaux reçoivent, enregistrent, génèrent et traitent de grands volumes de données des utilisateurs, notamment des métadonnées, des données de localisation, des images, des contacts, des « Likes » ainsi que des indicateurs d'attention et d'intérêt, puis les utilisent à diverses fins. Même lorsque les utilisateurs demandent explicitement des informations sur leurs données, les indications fournies sont souvent très peu transparentes et n'indiquent pas clairement quelles données spécifiques sont créées et comment la plateforme ou des tiers les récoltent et les utilisent à des fins de profilage ou autres.

Certaines données collectées par les plateformes des médias sociaux proviennent directement des individus (ce sont les « données déclarées »), par exemple lorsqu'ils créent un compte (nom, nom d'utilisateur, parfois copie d'un document d'identité, numéro de téléphone, adresse électronique et adresse physique) ou lorsqu'ils publient des photographies ou des commentaires sur leur profil²⁶⁸.

Les plateformes des médias sociaux traitent également des « données déduites » ; ce sont des données supplémentaires qui ne proviennent pas directement des utilisateurs, mais qui sont extrapolées sur la base de leurs données déclarées. Les données déclarées comprennent les données fournies directement par l'utilisateur et les données le concernant issues d'autres applications ou plateformes qui transfèrent parfois automatiquement des données personnelles aux plateformes de médias sociaux lorsque l'utilisateur ouvre l'application ou accède à ses services,

²⁶⁸ CICR et Privacy International, 2018, p. 34.

même avant l'obtention de son consentement²⁶⁹. Par exemple, c'est le cas lorsqu'une boutique en ligne informe la plateforme de médias sociaux que l'utilisateur a consulté son site Web, de sorte que la plateforme puisse utiliser ses préférences d'achat pour lui proposer des publicités ciblées.

Les plateformes de médias sociaux combinent généralement les données recueillies auprès de différentes sources et, en utilisant l'analyse de données²⁷⁰, créent un profil utilisateur pour surveiller les activités et le comportement de l'utilisateur en question²⁷¹. Par exemple, les fournisseurs peuvent déterminer qui sont ses amis en fonction de la fréquence à laquelle ils communiquent et interagissent sur les médias sociaux²⁷². Comprendre les habitudes et les comportements d'une personne permet aux plateformes de lui proposer des services ciblés et du contenu personnalisé²⁷³.

Les faits démontrent qu'il est possible d'établir un profil type d'identité à partir des attributs comportementaux numériques d'un individu, c'est-à-dire son activité en ligne²⁷⁴. Il est donc possible d'utiliser les traces numériques laissées par une personne pour créer un profil numérique, sans qu'elle le sache²⁷⁵, de déduire des informations la concernant, notamment son sexe, son orientation sexuelle, sa religion, son emplacement géographique et ses relations interpersonnelles, et même d'anticiper ses comportements²⁷⁶. Ce type de profil est ensuite utilisé pour de la publicité ciblée, mais également pour des campagnes politiques et de la prévision policière²⁷⁷. Cela signifie que si les organisations humanitaires encouragent les bénéficiaires à interagir avec elles sur les médias sociaux, elles peuvent potentiellement faciliter ce type de ciblage.

²⁶⁹ Privacy International, « Investigating Apps interactions with Facebook on Android », 2019 : <https://privacyinternational.org/appdata>.

²⁷⁰ Analyse de données et big data.

²⁷¹ Groupe de travail « Article 29 » sur la protection des données de l'UE, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, 2018, p. 13 : https://www.cdpd.bg/userfiles/file/WP29/wp251rev01_fr.pdf.

²⁷² CICR et Privacy International, 2018, p. 35.

²⁷³ Pour en savoir plus sur la publicité ciblée, voir : Privacy International, « AdTech » : <https://privacyinternational.org/topics/adtech>.

²⁷⁴ A. Beduschi et al., 2017, p. 8.

²⁷⁵ Par exemple, les comptes fantômes de Facebook. Voir : <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy>.

²⁷⁶ CICR et Privacy International, 2018, p. 90.

²⁷⁷ Voir, par exemple : A. Meijer and M. Wessels, « Predictive Policing: Review of Benefits and Drawbacks », *International Journal of Public Administration*, vol. 42, n° 12, 2019, p. 1031-1039 : <https://www.tandfonline.com/doi/full/10.1080/01900692.2019.1575664>. On considère que la prévision policière relève des pratiques d'application des lois.

EXEMPLES DE DONNÉES POUVANT ÊTRE COLLECTÉES :

Facebook divise les données collectées en différentes catégories : les données fournies par un utilisateur, les données concernant un utilisateur fournies par d'autres utilisateurs, les données sur les réseaux et connexions d'un utilisateur, les informations relatives aux paiements et celles relatives à l'appareil utilisé, ainsi que les informations reçues de partenaires, tels que les annonceurs et les concepteurs et éditeurs d'applications²⁷⁸. À chaque catégorie correspond une longue liste de données collectées par la plateforme, notamment :

les communications ainsi que d'autres informations que vous fournissez lorsque vous utilisez nos produits, notamment lorsque vous créez un compte, lorsque vous créez ou partagez du contenu, ou lorsque vous communiquez avec d'autres personnes ou leur envoyez des messages. Cela peut comprendre des informations présentes dans le contenu que vous fournissez (par exemple, des métadonnées) ou concernant un tel contenu, telles que le lieu où a été prise une photo ou la date à laquelle un fichier a été créé²⁷⁹.

Cette liste inclut également « les informations concernant les opérations et les comportements sur l'appareil, par exemple, lorsqu'une fenêtre est mise au premier plan ou en arrière-plan, ainsi que les mouvements de la souris²⁸⁰ », les signaux Bluetooth et les informations concernant les points d'accès wifi, les balises et les tours de télécommunication à proximité.

De son côté, Twitter collecte des données relatives aux informations de base sur les utilisateurs (comme le nom sous lequel un utilisateur s'inscrit, le nom d'utilisateur et l'adresse électronique), des informations sur le profil, des informations sur les contacts et des informations publiques (tweets et métadonnées générées par ces derniers, comme l'heure et le lieu)²⁸¹.

13.1.2.2 Quelles sont les données susceptibles d'être partagées avec des tiers ?

Certaines plateformes de médias sociaux partagent les informations qu'elles collectent avec d'autres fournisseurs de services, par exemple à des fins de publicité ciblée à l'intention d'individus ayant des profils spécifiques. Au vu de la croissance exponentielle des plateformes de médias sociaux, le nombre de personnes et d'agences de publicité ayant accès aux informations personnelles a fortement augmenté ces dernières années, multipliant ainsi les risques que des individus fassent l'objet d'un suivi grâce à différentes méthodes. Ces plateformes reçoivent en

²⁷⁸ Politique d'utilisation des données de Facebook : https://www.facebook.com/full_data_use_policy.

²⁷⁹ Ibid.

²⁸⁰ Ibid.

²⁸¹ CICR et Privacy International, 2018, p. 96.

outre des données d'autres parties et organisations dans le cadre de partenariats, et ces données supplémentaires sont utilisées pour affiner les profils des utilisateurs à diverses fins, comme la publicité.

EXEMPLES DE PARTAGE DES DONNÉES POSTÉES SUR LES MÉDIAS SOCIAUX :

Facebook partage des informations agrégées et collectées auprès d'utilisateurs et de non-utilisateurs du réseau avec d'autres entreprises qu'elle détient (notamment Instagram, WhatsApp et Messenger) et des partenaires tiers. Cela permet aussi aux utilisateurs de partager des données stockées sur Facebook avec des applications, des sites Web ou d'autres services tiers qui utilisent Facebook ou qui y sont intégrés²⁸². Les utilisateurs peuvent donc (consciemment ou non) partager des données qui ne les concernent pas exclusivement, comme leur liste d'amis. Par conséquent, « même lorsqu'un utilisateur verrouille son profil, ses données peuvent être collectées par une application tierce que l'un de ses amis utilise²⁸³ ».

Facebook offre également diverses options aux publicitaires quant à l'utilisation de profils d'utilisateur. Par exemple, les publicitaires peuvent télécharger une liste d'adresses électroniques ou de numéros de téléphone de clients enregistrés et demander à Facebook de trouver leurs profils de médias sociaux, avec pour objectif le ciblage à des fins de marketing (ce que l'on appelle les « audiences personnalisées²⁸⁴ »). De cette manière, ils bénéficient d'informations agrégées fournies par Facebook, tandis que la plateforme de médias sociaux collecte également des données auprès d'eux. Les entreprises peuvent aussi demander à Facebook de trouver des profils similaires à ceux de clients existants en vue d'élargir la portée de leur publicité, de se concentrer sur une zone géographique, une population ou un sexe spécifiques, ou même d'installer des pixels Facebook²⁸⁵ sur leur site Web, de sorte que dès qu'un utilisateur de Facebook consultera le site Web de l'entreprise, il recevra de la publicité de cette dernière sur sa page Facebook²⁸⁶. Cependant, depuis décembre 2019, Facebook n'autorise plus l'utilisation des numéros de téléphone fournis par les utilisateurs à l'inscription (dans le cadre de l'authentification à

²⁸² Politique d'utilisation des données de Facebook.

²⁸³ CICR et Privacy International, 2018, p. 96.

²⁸⁴ Facebook, « À propos des audiences personnalisées créées à partir de listes de clients » : <https://fr-fr.facebook.com/business/help/341425252616329?id=2469097953376494>.

²⁸⁵ Le pixel Facebook est un outil d'analyse qui permet aux entreprises de mieux cibler leurs publicités en mesurant leur efficacité et en suivant les actions entreprises par les internautes sur leur site Web. Voir : « À propos du pixel Facebook » : https://fr-fr.facebook.com/business/help/742478679120153?id=1205376682832142&helpref=page_content.

²⁸⁶ B.V. Alsenoy et al., *From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms*, Commission de la protection de la vie privée (Belgique), 2015, p. 55-64 : <https://www.law.kuleuven.be/citip/en/news/facebook-1/facebook-revised-policies-and-terms-v1-2.pdf>.

deux facteurs) pour faire des suggestions d'amis²⁸⁷. Ce changement de pratiques de l'entreprise démontre qu'elle reconnaît davantage les implications du partage de données entre plateformes et tiers. C'est ce dont témoigne le lancement de la nouvelle fonctionnalité « Activité en dehors de Facebook²⁸⁸ », qui permet aux utilisateurs de distinguer les informations obtenues par des tiers de celles de leur profil Facebook.

De son côté, Twitter laisse le choix à ses utilisateurs de refuser la plupart de ses activités de traitement. Tout le contenu publié et partagé sur la plateforme est néanmoins public par défaut, sauf indication contraire de l'utilisateur. En pratique, cela signifie que Twitter :

peut divulguer et partager les informations publiques d'un utilisateur (telles que les informations concernant son profil, ses tweets publics ou ses followers) avec de nombreux autres utilisateurs, services et organisations. Twitter se réserve également le droit de déduire, à partir de ces données, quels sujets seraient susceptibles d'intéresser l'utilisateur²⁸⁹.

13.1.2.3 Quelles données les organismes chargés de l'application des lois et les autorités publiques peuvent-ils obtenir ?

Le droit national peut exiger des plateformes de médias sociaux qu'elles stockent les données personnelles des utilisateurs de manière à ce que les pouvoirs publics puissent y accéder pour identifier un individu ou obtenir des informations sur son activité en ligne, à des fins d'application des lois²⁹⁰. Certaines juridictions – pas toutes – exigent un mandat pour accéder à ces informations.

Même si certaines informations sur les demandes d'accès des gouvernements sont publiquement accessibles, en particulier dans les pays dotés d'un appareil judiciaire développé, seules très peu d'entreprises du secteur des médias sociaux publient des rapports de transparence²⁹¹.

²⁸⁷ K. Paul, « Facebook separates security tool from friend suggestions, citing privacy overhaul », Reuters, 19 décembre 2019 : <https://www.reuters.com/article/us-facebook-privacy-idUSKBN1YN26Q>.

²⁸⁸ Facebook, « Lancement de la fonctionnalité “Activité en dehors de Facebook” pour voir et contrôler les informations que les applications et sites web partagent avec Facebook », 20 août 2019 : <https://about.fb.com/fr/news/2019/08/lancement-de-la-fonctionnalite-activite-en-dehors-de-facebook-pour-voir-et-controler-les-informations-que-les-applications-et-sites-web-partagent-avec-facebook/>.

²⁸⁹ CICR et Privacy International, 2018, p. 97.

²⁹⁰ *Ibid.*, p. 34.

²⁹¹ Facebook, « Government Requests for User Data », 2018 : <https://transparency.facebook.com/government-data-requests> ; Twitter, « Rapport de transparence de Twitter », 2018 : <https://transparency.twitter.com/fr.html>.

Grâce à l'utilisation de divers outils, y compris ceux fournis par les plateformes elles-mêmes (appelés « firehose »), les organismes chargés de l'application des lois et d'autres tiers peuvent accéder directement aux médias sociaux via l'*open-source intelligence* (OSINT), c'est-à-dire le recueil d'informations à partir de données accessibles au public. Ils peuvent également recourir à des techniques de *social media intelligence* (SOCMINT), qui consistent à surveiller et collecter des informations publiques et privées sur les plateformes des médias sociaux²⁹². Dans de nombreux pays, ces pratiques ne sont pas réglementées, et la législation est souvent floue quant à la légalité de cette surveillance. D'autres techniques invasives permettent également d'extraire des données et informations stockées physiquement sur un appareil²⁹³ ou dans des applications basées sur le cloud²⁹⁴. Comme pour le SOCMINT, les technologies d'extraction de données sur téléphones mobiles et sur le cloud sont utilisées de manière peu transparente et ne sont pas réglementées dans un certain nombre de pays. En pratique, comme les médias sociaux stockent souvent les données sur un cloud, ces méthodes permettent d'obtenir l'accès à un très grand volume de données personnelles.

13.2 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

Les organisations humanitaires ne peuvent véritablement contrôler la manière dont les plateformes de médias sociaux fonctionnent ni comment les données y sont produites et traitées. Elles peuvent toutefois, et doivent, procéder à une évaluation des risques afin de comprendre les conséquences de l'utilisation des médias sociaux pour communiquer avec les bénéficiaires, et ce, avant de décider si utiliser ou non ces plateformes, comment les utiliser et pour quelles finalités.

Lorsqu'elles utilisent les médias sociaux, les organisations humanitaires partent du principe que les bénéficiaires ont déjà accepté, d'une manière ou d'une autre, les conditions générales de la plateforme. Cela ne les libère toutefois pas de leur obligation de mener une AIPD²⁹⁵, dont l'objectif est d'identifier comment l'utilisation des médias sociaux affectera les bénéficiaires, et de déterminer les mesures que l'organisation peut prendre pour atténuer les risques éventuels. À cet

²⁹² Privacy International, « Social Media Intelligence » : <https://privacyinternational.org/explainer/55/social-media-intelligence>.

²⁹³ Voir, par exemple : Privacy International, « Push This Button For Evidence: Digital Forensics » : <https://privacyinternational.org/explainer/3022/push-button-evidence-digital-forensics>; et Privacy International, « Can the police limit what they extract from your phone? », 14 novembre 2019 : <https://privacyinternational.org/node/3281>.

²⁹⁴ Privacy International, « Cloud extraction technology: the secret tech that lets government agencies collect masses of data from your apps », 7 janvier 2020 : <https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data>.

²⁹⁵ Voir [chapitre 5 : Analyses d'impact relatives à la protection des données](#).

égard, une AIPD doit non seulement analyser les risques en matière de protection des données, mais aussi évaluer si l'utilisation des médias sociaux dans un contexte spécifique pourrait entraîner des violations des droits humains ou causer un autre préjudice aux individus concernés. Ces risques doivent ensuite être mis en balance avec les avantages potentiels.

Il est utile de souligner une fois encore qu'en plus du contenu généré par les utilisateurs et fourni dès la création de leur(s) compte(s), l'utilisation des médias sociaux génère un grand volume de données et métadonnées que les plateformes ne déclarent pas de manière proactive. Par conséquent, les utilisateurs peuvent même ne pas avoir conscience que ces données sont générées et traitées²⁹⁶. Par exemple, le simple fait de cliquer sur le bouton « Like » ou sur des liens qui redirigent l'utilisateur vers d'autres sites Web génère des métadonnées.

Ces dernières années, de nombreux gouvernements ont obtenu l'accès à d'importantes quantités de données et métadonnées issues des médias sociaux, ainsi qu'à des outils d'analyse puissants qu'ils ont pu utiliser pour identifier des tendances à partir de ces données et dresser le profil d'individus et de groupes²⁹⁷. L'AIPD doit par conséquent aller au-delà de la simple vérification du respect des exigences de protection des données. Elle doit également analyser l'incidence, positive ou négative, que l'utilisation d'une application ou d'une plateforme pourrait sur divers droits fondamentaux, et tenir compte des implications éthiques et sociales du traitement de données par les organisations internationales²⁹⁸.

Le traitement de métadonnées peut comporter des risques importants. En 2014, par exemple, un ancien directeur de la National Security Agency (NSA, Agence nationale de la sécurité américaine) a déclaré que l'agence était prête à exécuter des personnes sur la base d'informations extraites de métadonnées²⁹⁹. Le secteur des technologies financières et les agences de publicité emploient également diverses techniques pour exploiter ces données³⁰⁰. C'est pourquoi il est important que les organisations humanitaires tiennent dûment compte des finalités non humanitaires et des conséquences de l'utilisation des médias sociaux lorsqu'elles mènent une AIPD et élaborent leur stratégie d'utilisation des médias sociaux.

De la même façon, l'AIPD doit tenir compte du fait que les modèles commerciaux des fournisseurs de médias sociaux reposent sur la monétisation des données des utilisateurs (par exemple pour le ciblage publicitaire), ce qui signifie que les données

296 CICR et Privacy International, 2018, p. 17.

297 *Ibid.*, p. 29.

298 A. Mantelero, « AI and Big Data: A blueprint for a human rights, social and ethical impact assessment », *Computer Law & Security Review*, vol. 34, n° 4, 2018, p. 754-772 : <https://doi.org/10.1016/j.clsr.2018.05.017>.

299 CICR et Privacy International, 2018, p. 22.

300 *Ibid.*, p. 23-24.

générées à des fins humanitaires sur ces plateformes risquent d'être exploitées à des fins commerciales et de surveillance.

Les organisations humanitaires doivent également déterminer si les plateformes de médias sociaux sont le moyen le plus sûr et le plus fiable pour communiquer avec les bénéficiaires. Dans les situations d'urgence, par exemple, les gouvernements peuvent fermer les médias sociaux pour éviter que s'installe un climat de peur ou que de fausses informations circulent³⁰¹; les organisations humanitaires devront donc prévoir d'autres moyens de communication.

13.3 CONSIDÉRATIONS ÉTHIQUES ET AUTRES DÉFIS

Pour les organisations humanitaires, le fait d'associer les plateformes de médias sociaux à leurs activités soulève inévitablement des questions d'ordre éthique, car elles n'ont aucun contrôle sur les politiques de protection des données et de respect de la vie privée de ces tierces parties. Beaucoup de ces plateformes dépendent de l'exploitation et de la monétisation des données des utilisateurs³⁰² – tant des données déclarées que déduites, susceptibles de dévoiler des informations sensibles, comme l'orientation sexuelle, la religion, l'opinion politique et l'origine ethnique d'une personne³⁰³. En communiquant avec les bénéficiaires sur les médias sociaux, les organisations humanitaires contribuent à la production de données et métadonnées à partir desquelles ces informations sont déduites³⁰⁴.

De même, les plateformes de médias sociaux modifient constamment leurs conditions générales, leurs politiques en matière de respect de la vie privée et leurs activités de traitement, sans toujours demander le consentement des utilisateurs. En outre, même si les utilisateurs sont conscients que la plateforme traite des données déclarées, les plateformes ne sont pas toujours transparentes quant aux informations qu'elles déduisent de ces données – et, plus important encore, de celles obtenues d'autres sources (activité en ligne, autres utilisateurs et tiers, notamment) et de celles générées dès la conception et par défaut³⁰⁵ du fait de la conception et du fonctionnement de ces plateformes. Les informations rassemblées,

301 Voir, par exemple : J. Wakefield, « Sri Lanka attacks: The ban on social media », BBC, 23 avril 2019 : <https://www.bbc.com/news/technology-48022530>.

302 Voir, par exemple : Privacy International, « Guess what? Facebook still tracks you on Android apps (even if you don't have a Facebook account) », 5 mars 2019 : <https://privacyinternational.org/blog/2758/appdata-update>; et Privacy International, *How Apps on Android Share Data with Facebook – Report*, 2018 : <https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report>.

303 CICR et Privacy International, 2018, p. 89–90.

304 *Ibid.*, p. 91.

305 *Ibid.*, p. 102.

et au final les décisions prises sur la base de ces données, peuvent avoir de graves répercussions sur la vie d'un utilisateur, comme l'illustre l'exemple suivant :

On utilise de plus en plus souvent les données des médias sociaux pour évaluer la solvabilité des utilisateurs qui demandent un prêt et pour surveiller ceux à qui l'on a déjà accordé un prêt. Ces évaluations reposent sur une série d'indicateurs qui classent les personnes dans les deux catégories suivantes : « emprunteur fiable et de confiance » ou « emprunteur peu fiable et à risque³⁰⁶ ».

En plus des risques associés aux données que les bénéficiaires partagent sur les plateformes de médias sociaux, les organisations humanitaires doivent être conscientes des informations qu'elles-mêmes partagent. Certains contenus, comme des photographies ou des vidéos publiques où apparaissent des bénéficiaires, peuvent avoir des conséquences négatives sur les individus en question – que ce soit en termes de profilage et ciblage réalisés par des entreprises, de persécution, d'intimidation, de chantage, de discrimination, d'usurpation d'identité ou de perte de contrôle sur leurs données.

Les organisations doivent aussi garder à l'esprit que les médias sociaux ne sont pas toujours le moyen le plus utile ou efficace pour toucher un public donné. L'utilisation des médias sociaux est souvent faible dans les zones rurales et reculées, et tous les membres d'une population cible ne disposent pas forcément du même accès à ces technologies. De même, dans certains contextes, la plupart des utilisateurs de médias sociaux seront des hommes, ce qui rendra l'utilisation de ces plateformes moins efficace pour des initiatives en faveur de la santé des femmes.

13.4 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Lorsque les organisations humanitaires utilisent les médias sociaux à des fins de communication, leur rôle en ce qui concerne le traitement des données personnelles des bénéficiaires n'est pas toujours clair. Par exemple, lorsqu'elles créent une page ou un profil institutionnel sur une plateforme de médias sociaux, les conditions générales de la plateforme peuvent autoriser le fournisseur à traiter davantage de données via cette page, ou à dresser le profil des utilisateurs à des fins de publicité. Dans ce cas, l'organisation pourrait être considérée comme responsable conjoint avec la plateforme et porter ainsi une partie de la responsabilité du traitement des données. Toutefois, lorsqu'une organisation ne fait qu'utiliser la plateforme pour communiquer avec les bénéficiaires à travers une page, un profil ou un groupe créé par les bénéficiaires eux-mêmes, il est plus difficile d'établir le rôle et les responsabilités de l'organisation.

³⁰⁶ CICR et Privacy International, 2018, p. 106. Voir aussi : Privacy International, « Fintech » : <https://privacyinternational.org/topics/fintech>.

EXEMPLE D'UN CONTRÔLE CONJOINT :

En 2018, la Cour de justice de l'Union européenne (CJUE), dans l'affaire C-210/16, a décidé que les administrateurs des pages Facebook devaient être qualifiés de responsables du traitement dans le cadre de la collecte et du traitement des données à caractère personnel effectués par Facebook via leurs pages fan (une page fan est une page institutionnelle créée par une entreprise ou une organisation sur la plateforme Facebook pour communiquer avec les utilisateurs de Facebook et partager du contenu concernant leurs activités³⁰⁷). Comme les pages fan sont hébergées sur la plateforme Facebook, Facebook recueille des informations sur ceux qui y ont accès ou qui l'utilisent, indépendamment du fait qu'ils aient ou non un compte Facebook. Facebook utilise ces informations pour établir des statistiques concernant les visiteurs des pages fan, qui sont ensuite partagées avec l'administrateur de la page.

Selon la Cour de justice, les administrateurs de ces pages (c'est-à-dire les organisations qui les créent et les gèrent) sont responsables du traitement, car la création d'une page fan « offre à Facebook la possibilité de placer des cookies sur l'ordinateur ou sur tout autre appareil de la personne ayant visité sa page fan, que cette personne dispose ou non d'un compte Facebook » (par. 35). Par ailleurs, du moment que les administrateurs définissent les paramètres spécifiques que Facebook doit collecter pour établir des statistiques sur les visiteurs des pages, on considère qu'ils participent à la détermination des moyens et des finalités du traitement.

Bien que cet arrêt soit ancré dans le contexte réglementaire de l'Union européenne et ne concerne que Facebook, l'influence de la législation de l'UE en matière de protection des données fait que cette définition générale du contrôle (bien que controversée) peut également être adoptée dans d'autres régions. Dans une telle éventualité, les organisations humanitaires pourraient être considérées comme responsables des données personnelles que traitent les plateformes de médias sociaux hébergeant leur page. En pratique, cela signifie que lorsque la plateforme traite des données personnelles collectées sur la page de l'organisation à des fins non humanitaires, l'organisation en question pourrait être tenue pour responsable de ce traitement.

Les organisations humanitaires doivent dès lors faire tout leur possible pour être parfaitement au fait des modèles commerciaux, des politiques de protection de la vie privée et des protocoles de sécurité des plateformes de médias sociaux qu'elles utilisent, car elles pourraient être tenues responsables de tout usage

307 Cour de justice de l'Union européenne (CJUE), Affaire 210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH, Arrêt ECLI:EU:C:2018:3885, juin 2018 : <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62016CJ0210&from=FR>.

abusif des données, par la plateforme ou des tiers. En cas de doute concernant le respect des politiques de protection des données, des droits humains et des principes humanitaires, les organisations doivent toujours opter pour un moyen de communication plus sûr.

13.5 PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

13.5.1 FONDEMENTS JURIDIQUES DU TRAITEMENT DE DONNÉES PERSONNELLES

Bien que les organisations humanitaires ne puissent contrôler le fonctionnement des plateformes de médias sociaux ni le traitement qu'elles font des données, elles doivent néanmoins déterminer la base juridique pour le traitement des données qu'elles demandent ou reçoivent via les médias sociaux. Par exemple, elles peuvent parfois utiliser des photos de bénéficiaires dans le cadre de campagnes de relations publiques. Lorsque le consentement est un fondement juridique, un individu doit être en mesure de le retirer. Néanmoins, lorsqu'une image ou une vidéo est publiée en ligne, l'organisation peut perdre le contrôle des copies et reproductions qui en sont faites et, si un bénéficiaire retire son consentement, elle peut se trouver dans l'incapacité de supprimer entièrement ces contenus.

Les organisations humanitaires doivent identifier une base juridique pour chaque activité de traitement³⁰⁸. Souvent, elles utilisent le même profil ou la même page dans les médias sociaux pour leurs activités humanitaires, leurs campagnes de sensibilisation et leurs collectes de fonds, ce qui complexifie concrètement la différenciation de chaque finalité. Dans de tels cas, il est important de tenir compte de la finalité de chaque composante d'une activité de traitement et de la documenter en conséquence³⁰⁹.

13.5.2 INFORMATION

Les individus doivent obtenir des informations claires et en temps opportun concernant le traitement de leurs données par le responsable du traitement³¹⁰, précisant quelles données sont collectées (par exemple pour fournir un service), quelles données sont générées par l'utilisation du service, quelles sont les finalités de la collecte et qui peut accéder aux données personnelles des individus, les partager ou les utiliser. Ces informations permettent aux personnes concernées de prendre des décisions éclairées concernant l'utilisation d'un service spécifique et de comprendre comment exercer leurs droits. Cela dit, lorsque les organisations humanitaires interagissent avec les bénéficiaires via les médias sociaux, les données sont

308 Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

309 Voir [chapitre 3 : Fondements juridiques du traitement des données personnelles](#).

310 Voir [section 2.10 : Information](#).

principalement générées et traitées directement via les plateformes elles-mêmes, ce qui laisse peu de contrôle aux organisations humanitaires sur les actions mentionnées plus haut. Les organisations devraient toutefois s'engager à fournir des informations pertinentes dans la mesure du possible.

Il est important de souligner une fois encore que les plateformes modifient et mettent à jour régulièrement leurs politiques en matière de protection de la vie privée et de protection des données, ce qui fait qu'il peut être extrêmement difficile pour les utilisateurs de comprendre quelles données sont générées et traitées (autrement dit, comment elles sont utilisées et avec qui elles sont partagées³¹¹). Il n'est donc pas facile pour les organisations humanitaires d'appréhender les risques liés à l'utilisation des plateformes de réseaux sociaux, ni de déterminer la nature des informations qu'elles doivent fournir aux personnes concernées. À tout le moins, il est conseillé aux organisations humanitaires d'informer les bénéficiaires des activités de traitement dont elles sont responsables – par exemple, d'expliquer pourquoi elles communiquent sur les médias sociaux et comment les informations que les bénéficiaires partagent avec elles seront utilisées et pour quelles finalités.

Bien que les organisations humanitaires ne contrôlent pas l'utilisation que font les plateformes de médias sociaux des données collectées, certaines ont lancé des campagnes de sensibilisation en ligne pour expliquer les risques associés aux médias sociaux et préciser ce que doivent faire les bénéficiaires pour protéger leurs données. Au Mexique, par exemple, le HCR utilise la page El Jaguar pour communiquer avec les bénéficiaires. L'organisation a publié une vidéo sur cette page pour les alerter des risques associés à l'utilisation de Facebook et leur indiquer comment les réduire³¹².

Ce type de campagnes aide les bénéficiaires à identifier l'ensemble des parties et organisations qui peuvent accéder aux données qu'ils produisent sur les médias sociaux, et à comprendre les risques pouvant découler de l'utilisation de ces plateformes. Néanmoins, le fait d'informer les bénéficiaires sur les données des médias sociaux et les politiques de protection de la vie privée peut s'avérer peu utile s'il n'existe aucune alternative à la plateforme qu'ils utilisent. Les organisations humanitaires devraient veiller à informer les bénéficiaires des risques les plus probables qu'ils encourent, par exemple lorsqu'ils rejoignent des groupes ou suivent des pages sur les médias sociaux ; elles devraient également leur expliquer comment d'autres personnes peuvent voir leur appartenance à ces communautés et utiliser cette information contre eux. Cet aspect est particulièrement important car, outre les préoccupations liées à la protection des données, l'utilisation des médias sociaux présente d'autres risques, tels que la surveillance et l'identification ultérieure (et l'éventuelle localisation) de personnes et de groupes vulnérables par des tiers mal intentionnés.

³¹¹ CICR et Privacy International, 2018, p. 17.

³¹² Voir la vidéo de la campagne (en espagnol) à l'adresse : <https://www.facebook.com/ConfiaEnElJaguar/videos/874221649451680/>.

13.5.3 CONSERVATION DES DONNÉES

Conformément au principe de conservation des données, celles-ci doivent être conservées pour une durée définie nécessaire aux finalités du traitement. Cette durée peut être de trois mois, d'un an, se prolonger tant qu'une crise se poursuit, ou s'inscrire dans un autre cadre temporel³¹³. Lorsque, au moment de la collecte, il est impossible de définir pour combien de temps les données devront être conservées, il convient de reconsidérer la question à la fin d'une période initiale.

Lorsque les organisations humanitaires interagissent avec les bénéficiaires via les médias sociaux, les plateformes collectent et conservent elles-mêmes leurs données. La durée de conservation varie de ce fait d'une plateforme à une autre.

EXEMPLES TIRÉS DE LA POLITIQUE DE FACEBOOK EN MATIÈRE DE CONSERVATION DES DONNÉES :

La politique de Facebook en matière d'utilisation des données précise que les données sont conservées jusqu'à ce qu'il ne soit plus nécessaire de fournir les services ou jusqu'à la suppression du compte, bien qu'il apparaisse que la plateforme conserve certaines données même après la suppression d'un compte³¹⁴. La politique détaille ensuite :

« Il s'agit d'une décision au cas par cas qui dépend d'aspects tels que la nature des données, la raison de leur collecte et de leur traitement et les besoins de conservation légaux ou opérationnels concernés. Par exemple lorsque vous faites une recherche sur Facebook, vous pouvez consulter et supprimer cette recherche de votre historique de recherche à tout moment, mais l'enregistrement de cette recherche n'est supprimé qu'au bout de six mois. Si vous envoyez une copie de votre pièce d'identité officielle à des fins de vérification de votre compte, nous supprimons cette copie 30 jours après l'envoi³¹⁵. »

Il arrive que certaines plateformes de médias sociaux partagent des données ou des informations avec des tiers. Ces tiers peuvent avoir des règles différentes en matière de conservation des données. Le fait que les utilisateurs de médias sociaux doivent accepter les conditions générales pour utiliser ces services soulève des questions quant à leur acceptation des politiques de conservation des tiers. Les organisations humanitaires doivent par conséquent analyser ces politiques, évaluer les risques éventuels qu'elles présentent pour les bénéficiaires ou pour elles-mêmes, et prendre une décision éclairée concernant l'utilisation de la plateforme au regard de l'objectif visé.

³¹³ Voir [section 2.7: Conservation des données](#).

³¹⁴ A. Picchi, « OK, you've deleted Facebook, but is your data still out there? », CBS News, 23 mars 2018 : <https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/>.

³¹⁵ Politique d'utilisation des données de Facebook.

Les organisations humanitaires sont également tenues de définir des durées et des politiques de conservation des données qu'elles collectent auprès des bénéficiaires via les interactions, groupes et pages sur les médias sociaux. Elles doivent expliquer ces durées et politiques à leur personnel ainsi qu'aux bénéficiaires.

13.5.4 SÉCURITÉ DES DONNÉES

Les organisations humanitaires doivent effectuer une AIPD (voir section 13.2 ci-dessus) en tenant compte du modèle commercial, des politiques, des conditions générales et de l'écosystème de la plateforme, ainsi que de toute mesure de sécurité que cette dernière a mise en place pour protéger les données traitées. Même lorsque la plateforme ne partage pas ouvertement ces informations, il peut être utile de commencer par analyser des cas de violations de données auxquels elle a été confrontée par le passé, la réponse qu'elle a adoptée et les autres vulnérabilités connues. Il est également important de comprendre comment la plateforme traite les données des utilisateurs et quelles mesures sont en place pour garantir leur conservation en toute sécurité.

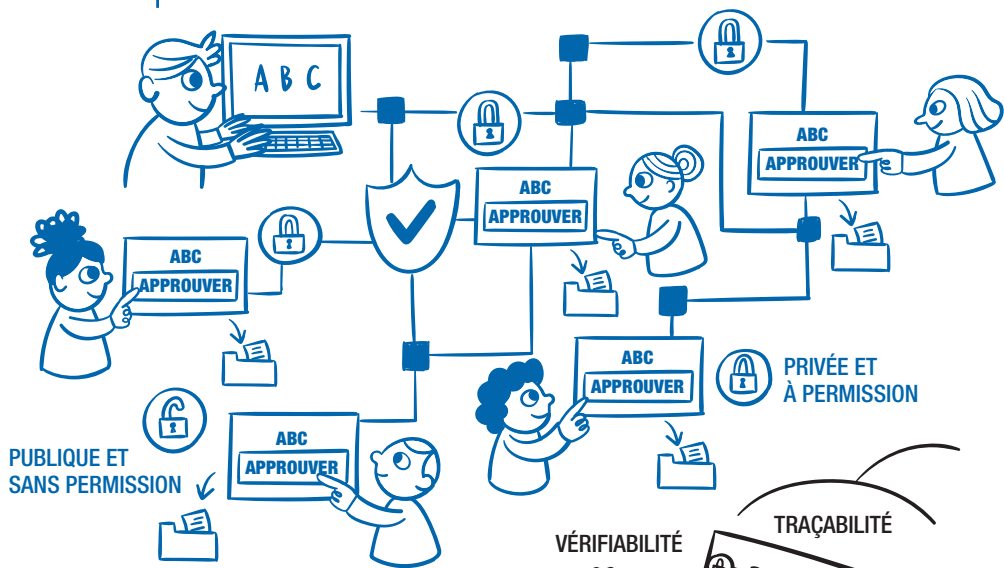
En interne, il est conseillé aux organisations humanitaires de veiller à prendre les mesures appropriées pour protéger les données qu'elles collectent auprès de bénéficiaires, par exemple en utilisant un identifiant et un mot de passe fort, en limitant l'accès à ceux qui en ont besoin et en formant leur personnel à la gestion correcte des données.

13.6 TRANSFERT INTERNATIONAL DE DONNÉES

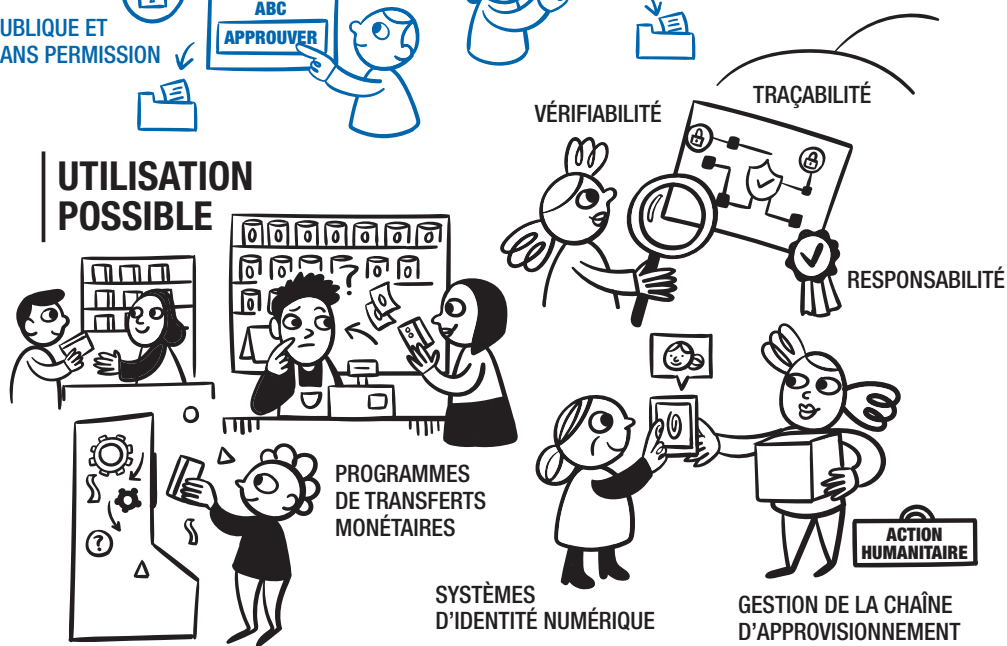
Les données traitées via les plateformes de médias sociaux traversent couramment les frontières, ce qui suscite des préoccupations en termes de protection des données personnelles. Malgré l'existence de mécanismes contractuels reconnus, il peut être difficile pour les organisations humanitaires de s'en servir efficacement, du fait surtout qu'elles ne contrôlent pas les plateformes de médias sociaux. Ceci étant, les organisations doivent faire tout leur possible pour veiller à ce que le fournisseur mette en place des dispositions permettant d'encadrer le transfert des données³¹⁶. Déterminer le droit et la juridiction applicables peut également s'avérer complexe, une analyse de risque adéquate et ciblée étant impossible à réaliser si le choix de la juridiction et du droit n'a pas été clairement établi dans les politiques de gouvernance des médias sociaux.

316 Voir [chapitre 4 : Transfert international de données](#).

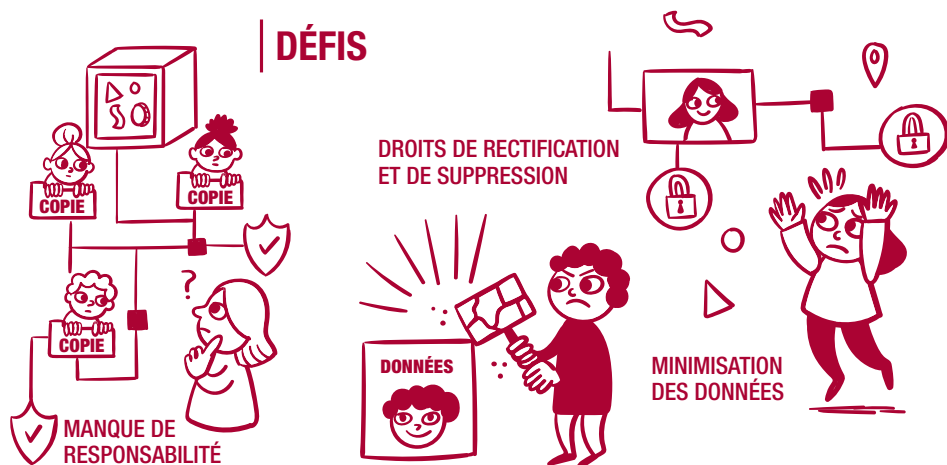
BLOCKCHAIN



UTILISATION POSSIBLE



DÉFIS



CHAPITRE 14

BLOCKCHAIN³¹⁷

317 Les auteurs souhaitent remercier Robert Riemann (Contrôleur européen de la protection des données), Giulio Coppi (Norwegian Refugee Council) et Bryan Ford (École polytechnique fédérale de Lausanne) pour leur aide à la rédaction de ce chapitre.

14.1 INTRODUCTION

Ces dernières années, le terme *blockchain* est devenu à la mode et de nombreuses organisations, y compris dans le secteur humanitaire, tentent de trouver une utilité à cette technologie. Par exemple, la blockchain pourrait améliorer l'efficacité des programmes humanitaires impliquant des transactions financières ou un suivi de l'approvisionnement³¹⁸. Elle pourrait également augmenter la transparence et la confiance quant à l'intégrité des informations³¹⁹. Ces améliorations pourraient cependant être contrebalancées par un certain nombre de problèmes pratiques et de défis en termes de protection des données. Nous les passerons en revue ci-après, de même que les avantages et les risques escomptés.

Ce chapitre présente le fonctionnement et l'architecture de la technologie de la blockchain de façon simplifiée (sections 14.1.1 à 14.1.3). Vu la complexité de cette technologie, cette présentation n'a pas vocation à être exhaustive. Elle vise simplement à appuyer l'analyse qui est faite de cette technologie du point de vue de la protection des données dans les sections 14.2 à 14.7 ci-après³²⁰.

14.1.1 QU'EST-CE QU'UNE BLOCKCHAIN ?

Une blockchain est « en substance une base de données décentralisée fonctionnant en mode ajout uniquement qui est gérée par un algorithme de consensus et stockée sur plusieurs nœuds (informatiques)³²¹ ». Cette définition comprend un certain nombre d'éléments techniques qui seront expliqués plus en détail ci-dessous. La technologie de la blockchain est essentiellement un moyen spécifique de stocker des données dans une base de données. De ce fait, une blockchain peut stocker tout type de données, y compris des données personnelles. Dans une blockchain, chaque élément de donnée est stocké l'un après l'autre dans une chaîne (d'où le « mode ajout uniquement³²² »). Cette opération est réalisée en groupant des données en blocs et en ajoutant à chaque nouveau bloc un identifiant cryptographique (une référence ou un lien) qui le relie au bloc précédent.

³¹⁸ V. Ko et A. Verity, *Blockchain for the Humanitarian Sector: Future Opportunities*, OCHA, 2016, p. 12-14 : <https://reliefweb.int/sites/reliefweb.int/files/resources/BlockChain%20for%20the%20Humanitarian%20Sector%20-%20Future%20Opportunities%20-%20November%202016.pdf>.

³¹⁹ *Ibid.*, p. 8.

³²⁰ Pour des définitions et explications plus détaillées sur la technologie des blockchains, veuillez consulter : J. Bacon *et al.*, « Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers », *Richmond Journal of Law & Technology*, vol. 25, n° 1, 2018 : <https://jolt.richmond.edu/Blockchain-demystified-a-technical-and-legal-introduction-to-distributed-and-centralised-ledgers/>.

³²¹ M. Finck, « Blockchains and Data Protection in the European Union », *European Data Protection Law Review*, vol. 4, n° 1, 2018, p. 17 : <https://doi.org/10.21552/edpl/2018/1/6>.

³²² Notons que cette propriété est la raison pour laquelle on les appelle également registres : livres qui stockent des transactions (traditionnellement monétaires) en mode ajout seulement.

La conception des blockchains vise à augmenter la sécurité (au sens large du terme). Comme mentionné plus haut, l'objectif principal de la technologie de la blockchain est d'augmenter la transparence et la confiance quant à l'intégrité de la base de données. Les blockchains sont « distribuées » et souvent « décentralisées ». Bien qu'il s'agisse de deux notions différentes, elles ont un point commun : elles indiquent que les données traitées ne sont pas gérées et stockées de manière centrale. Le terme « distribué » s'entend ici de la présence de plusieurs copies de bases de données stockées sur différents ordinateurs, tandis que le terme « décentralisé » signifie que le pouvoir et l'autorité de décider quelles données sont ajoutées au registre ne reviennent pas à une seule entité ou un seul individu, mais sont partagés entre plusieurs entités ou individus devant dès lors collaborer. Dans ce chapitre, on désignera ces entités ou individus sous le nom de « validateurs » (car ils valident ensemble les données à stocker dans la blockchain). Généralement, plus les validateurs sont nombreux, plus les règles à suivre pour s'entendre sont complexes. Ces règles sont définies dans un « protocole de consensus » (voir section 14.1.2 ci-dessous pour plus de détails).

Les ordinateurs qui détiennent une copie de la blockchain sont appelés « nœuds » (puisque'ils représentent des nœuds dans un vaste réseau). Les nœuds peuvent être passifs (s'ils stockent uniquement une copie à jour de la blockchain) ou actifs. Les nœuds actifs sont aussi des validateurs et on dit généralement qu'ils font du « minage » de données (c'est-à-dire qu'ils participent au protocole de consensus pour valider de nouveaux ajouts). Par analogie, les validateurs sont parfois appelés « mineurs ».

Les « utilisateurs » sont les participants qui souhaitent ajouter des informations à la blockchain (autrement dit, qui créent des données devant être validées et enregistrées dans la blockchain).

Une information ne sera ajoutée dans une blockchain qu'après validation. Il est donc extrêmement complexe pour un acteur malveillant d'ajouter des données dans une blockchain, tout ajout devant d'abord être accepté par le validateur.

En outre, les blocs de données contenus dans une blockchain sont horodatés, comme mentionné plus haut, et comportent un lien cryptographique (identifiant ou référence) qui les relie au bloc précédent. Cela signifie que si une partie malveillante parvenait à modifier les données contenues dans un bloc spécifique, elle devrait également modifier le bloc suivant (en raison du changement de son identifiant cryptographique), ainsi que tous les blocs subséquents, jusqu'à la fin de la chaîne. Ces modifications ne passeraient certainement pas inaperçues du fait de la conception décentralisée de la blockchain, qui implique la validation de chacune d'elles par un validateur. Comme il est en pratique très complexe (mais pas entièrement impossible) de modifier des informations dans les blockchains, on les appelle souvent des registres immuables³²³.

323 Finck, 2018, p. 19.

Lorsque de nouvelles informations sont ajoutées à la blockchain, un mécanisme basé sur une paire de clés publique et privée est utilisé afin de sécuriser la transaction³²⁴. Chaque utilisateur de la blockchain doit posséder une (ou plusieurs) paire de clés. La clé publique – ou une valeur qui en est dérivée – représente l'adresse de l'utilisateur sur la blockchain. Cette adresse est publique et permet de vérifier l'origine et – parfois – la destination des informations. Bien que les clés publiques ne puissent, à elles seules, dévoiler l'identité de la personne à laquelle elles sont rattachées, elles sont considérées comme des données personnelles pseudonymisées car elles sont liées à une personne spécifique (l'utilisateur qui a ajouté l'information). Elles pourraient par exemple permettre de remonter à l'adresse IP d'une personne, ce qui pourrait mener à son identification³²⁵. Comme les blockchains sont quasi immuables, les clés publiques peuvent potentiellement rester dans la blockchain aussi longtemps que le registre existe.

Certaines des caractéristiques susmentionnées de la technologie de la blockchain peuvent présenter des avantages pour les organisations humanitaires. Par exemple, l'architecture décentralisée peut augmenter la sécurité, puisque ces systèmes ne présentent pas de point unique de défaillance ou de compromission. Cela signifie que les éventuelles attaques doivent compromettre plusieurs liens pour compromettre l'ensemble de la blockchain. Cette caractéristique augmente l'intégrité du système, car elle est réputée garantir le caractère immuable des données en presque toute circonstance.

Compte tenu du caractère horodaté et quasi immuable des informations, et du fait que les responsabilités soient partagées, certains affirment³²⁶ que la blockchain est surtout utile dans les situations suivantes :

- suivi de la propriété d'actifs complexes au fil du temps ;
- implication de plusieurs groupes ou parties prenantes ;
- absence d'une autorité centrale bien établie et efficace (aussi appelée tiers de confiance) ;
- nécessité d'une collaboration entre les groupes ou parties prenantes ;
- exigence d'un relevé ou d'une preuve des transactions.

Ces exemples montrent que l'un des principaux avantages de la technologie de la blockchain est l'absence d'un point unique de défaillance ou de compromission. Cela s'explique par la conception distribuée du registre, qui implique que plusieurs nœuds doivent collaborer pour ajouter de nouvelles données à la blockchain. En outre, puisque l'ensemble du registre est copié sur plusieurs nœuds, il devient difficile de modifier des informations dans ce dernier, et les données demeurent accessibles même si un nœud est compromis ; l'intégrité du registre s'en trouve ainsi renforcée.

³²⁴ Finck, 2018, p. 19.

³²⁵ *Ibid.*, p. 24-25.

³²⁶ Ko et Verity, 2016, p. 9.

Il est important de souligner qu'il n'est pas utile de recourir à la technologie de la blockchain si le niveau d'intégrité ne présente aucun problème (c'est-à-dire s'il y a une confiance suffisante entre les participants à un programme spécifique et si le niveau de vérifiabilité est suffisant) ou simplement si d'autres technologies offrent un niveau d'intégrité et de disponibilité suffisant. Dans ce cas, la mise en œuvre d'une solution plus traditionnelle, par exemple avec une base de données centralisée, peut s'avérer plus efficace, plus rapide, moins onéreuse et globalement plus adaptée d'un point de vue de la protection des données.

14.1.2 TYPES DE BLOCKCHAIN

Une blockchain peut être construite de différentes manières, en fonction des choix de conception du système. Par exemple, une décision clé concerne le caractère public ou privé de la blockchain. Bien qu'il n'existe aucune définition universelle, les définitions suivantes sont couramment utilisées :

Blockchain	Sans permission : tout le monde peut devenir validateur (nœud ou mineur).	À permission : les validateurs (nœuds ou mineurs) sont prédéfinis et autorisés par un organisme de contrôle.
Publique : tout le monde peut accéder (« voir » ou « lire ») aux données stockées sur la blockchain et ajouter des transactions.	Tout le monde peut lire les transactions (publiques) sur la blockchain et participer au mécanisme de consensus en tant que validateur de nouvelles transactions. Il est toutefois important de souligner que les données ajoutées au registre peuvent être chiffrées, auquel cas il sera impossible de déchiffrer et de lire le contenu sans la clé de déchiffrement. L'horodatage et les clés publiques restent néanmoins visibles par tous. Ce type de blockchain (publique sans permission) est utilisé par le bitcoin.	Tout le monde peut lire les transactions (publiques) sur la blockchain, mais seules les parties prédéfinies peuvent devenir validateurs et participer au mécanisme de consensus pour valider de nouveaux ajouts. Ces blockchains pourraient par exemple améliorer la transparence d'une chaîne d'approvisionnement, puisque seules les parties impliquées dans l'approvisionnement en biens seraient autorisées à modifier le registre (en tant que validateurs), mais quiconque pourrait vérifier les transactions.
Privée : seuls les utilisateurs autorisés peuvent accéder aux données sur la blockchain.	En théorie, ce type de blockchain autorise l'accès aux données stockées uniquement aux parties prédéfinies ; mais tout le monde peut participer à la validation de nouveaux ajouts. En pratique, ce type de blockchain est néanmoins complexe à mettre en œuvre, car les validateurs peuvent stocker une copie complète du registre. Par conséquent, il serait difficile de développer une plateforme sur laquelle les validateurs ne seraient pas autorisés à accéder aux informations du registre.	Seuls les utilisateurs prédéfinis peuvent accéder (« lire ») aux données stockées sur la blockchain et seuls les validateurs prédéfinis (pas nécessairement les mêmes utilisateurs) peuvent participer à la validation de nouveaux ajouts.

En plus de déterminer quels utilisateurs peuvent « lire » ou « écrire » des données sur la blockchain, les concepteurs du système doivent également définir les modalités de validation à adopter. Les processus de validation des blockchains sont régis par des mécanismes de consensus (ou protocoles de consensus) constitués d'un ensemble de règles prédéfinies qui distribuent la responsabilité entre les parties. Ces règles permettent de stocker des données de manière immuable sans autorité centrale (ou tiers de confiance), préservant ainsi l'intégrité du registre³²⁷. Autrement dit, les mécanismes de consensus définissent comment les nouvelles informations sont validées par les participants à la blockchain et, le cas échéant, comment elles sont ajoutées au registre.

Il existe différents types de mécanismes de consensus. Par exemple, dans le cas de blockchains qui utilisent le mécanisme de la preuve de travail (*proof-of-work*), les validateurs doivent obtenir le droit de valider une transaction en résolvant des problèmes mathématiques complexes en recourant à la force de calcul brute, ce qui implique un investissement considérable en puissance de calcul et en électricité³²⁸. Dans le cas du mécanisme de la preuve d'enjeu (*proof-of-stake*), les participants disposent simplement d'un droit de vote, la pondération de leur vote pouvant néanmoins varier en fonction de leur part dans la blockchain.

Pour illustrer certains des choix à faire lors de la conception d'une blockchain, il est utile de penser au système comme à une société. Les sociétés tiennent généralement des réunions du conseil d'administration, et des règles sont établies pour définir comment les membres du conseil d'administration sont choisis et qui a le droit de voter et de prendre des décisions. Une première option consiste à avoir un groupe fermé d'individus qui décident qui rejoint ou quitte le conseil (comme dans le cas d'une blockchain à permission). Une autre possibilité est de permettre à quiconque à siéger au conseil pour autant qu'il achète suffisamment « d'actions » de la société pour avoir un droit de vote (comme dans le cas d'une blockchain avec preuve d'enjeu). Une troisième option est de décider que quiconque peut siéger au conseil pour autant qu'il puisse démontrer qu'il a consacré suffisamment d'énergie à une tâche donnée au cours des dix dernières minutes – une barrière artificielle à l'entrée (comme dans le cas d'une blockchain avec preuve de travail).

327 W. Al-Saqaf et N. Seidler, « Blockchain technology for social impact: opportunities and challenges ahead », *Journal of Cyber Policy*, vol. 2, n° 3, 2017, p. 2 : <https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1400084>.

328 M. Pisa and M. Juden, *Blockchain and Economic Development: Hype vs. Reality*, Center for Global Development, Washington, D.C., 2017, p. 8 : https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf.

14.1.3 LA BLOCKCHAIN EN PRATIQUE

Les chercheurs et les spécialistes considèrent que la technologie de la blockchain présente les avantages et les défis suivants³²⁹ :

Avantages :

- La présence d'un tiers de confiance (une autorité centrale) n'est pas nécessaire pour assurer l'intégrité d'un registre partagé : les transactions inscrites dans une blockchain sont vérifiées par les participants grâce à un mécanisme de consensus. L'étendue de cet avantage varie toutefois en fonction des modalités d'utilisation de la blockchain.
- L'absence de tiers de confiance réduit les coûts. Par exemple, une blockchain pourrait permettre de réaliser des transferts monétaires transfrontaliers directement entre les parties à une transaction ; il ne serait alors plus nécessaire de faire appel à une banque ou un autre établissement financier, souvent synonyme de frais.
- Une blockchain fonctionne comme une piste d'audit, la manière dont les données sont stockées et connectées pouvant permettre de retracer plus facilement l'origine et les mouvements des biens matériels liés à un jeton numérique³³⁰.
- La transparence est améliorée, particulièrement pour les blockchains publiques, car davantage de parties peuvent accéder au registre. Pour les blockchains privées, cet avantage peut cependant être moindre, voire parfois inexistant.
- Les blockchains augmentent l'intégrité et la disponibilité, car elles offrent une résilience opérationnelle et ne présentent pas de point unique de défaillance ou de compromission³³¹.

Défis :

- Une structure de gouvernance appropriée doit être identifiée pour chaque solution de blockchain.
- Bien que l'on considère que les blockchains ne requièrent pas de « tiers de confiance », certaines parties du système doivent néanmoins être considérées comme des entités de confiance. Il s'agit notamment des développeurs du code, ainsi que des concepteurs des applications qui interagissent avec la blockchain ou les services de cloud où peuvent être stockées les données.
- La blockchain augmente le nombre de points d'accès à travers lesquels des attaques peuvent être menées par des tiers malveillants, ce qui pose des risques pour la sécurité. Par ailleurs, certains mécanismes de consensus – bien que très peu utilisés – considèrent qu'une transaction est valide lorsque 51% des validateurs l'approuvent. De ce fait, si un consortium de validateurs prend le contrôle de 51% des nœuds, ils peuvent contrôler conjointement le registre.

³²⁹ Pour plus de détails, voir : M. Finck, 2018, et J. Bacon *et al.*, « Blockchain Demystified », Legal Studies Research Paper n° 268/2017, Queen Mary University of London, School of Law, 2017 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218.

³³⁰ Pisa et Juden, 2017, p. 9.

³³¹ D'autres caractéristiques de la technologie peuvent toutefois la rendre plus vulnérable aux attaques (voir les défis plus bas et la section 14.5.4 sur la sécurité des données).

- La technologie est tributaire d'une connexion Internet.
- Certaines blockchains, comme celles qui utilisent des protocoles de preuve de travail, consomment bien plus d'électricité que des technologies alternatives³³².
- Les individus doivent être informés (par le biais de notices d'information) du traitement qui est fait de leurs données personnelles et doivent pouvoir exercer leurs droits à cet égard (par exemple le droit de faire supprimer ou rectifier des données et celui de retirer leur consentement).
- Les blockchains privées à permission peuvent être plus adaptées pour certains types de programmes humanitaires (comme les programmes de transferts monétaires), car ces architectures impliquent un nombre limité de participants. Dans certains cas, cela peut toutefois mener à la réintroduction d'un tiers de confiance et à une diminution de la transparence.
- La compatibilité avec les exigences en matière de protection des données dans différentes juridictions est un problème (voir ci-dessous).
- Bien que la technologie de la blockchain puisse permettre d'augmenter la transparence dans de nombreux cas, elle ne résout pas les problèmes sous-jacents qui créent ce que l'on appelle des « mauvaises données » (*bad data*). Autrement dit, si quelqu'un enregistre des données peu fiables sur une blockchain, elles resteront peu fiables et le système ne pourra pas produire les avantages escomptés³³³.

Ces avantages et défis de la blockchain influencent grandement son utilisation. Les blockchains sont souvent utilisées pour gérer des historiques de transactions relatives à la propriété, la conservation ou la responsabilité d'actifs, tels que les cryptomonnaies. Elles sont également utilisées pour authentifier ou horodater des documents (certifications de chaînes d'approvisionnement, certificats numériques ou autres) et pour faire appliquer les conditions d'un contrat (à travers l'utilisation de contrats intelligents, ou *smart contracts*)³³⁴.

14.1.4 UTILISATIONS DANS LE SECTEUR HUMANITAIRE

Depuis peu, les organisations humanitaires se penchent sur les applications possibles de la blockchain et ont lancé des projets pilotes utilisant cette technologie³³⁵. Bien qu'il n'y ait que peu d'informations sur les avantages et les risques de cette

³³² Bacon *et al.*, 2018, p. 15.

³³³ Pisa et Juden, 2017, p. 49.

³³⁴ Ce chapitre ne traitera pas des contrats intelligents, qui sont une fonctionnalité de la blockchain. Pour plus d'informations sur les contrats intelligents, voir : M. Finck, « Smart Contracts as a Form of Solely Automated Processing Under the GDPR », *Max Planck Institute for Innovation & Competition Research Paper n° 19-01*, 2019a : <https://ssrn.com/abstract=3311370> ou <http://dx.doi.org/10.2139/ssrn.3311370>.

³³⁵ Pour plus d'informations concernant l'utilisation des blockchains dans le secteur humanitaire, voir : G. Coppi et L. Fast, *Blockchain and distributed ledger technologies in the humanitarian sector*, HPG Commissioned Report, 2019 : <https://cdn.odi.org/media/documents/12605.pdf>.

technologie, les applications suivantes ont été proposées pour les organisations humanitaires³³⁶ :

- **Programmes de transferts monétaires (PTM)**³³⁷ : la blockchain pourrait améliorer l'efficacité d'un PTM à travers l'utilisation d'un système d'enregistrement des transactions sécurisé et bien structuré qui, en retour, augmenterait la transparence et garantirait que les données stockées dans le système n'ont pas été altérées. L'application de la technologie de la blockchain aux PTM pourrait également permettre de réduire le coût des paiements en espèces numériques, augmenter leur efficacité et leur traçabilité, ainsi que leur interopérabilité entre plusieurs organisations. Cette technologie permettrait en outre de sécuriser davantage les transactions, puisqu'elle est réputée offrir une résilience opérationnelle et ne pas présenter de point unique de défaillance ou de compromission (voir section 14.5.4 pour plus d'informations sur la blockchain et la sécurité).
- **Optimisation et suivi des chaînes logistiques** : les chaînes d'approvisionnement humanitaires sont extrêmement complexes et dynamiques ; il est donc difficile d'assurer un suivi rigoureux. La technologie de la blockchain permettrait de rendre ces opérations plus transparentes. Par exemple, dans le cas de fournitures médicales, une blockchain pourrait contenir des enregistrements pratiquement immuables des dates et heures (horodatage) auxquelles les fournitures ont quitté l'entrepôt, ont quitté le pays d'origine, sont arrivées dans le pays de destination, ont été réceptionnées par la section locale de l'organisation humanitaire et sont arrivées à l'hôpital de destination. Comme une blockchain est un registre public, elle peut servir de plateforme de données transparente pour retracer l'origine, l'utilisation et la destination des fournitures humanitaires.
- **Suivi des financements des donateurs** : le suivi et la surveillance entre pairs des dons pourraient permettre de développer des modèles financiers ayant supprimé l'intermédiaire traditionnel³³⁸ (ou tiers de confiance³³⁹). Ces modèles pourraient réduire les coûts de transaction associés aux financements humanitaires internationaux et améliorer le suivi des dons, y compris ceux du grand public. La technologie de la blockchain pourrait toutefois être utilisée pour effectuer des dons de manière anonyme, ce qui pourrait constituer un problème pour les organisations humanitaires dont les politiques de financement sont plus strictes et requièrent l'identification des donateurs.

³³⁶ Exemples tirés de l'article de Ko et Verity, 2016.

³³⁷ Voir, par exemple : Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge (IFRC), *Learning Review: Blockchain Open Loop Cash Transfer Pilot Project*, 2018 : <https://www.alnap.org/help-library/blockchain-open-loop-cash-transfer-pilot-project>.

³³⁸ Ko et Verity, 2016, p. 13.

³³⁹ Finck, 2018, p. 18.

- **Compréhension commune des situations de conflit** : le protocole Whiteflag³⁴⁰ (utilisé par le CICR) vise à offrir un moyen de communication neutre à toutes les parties impliquées dans un conflit. Il est conçu pour fournir un système de messagerie permettant de partager en temps réel des informations sur les situations d'urgence, les dangers locaux, la présence de mines, les déplacements de population et d'autres problèmes, tout en ayant l'assurance que ces informations n'auront pas été altérées par un tiers malveillant. Dans ce dispositif, les participants n'ont pas besoin de se faire mutuellement confiance. Bien que le caractère public de ces informations puisse contribuer à localiser des civils et à évaluer le respect des principes de distinction et de proportionnalité dans les attaques, il peut aussi être utilisé pour cibler des groupes identifiés.

EXEMPLE :

Dans le cadre de son projet pilote de transfert de fonds en boucle ouverte à l'aide de la blockchain³⁴¹, la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge et la Croix-Rouge du Kenya ont utilisé cette technologie pour enregistrer les transferts monétaires en espèces effectués en faveur des bénéficiaires victimes de la sécheresse. L'objectif de ce pilote était d'évaluer l'utilisation et la valeur ajoutée de la blockchain dans le cadre des PTM. Les transferts eux-mêmes ont été effectués indépendamment de la blockchain, par l'intermédiaire d'un partenariat conventionnel avec un fournisseur de téléphonie mobile local et une société de gestion des informations. Néanmoins, l'utilisation d'une blockchain privée à permission a permis d'enregistrer les transactions de manière distribuée et pratiquement immuable, avec à la clé une plus grande transparence entre les participants (uniquement ceux qui avaient accès à la blockchain), la création d'une piste d'audit (grâce à l'horodatage des enregistrements) et une amélioration de la sécurité (du fait de l'absence d'un point unique de défaillance ou de compromission).

Deux défis de taille se sont présentés dans le cadre du projet. Premièrement, la modification des registres s'est avérée complexe, par exemple lors de l'annulation d'une transaction suite à une demande de paiement enregistrée par erreur. Deuxièmement, comme l'aide ne pouvait être fournie qu'après obtention du consentement des bénéficiaires, il est peu probable que celui-ci ait été donné de façon libre et éclairée³⁴².

³⁴⁰ Site du projet : <https://www.whiteflagprotocol.net>.

³⁴¹ IFRC, *Learning Review: Blockchain Open Loop Cash Transfer Pilot Project*, 2018.

³⁴² Voir [section 3.2: Consentement](#).

14.2 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

L'utilisation de la blockchain dans les programmes humanitaires peut présenter de nombreux défis en termes de protection des données qui ne se poseraient pas dans d'autres contextes. C'est l'une des raisons pour lesquelles il est important d'effectuer une analyse d'impact relative à la protection des données (AIPD) avant de mettre en place des systèmes de blockchain. Une AIPD peut permettre de déterminer si le déploiement d'un tel système est nécessaire et proportionné. Si l'organisation décide que c'est le cas, l'AIPD peut également permettre d'identifier, de gérer et de réduire les risques et les défis associés à l'utilisation de la blockchain. Il existe de nombreux modèles et documents concernant les AIPD³⁴³, mais aucun n'a été spécifiquement élaboré pour l'utilisation de la blockchain dans le contexte humanitaire. Les organisations doivent donc adapter les modèles d'AIPD existants ou concevoir de nouveaux modèles spécifiques aux blockchains³⁴⁴.

Une AIPD est un processus systématique et adaptatif qui couvre à la fois les questions générales relatives au traitement des données personnelles et les questions concernant l'utilisation d'un type spécifique de technologie (dans ce cas, celle de la blockchain). Comme mentionné plus haut dans ce chapitre, les blockchains présentent des avantages et des défis pour les organisations humanitaires. Dans la plupart des cas, malgré les avantages attendus, aucune amélioration concrète n'a été constatée. Lors du processus d'AIPD, les organisations humanitaires devraient donc clairement identifier les avantages, les défis et les risques associés à l'utilisation de la blockchain, par rapport aux autres technologies. Cette approche n'a rien de nouveau, mais elle est particulièrement importante lors de l'utilisation d'une technologie émergente comme la blockchain.

Compte tenu des différentes formes que peuvent prendre les blockchains, l'AIPD doit aussi couvrir les questions de gouvernance et de conception pour chaque application individuelle. En raison de la diversité des applications envisageables et de la complexité technique des blockchains, les organisations humanitaires peuvent aussi établir un cadre décisionnel pour les aider à déterminer s'il y a lieu d'utiliser la technologie de la blockchain, et le cas échéant définir les mesures de protection à prendre. Certains auteurs ont proposé des cadres décisionnels généraux pour

³⁴³ Voir, par exemple : Commission nationale de l'informatique et des libertés (CNIL), « Publication des lignes directrices du G29 sur les DPIA », 22 octobre 2019 : <https://www.cnil.fr/fr/ce-qu'il-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd> ; Bureau du Commissaire à l'information du Royaume-Uni, *Sample DPIA template*, 2018 : https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx?mc_phishing_protection_id=28047-br1tehqudu81ea0ar3q10.

³⁴⁴ Pour plus d'informations sur les modèles d'AIPD et leur conception, voir [chapitre 5](#).

la mise en œuvre d'une blockchain³⁴⁵. Ces modèles génériques ne tiennent toutefois pas compte des problèmes de protection des données que soulève l'utilisation de cette technologie dans le secteur humanitaire. C'est pourquoi un cadre décisionnel spécifique à la blockchain est joint en annexe à ce chapitre.

La réalisation d'une AIPD peut aussi être essentielle pour identifier une base juridique appropriée pour l'utilisation d'une blockchain. Le processus d'AIPD devrait tenir compte de l'impact qu'un type spécifique de blockchain (celui envisagé dans la situation en question) pourrait avoir sur les droits des personnes concernées et l'application des principes de protection des données. Cette analyse permettra aux organisations humanitaires de choisir la solution qui limitera au mieux les risques éventuels.

L'AIPD doit permettre aux organisations humanitaires d'avoir une vision claire de l'impact que la blockchain aurait sur la proportionnalité du traitement des données. Sur la base de cette analyse, une organisation sera en mesure de déterminer s'il existe des moyens moins intrusifs, comme les bases de données traditionnelles, pour répondre à ses besoins tout en présentant moins de risques pour les bénéficiaires.

En plus d'analyser la conception technique du système, le processus d'AIPD devrait également tenir compte des problématiques et principes détaillés aux sections 14.3 à 14.7 ci-dessous.

14.3 PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT

La protection des données dès la conception et par défaut implique de concevoir une opération, un programme ou une solution de traitement en y intégrant d'emblée les principes clés de la protection des données de manière à offrir à la personne concernée la meilleure protection possible pour ses données. Ces principes clés de la protection des données sont les suivants :

- licéité, équité et transparence ;
- limitation des finalités ;
- minimisation des données ;
- exactitude ;
- durée de conservation limitée ;
- intégrité et confidentialité (sécurité) ;
- responsabilité ;
- protection des droits des personnes concernées dès la conception.

³⁴⁵ K. Wüst et A. Gervais, « Do you need a Blockchain? », article présenté lors de la Crypto Valley Conference on Blockchain Technology (CVCBT), 2018 : <https://eprint.iacr.org/2017/375.pdf>.

Consulter le chapitre 2 pour obtenir une description générale de ces principes, dont certains sont mis en contexte dans les sections ci-dessous.

À ce stade, il est important de prendre en compte les différents types de blockchain, toutes les options devant être envisagées lors de la conception d'un modèle conforme aux principes de protection des données.

Les blockchains privées à permission (voir les définitions à la section 14.1.2) sont les plus restrictives, puisqu'une ou plusieurs parties définissent qui a le droit de valider des informations dans la blockchain et qui peut accéder aux données du registre. Il peut dès lors être plus facile de concevoir des blockchains privées à permission qui soient conformes aux principes de protection des données³⁴⁶. Dans certains cas, le fait de restreindre les droits des participants peut toutefois aller à l'encontre de l'objectif même de la technologie de la blockchain, en ayant pour effet de réintroduire un tiers de confiance et, potentiellement, un point unique de défaillance ou de compromission.

Les blockchains publiques doivent quant à elles être conçues de sorte à ne pas stocker de données personnelles (c'est toujours une option à privilégier, même pour les registres privés). Il est alors préférable de stocker les données personnelles « hors chaîne » (c'est-à-dire en dehors du registre). Dans ce cas, le registre public contient simplement un identifiant cryptographique qui confirme qu'un document ou une information spécifique a été stocké à un autre endroit (par exemple sur le serveur d'une organisation humanitaire³⁴⁷). Les données elles-mêmes ne sont pas conservées sur la blockchain. Toutefois, même avec cette conception, il est important de rappeler que les clés publiques des individus incluses dans la blockchain restent des données personnelles. Pour ce qui est de savoir si les identifiants cryptographiques constituent eux aussi des données personnelles, la question fait débat³⁴⁸.

346 M. Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*, Panel for the Future of Science and Technology, Service de recherche du Parlement européen (EPRS), 2019b, p. 1 : [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

347 Un identifiant cryptographique (ou pointeur de hachage) est la transformation mathématique unidirectionnelle d'une entrée donnée (un message ou un document) en une combinaison de lettres et chiffres d'une longueur fixe (sortie). À chaque fois qu'une entrée spécifique est hachée, la sortie est identique, mais toute modification de l'entrée (par exemple, ajout ou suppression d'une virgule) modifiera entièrement le pointeur de hachage (Pisa et Juden, 2017). L'ajout d'un pointeur de hachage à la blockchain permet ainsi à une personne de vérifier qu'un document a bien été stocké, puisqu'un nouvel hachage du document générerait le même pointeur que celui contenu dans le registre.

348 Finck, 2019b, p. 30.

14.4 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Les blockchains, en tant que registres distribués, peuvent impliquer une multitude d'organismes et d'entités. Par conséquent, il peut être complexe d'établir quelles parties doivent être considérées comme responsables du traitement et lesquelles doivent être considérées comme sous-traitants. À titre de précision, les rôles respectifs de chacun sont indiqués ci-dessous :

- Les **responsables du traitement** définissent les moyens et les finalités du traitement. Ils sont responsables du traitement des données personnelles et de la mise en œuvre des droits des personnes concernées. Ils doivent respecter les principes de protection des données et répondre aux demandes des individus portant sur l'exercice de leurs droits d'accès, de rectification et de suppression. Si plusieurs responsables du traitement sont impliqués dans la blockchain, ou si de nouveaux utilisateurs considérés comme responsables du traitement rejoignent la blockchain, leurs responsabilités respectives en matière de traitement des données devraient être définies dans un accord écrit.
- Les **sous-traitants** suivent les instructions des responsables du traitement et sont tenus d'assurer la sécurité des données. Ils doivent également informer les responsables du traitement des moyens utilisés pour traiter les données et de tout problème ou toute plainte relative à l'intégrité, la confidentialité et la disponibilité des données.

Chaque architecture de blockchain (voir section 14.1.2) peut avoir différentes implications sur la définition des rôles des différentes parties chargées du registre. Il est important de préciser que lors de l'identification du responsable du traitement, la détermination des finalités du traitement est plus importante que la sélection des moyens. Au regard de ce qui précède et des principales parties impliquées dans les blockchains, les situations suivantes peuvent être envisagées :

- Dans une blockchain à permission, il est possible d'identifier une partie centrale (ou intermédiaire) répondant à la qualification de responsable du traitement (par exemple l'opérateur système qui accorde les droits « d'écriture ») tandis que les nœuds seraient qualifiés de sous-traitants.
- Dans une blockchain sans permission, il n'y aura pas d'intermédiaire central, car le réseau est opéré par tous les nœuds de manière décentralisée. Chaque nœud peut ici répondre à la qualification de responsable du traitement, puisque chacun d'eux décide de manière autonome s'il souhaite rejoindre la chaîne pour les finalités établies³⁴⁹. Cette conclusion ne fait cependant pas l'unanimité.
- Certains affirment que les nœuds sont des responsables du traitement, car le fait de rejoindre un réseau de blockchain revient à définir les finalités du traitement³⁵⁰. D'autres estiment au contraire que les nœuds ne sont pas des

³⁴⁹ Finck, 2018, p. 26-27.

³⁵⁰ *Ibid.*, p. 26.

responsables du traitement³⁵¹. Il est également important de relever que les nœuds ne voient parfois que la version chiffrée des données et qu'ils utilisent un logiciel qui ne leur permet pas de modifier le registre. Ils ne peuvent donc pas « voir » les données qui sont traitées, y compris les données personnelles, ni les modifier, et sont dès lors dans l'impossibilité de respecter les obligations qui incombent aux responsables du traitement en matière de protection des données.

- Les utilisateurs (organisations ou particuliers qui décident d'utiliser la blockchain) peuvent, quant à eux, être qualifiés de responsables du traitement dans certains cas, car ils définissent clairement les finalités du traitement (par exemple l'enregistrement d'une information spécifique sur la blockchain³⁵²). En outre, ils déterminent les moyens du traitement lorsqu'ils sélectionnent un type spécifique de blockchain. Cette interprétation ne peut néanmoins pas s'appliquer à tous les types de blockchain. Elle peut être vraie pour les blockchains publiques sans permission, mais celles privées à permission sont généralement établies par un consortium d'organisations, qui seront alors les responsables conjoints du traitement.

La Commission nationale de l'informatique et des libertés (CNIL) s'est attachée à définir des orientations sur ce sujet. Selon la CNIL³⁵³ :

- Les participants qui ont un droit d'écriture sur la blockchain sont considérés comme responsables du traitement lorsque les données inscrites sont en lien avec une activité professionnelle.
- Les personnes morales qui inscrivent des données sur une blockchain sont considérées comme responsables du traitement.
- Les mineurs (ou les nœuds) qui n'ajoutent pas de données à la blockchain, mais se limitent à vérifier l'authenticité des données (en participant au protocole de consensus), ne sont pas des responsables du traitement, car ils ne déterminent pas les moyens et les finalités de ce dernier ; ils peuvent toutefois être considérés comme sous-traitants lorsqu'ils suivent les instructions du responsable du traitement.
- Les utilisateurs de la blockchain peuvent être subdivisés en deux groupes :
 - ceux qui utilisent la blockchain à des fins professionnelles ou commerciales sont qualifiés de responsables du traitement ;
 - ceux qui utilisent le registre à des fins privées ne sont pas des responsables du traitement, car il s'agit là d'une activité purement personnelle qui n'est pas couverte par la plupart des législations en matière de protection des données.

³⁵¹ Bacon *et al.*, 2017, p. 64-65.

³⁵² *Ibid.*, p. 64.

³⁵³ CNIL, « La Blockchain : quelles solutions pour un usage responsable en présence de données personnelles ? », 2018 : https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

Compte tenu des différentes interprétations et orientations sur ce sujet, les organisations humanitaires souhaitant utiliser la technologie de la blockchain doivent veiller à ce que la gouvernance de la solution choisie intègre les concepts de responsable du traitement et de sous-traitant. Elles doivent aussi déterminer, le plus clairement possible, les responsabilités de chaque partie dans le cadre d'une activité de traitement donnée. Lorsque les responsables du traitement ne peuvent pas remplir leurs obligations dans une situation spécifique (s'agissant en particulier de permettre aux personnes concernées d'exercer leurs droits), une solution alternative doit être recherchée, du moment que l'utilisation de la blockchain sera vraisemblablement incompatible avec les principes de protection des données.

14.5 PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

Comme expliqué plus haut, il peut être problématique de concilier l'utilisation de la blockchain et les principes fondamentaux de la protection des données. En pratique, leur compatibilité dépend de l'architecture et de la conception de chaque solution de blockchain. Si cette section fournit des orientations générales, les organisations doivent, elles, tenir compte des caractéristiques propres à chaque application lors de l'analyse de compatibilité avec les principes de protection des données.

14.5.1 MINIMISATION DES DONNÉES

De par leur nature, les registres distribués apparaissent contraires au principe de minimisation des données, selon lequel il convient de limiter la quantité de données personnelles traitées au minimum nécessaire pour atteindre l'objectif et les finalités du traitement³⁵⁴. Cela tient notamment au fait que les données des blockchains peuvent être stockées de manière perpétuelle et qu'une copie de l'ensemble du registre est stockée sur plusieurs nœuds et sur de nombreux appareils. Il existe néanmoins des expédients. Les données personnelles peuvent être stockées hors de la blockchain, tandis que le registre ne conserve qu'un identifiant cryptographique des données stockées ailleurs. Dans ce cas, les données ne seront pas stockées de manière perpétuelle sur le registre ni partagées avec tous les nœuds. L'individu ou l'organisation qui stocke les données gardera le plein contrôle sur celles-ci et pourra ainsi appliquer le principe de minimisation des données au traitement effectué hors chaîne, et ce, sans modifier le registre lui-même. Pour ce qui de savoir si les identifiants cryptographiques constituent eux aussi des données personnelles, la question fait débat³⁵⁵.

354 Par exemple, conformément au Règlement général sur la protection des données (RGPD), article 5, point 1.c) et e), les données personnelles doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » et « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

355 Finck, 2019b, p. 30.

14.5.2 CONSERVATION DE DONNÉES

Le fait que les blockchains soient assimilées à des registres immuables et distribués constitue un problème au regard du principe de conservation des données³⁵⁶. Les données stockées sur une blockchain seront conservées sur plusieurs ordinateurs pour une période indéterminée. Dans ce cas, il est préférable de ne stocker aucune donnée personnelle dans les blockchains. Les données personnelles ne devraient par exemple pas être stockées dans des registres publics, ce type de blockchain étant accessible (lisible) à tous. C'est d'autant plus vrai pour les données personnelles particulièrement sensibles, comme les données sur l'origine ethnique ou les données médicales, qui ne devraient en aucun cas être stockées dans des blockchains.

14.5.3 PROPORTIONNALITÉ

La proportionnalité est un principe fondamental de la protection des données. Il exige généralement d'examiner si une action ou mesure liée au traitement de données personnelles est appropriée au regard de l'objectif visé. La proportionnalité suppose de définir des options et de choisir la moins intrusive eu égard aux droits des personnes concernées. Du fait de la complexité des blockchains, il peut toutefois être difficile de déterminer si une solution spécifique est proportionnée.

Comme pour les principes de minimisation et de conservation des données, une manière d'assurer le respect du principe de proportionnalité dans le cas d'une blockchain sans permission pourrait être de stocker les données personnelles hors chaîne. Cela dit, l'ajout d'une base de données hors chaîne peut entraîner la réintroduction d'un tiers de confiance (par exemple le fournisseur de services cloud chargé du stockage des données) et annuler ainsi les avantages attendus de l'utilisation de la blockchain. L'exigence de proportionnalité pourrait toutefois être respectée si les caractéristiques de la blockchain sont essentielles pour atteindre l'objectif prévu (par exemple lorsqu'il est primordial d'améliorer l'intégrité, la transparence et la disponibilité d'une solution existante) et si l'utilisation d'un modèle de base de données centralisée ne permet pas d'atteindre cet objectif (par exemple car les parties ne se font pas confiance). En tout état de cause, les risques pour les personnes concernées ne peuvent pas être exagérément élevés par rapport aux objectifs visés.

14.5.4 SÉCURITÉ DES DONNÉES

La sécurité des données est un aspect fondamental d'un système efficace de protection des données³⁵⁷. La sécurité est souvent liée à trois principes clés :

- **la confidentialité** : seules les parties autorisées doivent pouvoir accéder aux données ;
- **l'intégrité** : les parties non autorisées ne doivent pas pouvoir modifier les données, et les données ne doivent pas être perdues, détruites ou altérées ;

³⁵⁶ Voir [section 2.7 : Conservation des données](#).

³⁵⁷ Voir [section 2.8 : Sécurité des données et sécurité du traitement](#).

- **la disponibilité** : les données doivent pouvoir être mises à disposition (des parties autorisées) en cas de besoin.

La blockchain présente aussi bien des forces que des faiblesses au niveau de ces trois aspects de la sécurité, comme détaillé ci-après.

Pour ce qui est de la confidentialité, la nature distribuée des blockchains signifie que les mêmes données sont potentiellement reproduites et distribuées de manière large, ce qui implique une multiplication des points d'accès et des vulnérabilités. De plus, même si un système de blockchain utilise un chiffrement et des techniques de hachage complexes, les avancées dans le domaine de l'informatique quantique font que des informations pourraient être déchiffrées même sans clé de déchiffrement. Si, à l'avenir, le chiffrement ne devait plus garantir la sécurité et l'anonymat des données, toutes les données personnelles stockées sur des blockchains publiques pourraient être exposées. Les dommages pourraient alors être irréversibles, car les données stockées sur une blockchain ne peuvent généralement pas être supprimées. C'est une raison de plus pour laquelle il n'est pas recommandé de stocker des données personnelles sur la blockchain elle-même.

Concernant l'intégrité, le caractère immuable de la technologie de la blockchain et l'utilisation des protocoles de consensus offrent un avantage en termes de sécurité par rapport aux bases de données centralisées, en particulier parce que « le stockage de données sensibles sur des serveurs centralisés crée un effet “pot de miel” pour les pirates de tous bords et un point unique de défaillance³⁵⁸ ». Les blockchains ne présentent en revanche pas de point unique de défaillance ou de compromission et, à moins qu'un pirate n'arrive à contrôler suffisamment de nœuds pour contrôler aussi le protocole de consensus, le système a peu de chance d'être compromis.

Quant à la disponibilité, la blockchain présente là encore un avantage, car il s'agit d'un registre distribué et stocké sur plusieurs ordinateurs en même temps.

La résistance à un point unique de défaillance ou de compromission est fréquemment présentée comme la principale valeur ajoutée de la blockchain en termes de sécurité. Si ce n'est pas un impératif pour l'organisation, le choix d'une technologie traditionnelle autre que la blockchain peut s'avérer plus efficace, plus rapide et moins onéreuse. Par exemple, les techniques de partage de secret, réputées renforcer la protection des données chiffrées dans les registres distribués, peuvent être appliquées également aux bases de données traditionnelles ; leur usage n'est pas réservé aux blockchains. La technologie de la blockchain apporte ainsi une valeur ajoutée lorsque l'intégrité et la disponibilité sont fondamentales et que les participants ne se font pas confiance.

³⁵⁸ Pisa et Juden, 2017, p. 6.

14.6 DROITS DES PERSONNES CONCERNÉES

Les personnes concernées disposent de certains droits qui leur permettent de garder le contrôle sur leurs données personnelles. Comme expliqué ci-dessous, il peut cependant être difficile, voire impossible, d'un point de vue technique d'exercer ces droits dans le cadre de la blockchain.

14.6.1 DROIT D'ACCÈS

Les individus ont le droit de savoir si leurs données personnelles sont traitées par le responsable du traitement et d'obtenir une copie des données personnelles en question³⁵⁹. Dans le secteur humanitaire, lorsque des données personnelles sont stockées sur une blockchain, les organisations humanitaires devraient donc toujours participer en tant que nœuds et disposer d'une copie de l'ensemble du registre. De cette manière, elles peuvent s'assurer que l'ensemble de la base de données est disponible en tout temps et informer les bénéficiaires dont les données sont stockées sur la blockchain.

En revanche, lorsque des données personnelles sont stockées hors chaîne, le registre ne contient qu'un identifiant pointant vers les données hors chaîne. Dans ce cas, le scénario le plus probable est que les organisations humanitaires stockent elles-mêmes les données afin de pouvoir répondre aux demandes des personnes concernées conformément aux obligations juridiques.

14.6.2 DROIT DE RECTIFICATION

Les personnes concernées ont le droit d'exiger la correction de données erronées³⁶⁰. Dans une blockchain, la rectification d'informations peut néanmoins s'avérer problématique, car il est techniquement très difficile, mais pas impossible, de modifier des données une fois ajoutées au registre³⁶¹ (d'où l'emploi du terme « immuable »).

Si des données personnelles sont stockées sur la blockchain, une manière d'exercer ce droit consiste à ajouter de nouvelles données corrigées (comme instruction supplémentaire), tout en rendant les anciennes données inaccessibles (par exemple en supprimant la clé de déchiffrement nécessaire pour accéder aux données incorrectes). Cette solution ne fait cependant pas l'unanimité parmi les spécialistes et les chercheurs. Dans certains cas, il est également possible d'insérer une nouvelle

³⁵⁹ Voir [section 2.11: Droits des personnes concernées](#).

³⁶⁰ Voir [section 2.11: Droits des personnes concernées](#).

³⁶¹ D. Conte de Leon *et al.*, « Blockchain: properties and misconceptions », *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 11, n° 3, 2017 : https://www.researchgate.net/publication/321811785_Blockchain_properties_and_misconceptions. Voir aussi l'exemple du hard fork de la blockchain Ethereum pour contrer l'attaque de la DAO : <https://blog.ethereum.org/2016/07/20/hard-fork-completed/>.

transaction indiquant que les anciennes données doivent être corrigées. Néanmoins, le problème avec ces options est qu'au lieu de corriger les données d'origine, elles ne font qu'ajouter des données supplémentaires à la chaîne. De ce fait, il n'est pas certain que ces solutions puissent être acceptées comme des rectifications.

Compte tenu de ces limites, le meilleur moyen de faire face à ces difficultés est de stocker les données personnelles hors chaîne, où il est possible de les rectifier sans altérer le registre. Il convient toutefois de souligner que cette option réduirait grandement les avantages procurés par l'intégrité et à la disponibilité des blockchains, dont il a été question plus haut. Autrement dit, si l'intégrité et la disponibilité sont également importantes pour les données personnelles, l'utilisation d'une solution reposant sur des blockchains n'est alors pas recommandée.

14.6.3 DROIT DE SUPPRESSION

La nature presque immuable de la blockchain s'oppose sur le plan conceptuel au droit de suppression³⁶². Différentes options ont été proposées pour pallier ce problème. L'une d'elles, comme mentionné plus haut, est de rendre les données inaccessibles sur la chaîne, bien que toujours présentes. Pour ce faire, il est par exemple possible de supprimer la clé de déchiffrement nécessaire pour décrypter les données chiffrées. Cependant, certains chercheurs et spécialistes jugent cette approche insatisfaisante, car les données personnelles en question, bien que chiffrées, ne sont pas supprimées (comme le prévoit le droit de suppression), mais simplement rendues inaccessibles. Cela peut être problématique compte tenu des avancées des technologies de déchiffrement (voir l'analyse sur la sécurité des données plus haut).

Comme les données personnelles stockées hors chaîne peuvent être rectifiées et supprimées conformément aux exigences en matière de protection des données et sans altérer le registre distribué lui-même, le stockage hors chaîne est, là encore, l'option à privilégier.

³⁶² Finck, 2018, p. 30.

EXEMPLE :

Si une organisation humanitaire utilise la technologie de la blockchain pour un programme de transfert monétaire, elle demandera certainement aux bénéficiaires de créer un « portefeuille » sur la blockchain. Le fonctionnement d'un portefeuille est très similaire à celui d'une clé publique, c'est-à-dire qu'il peut être comparé à un nom d'utilisateur qui, à lui seul, ne permet pas d'identifier le bénéficiaire. Toutefois, l'organisation devra probablement maintenir hors chaîne une base de données ou un système de gestion des bénéficiaires reliant chaque portefeuille à un bénéficiaire unique.

Chaque fois qu'un transfert monétaire est effectué en faveur d'un bénéficiaire, une transaction sera ajoutée à la blockchain, précisant le montant du transfert, le portefeuille utilisé et la date de la transaction. Une fois la transaction validée par le protocole de consensus, elle sera stockée de manière immuable dans la blockchain. Si les bénéficiaires demandent la suppression de leurs données, il est techniquement impossible de supprimer leur portefeuille (qui constitue des données personnelles, au même titre qu'une clé publique) de la chaîne. Dans ce cas, une option serait de retirer la personne de la base de données ou du système de gestion hors chaîne, puisque c'est le seul endroit où le portefeuille est associé à un individu. Une fois le profil personnel supprimé, il ne devrait plus être possible de réidentifier l'individu.

14.6.4 RESTRICTIONS DES DROITS DES PERSONNES CONCERNÉES

L'analyse qui précède sur les droits d'accès, de suppression et de rectification montre à quel point il est difficile d'exercer ses droits relatifs à la protection des données lors de l'utilisation de la technologie de la blockchain. Comme les blockchains publiques sans permission sont, pour la plupart, incompatibles avec les droits des personnes concernées, la seule solution semble être de stocker les données personnelles hors chaîne. Néanmoins, ces droits ne sont pas absolus et peuvent parfois être restreints. Le responsable du traitement est autorisé à tenir compte de la technologie disponible et des coûts de mise en œuvre lorsque des personnes concernées demandent à exercer leurs droits. Il est toutefois important de souligner que ces restrictions ne sont acceptables que dans des cas exceptionnels³⁶³. Le chapitre 2 de ce manuel explique et illustre les situations dans lesquelles les droits des personnes concernées peuvent être restreints. Des doutes subsistent quant à la possibilité d'avoir une blockchain « conforme à la protection des données » lorsque le traitement implique des dérogations légitimes aux droits des personnes concernées. En outre, même lorsque la restriction de certains droits est jugée légitime, tous les autres principes de la protection des données (minimisation, nécessité, proportionnalité, sécurité, etc.) demeurent applicables.

363 Voir [section 2.11 : Droits des personnes concernées](#).

14.7 TRANSFERT INTERNATIONAL DE DONNÉES

Les données traitées dans les blockchains traversent couramment les frontières – en particulier lorsqu’il s’agit d’architectures publiques sans permission, auxquelles quiconque peut potentiellement accéder depuis n’importe où. Cela soulève des questions quant à la protection des données de la blockchain lors d’un transfert international³⁶⁴. Malgré l’existence de clauses contractuelles et d’autres mécanismes reconnus, de telles mesures peuvent être pratiquement impossibles à mettre en œuvre dans une blockchain.

La détermination du droit et de la juridiction applicables peut également s’avérer complexe, du moment qu’une analyse de risque adéquate et ciblée, comme prévu au chapitre 4 de ce manuel, est impossible à réaliser – sauf si le choix de la juridiction et du droit est clairement ancré dans la gouvernance de la blockchain (c’est le cas par exemple des blockchains privées à permission qui limitent l’emplacement géographique de ceux qui peuvent rejoindre la chaîne).

Les transferts internationaux peuvent être problématiques avec certains types de blockchain, par exemple les blockchains publiques sans permission qui ne sont pas limitées, comme celle utilisée par le bitcoin (une cryptomonnaie). Dans ce cas, aucune partie centrale ne contrôle qui participe au système et ne stocke une copie d’un registre. Les blockchains privées à permission et d’autres architectures offrent néanmoins plus de contrôle et permettent ainsi de limiter ces risques. Par conséquent, il est possible de gérer le problème des transferts à travers la gouvernance des blockchains, par exemple en y intégrant des garanties de protection des données (notamment en les codant en dur dans l’architecture des blockchains).

Les responsables du traitement doivent également informer les personnes concernées du partage de leurs données avec d’autres parties ou de leur transfert vers un pays tiers. Cela est généralement impossible – à quelques exceptions près – avec les blockchains publiques sans permission, puisque quiconque pourrait rejoindre le système et stocker une copie du registre. En revanche, dans le cas des blockchains à permission, les responsables du traitement ont davantage de contrôle et devraient partant pouvoir respecter cette exigence.

³⁶⁴ Voir [chapitre 4 : Transfert international de données](#).

PIÈCES JOINTES : CADRE DÉCISIONNEL POUR L'UTILISATION DE LA BLOCKCHAIN DANS L'ACTION HUMANITAIRE

Le cadre décisionnel suivant vise à orienter les organisations humanitaires au cours du processus de mise en œuvre des blockchains dans l'action humanitaire :

Étape 1 :

Cette étape est commune au déploiement de toute nouvelle technologie et n'est pas exclusive à la blockchain. Elle consiste à collecter des informations et définir le champ d'application en vue de répondre aux questions suivantes :

- Quel problème une solution de blockchain permettrait-elle de résoudre ?
- Dans le cadre de quel programme sera-t-elle appliquée et quels sont les besoins du programme ?
- Un système de blockchain est-il la technologie la moins invasive, la moins risquée et la plus facile à contrôler qui soit disponible pour gérer ce problème particulier ?
- Dans quel contexte la blockchain fonctionnera-t-elle ?
- Où fonctionnera-t-elle (dans un pays ou une région, ou à l'international) ?
- Qui sont les parties prenantes (bénéficiaires, autorités locales, partenaires financiers, opérateurs mobiles, autres organisations humanitaires, etc.) ?
- Quels sont les objectifs de la technologie (augmentation de l'efficacité interne, amélioration du positionnement, développement de programmes existants, respect des exigences des donateurs, gestion des risques, etc.) ?
- Quelles sont vos dispositions actuelles en termes de gouvernance et vos capacités informatiques ? La technologie peut-elle être mise en place et est-il possible de gérer les risques associés compte tenu des dispositions et capacités actuelles ?
- La manière dont la technologie contribuera à l'écosystème d'information local est-elle claire ?

Étape 2 :

Il convient d'établir si un système basé sur la blockchain est nécessaire pour atteindre les objectifs d'un programme humanitaire ou d'une autre initiative, en tenant compte des avantages et des défis associés à cette technologie (tels que mentionnés plus haut) dans le contexte particulier où elle sera mise en œuvre. Votre organisation doit veiller à déterminer quels sont ses besoins, si une blockchain pourra y répondre, quel sera l'impact du système sur les personnes concernées, comment leurs droits pourront être respectés et si un autre système protégeant davantage les personnes concernées et leurs droits pourrait répondre à ces mêmes besoins. Il faut se poser les questions suivantes :

- L'ordre des (trans)actions est-il important ?
- Existe-t-il une autorité centrale en laquelle vous pouvez avoir confiance ?
- Avez-vous besoin de stocker des données ?

- Avez-vous le soutien de votre équipe de gouvernance/support informatique?
- Comprenez-vous comment votre système contribuera à l'écosystème d'information local?

Étape 3:

Si votre organisation détermine qu'elle ne peut atteindre son objectif que grâce à une solution de blockchain, vous devez déterminer quel type de blockchain est le plus approprié ou nécessaire. Il faut se poser les questions suivantes:

- Plusieurs contributeurs sont-ils impliqués?
- Pouvez-vous utiliser un tiers de confiance «connecté en permanence»?
- Connaissez-vous tous les contributeurs?
- Faites-vous confiance à tous les contributeurs?
- Une vérifiabilité publique est-elle nécessaire?

Étape 4:

Consulter le service de la protection des données, l'équipe de support informatique et des pairs:

- Demander conseil.
- Mettre à profit l'expérience des autres. Par exemple, il est utile de contacter des pairs qui ont développé un système similaire ou utilisé la solution standard que vous envisagez de mettre en œuvre, et de demander conseil à des spécialistes de la blockchain.

Étape 5:

Effectuer une AIPD pour identifier et évaluer les conséquences du traitement des données personnelles. Une AIPD doit notamment inclure les questions suivantes:

- Quel est le droit applicable? S'applique-t-il à toutes les parties prenantes?
- Quels types de données personnelles sont traités? Parmi ces types, lesquels sont nécessaires pour la transaction stockée sur la blockchain?
- Le traitement est-il équitable, licite et transparent?
- Quelles sont les alternatives au stockage de données personnelles sur la blockchain elle-même? Un stockage hors chaîne est-il possible?
- Toutes les personnes concernées peuvent-elles exercer pleinement leurs droits? Si non, les restrictions sont-elles légales et proportionnées?
- Qui a le pouvoir de définir la gouvernance de la blockchain?
- Comment fonctionne la plateforme?
- Qui peut modifier la plateforme et dans quels cas est-il possible de mettre à jour des entrées du registre?
- Quels sont les risques posés par la technologie choisie? Comment chaque risque sera-t-il traité et atténué?
- Comment les individus peuvent-ils exercer leurs droits?

Étape 6 :

Mettre en œuvre les principes de la protection des données dès la conception et par défaut :

- Ces deux principes exigent une surveillance et une révision continues des mesures techniques et organisationnelles, en tenant compte des éléments suivants : la technologie disponible ; le coût de mise en œuvre ; la nature, la portée et le contexte du traitement ; les finalités du traitement et les risques (de probabilité et de gravité variables) pour les droits et libertés des personnes physiques que pose le traitement. Une nouvelle AIPD devrait être effectuée en cas de changement important au niveau de la technologie utilisée ou du type de données collectées.
- La protection des données dès la conception implique la prise en compte de facteurs tels que :
 - la conformité aux principes de la protection des données (licéité, équité et transparence, limitation de(s) la finalité(s), minimisation des données, exactitude, limitation de la durée de conservation, intégrité et confidentialité) ;
 - les droits des personnes concernées (par exemple, droit à l'information, droit d'accès, de suppression et de rectification) ;
 - toute autre obligation en matière de protection des données (par exemple, responsabilité et sécurité).
- La protection des données par défaut implique la prise en compte de facteurs tels que :
 - les types et catégories de données personnelles stockées ;
 - la quantité de données personnelles traitées ;
 - les finalités pour lesquelles elles sont traitées ;
 - la durée de conservation ;
 - l'accessibilité.

À l'étape de la collecte d'informations, si votre organisation arrive à la conclusion que d'autres systèmes sont plus appropriés que la blockchain, il est inutile d'aller plus loin que l'étape 1.

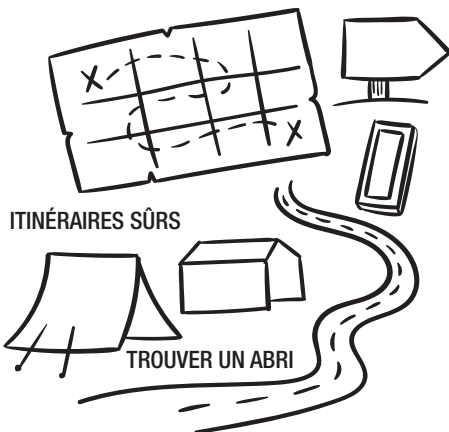
CONNECTIVITÉ COMME FORME D'AIDE



UTILISATION POSSIBLE



GARDER CONTACT
AVEC LES MEMBRES
DE LA FAMILLE



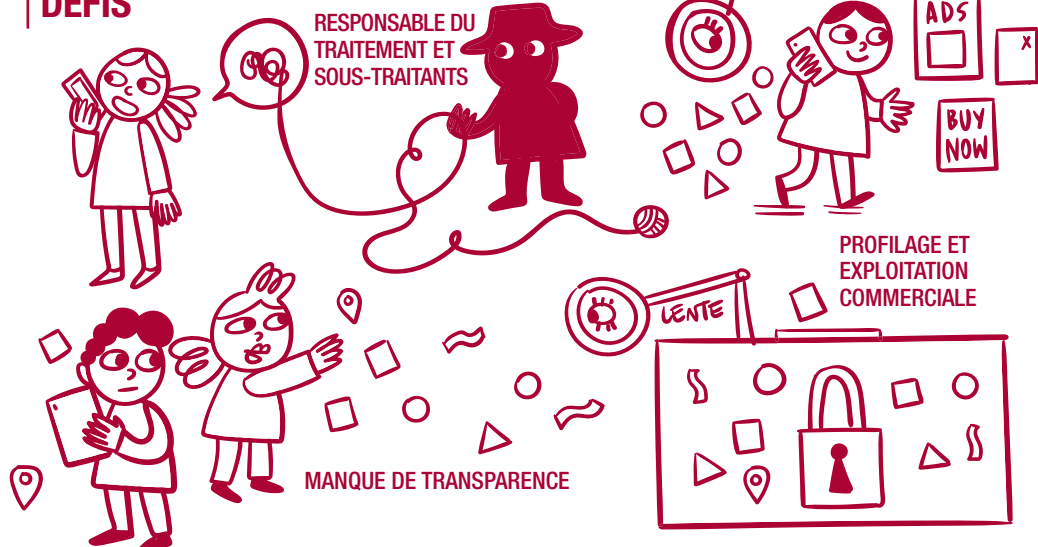
ITINÉRAIRES SÛRS

TROUVER UN ABRI

SERVICES HUMANITAIRES



DÉFIS



RESPONSABLE DU
TRAITEMENT ET
SOUS-TRAITANTS

SURVEILLANCE

PROFILAGE ET
EXPLOITATION
COMMERCIALE

MANQUE DE TRANSPARENCE

VENTE

CHAPITRE 15

CONNECTIVITÉ COMME FORME D'AIDE³⁶⁵

365 Les auteurs souhaitent remercier Robert Riemann (Contrôleur européen de la protection des données) et John Warnes (HCR) pour leur participation à la rédaction de ce chapitre.

15.1 INTRODUCTION

Dans les situations d'urgence, le fait de rester connecté peut aider les bénéficiaires à établir le contact avec des proches dont ils ont été séparés, à identifier des itinéraires sûrs, à trouver des abris, à interagir avec des organisations humanitaires et à obtenir une assistance humanitaire ou d'autres services. Cela dit, après une catastrophe, les réseaux de télécommunications sur lesquels repose la connectivité³⁶⁶ cessent souvent de fonctionner, empêchant les personnes touchées d'utiliser les canaux de communication dont ils dépendent de plus en plus. Les observations ont montré que les bénéficiaires attachent une grande importance à la connectivité. Par exemple, en 2016, des travailleurs humanitaires venant en aide aux migrants en Grèce ont indiqué que l'accès à Internet était souvent la première chose qu'on leur demandait, avant même la nourriture et l'eau³⁶⁷. Les organisations humanitaires reconnaissent l'importance de la connectivité et ont conçu divers programmes en conséquence.

Il est important de faire la différence entre la connectivité *comme forme d'aide* et la connectivité *pour l'aide*. Cette dernière désigne la connectivité qui permet aux travailleurs humanitaires de mener leurs activités, tandis que la première se réfère à la connectivité et aux services connexes qui sont fournis aux personnes touchées et qui, en tant que tels, sont une forme d'aide dans les situations d'urgence ou de crise prolongée.

Ce chapitre est centré sur les problèmes de protection des données découlant de la connectivité *comme forme d'aide*, à deux niveaux : communautaire et individuel. Au niveau communautaire, les organisations humanitaires installent généralement des bornes wifi ou offrent des services de connexion dans les centres communautaires. Dans ce cas, les organisations gèrent généralement les infrastructures physiques, comme les câbles et les faisceaux de fibres nécessaires pour offrir la connectivité, que les utilisateurs se partagent. Au niveau individuel, les organisations humanitaires peuvent aider les individus dans leurs échanges avec les fournisseurs de connectivité, mais ce sont les individus eux-mêmes qui sont responsables de leur connectivité³⁶⁸. La distinction entre ces deux niveaux a également des répercussions sur la responsabilité des organisations humanitaires en matière de protection des données.

366 Aux fins de ce chapitre, le terme « connectivité » désigne l'accès aux connexions mobiles et Internet.

367 L. Taylor, « Internet Is As Important As Food And Water To Refugees In Greece: Aid Groups », HuffPost, 22 juillet 2016 : https://www.huffpost.com/entry/internet-is-as-important-as-food-and-water-to-refugees-in-greece_n_57928a22e4b02d5d5ed1ac5b.

368 Voir, par exemple : UNHCR's Connectivity for Refugees initiative, Connections, 2019.

15.1.1 PRÉSENTATION DE LA CONNECTIVITÉ COMME OFFRE D'ASSISTANCE

Diverses initiatives et organisations œuvrent pour offrir une connectivité dans les situations d'urgence et éliminer les points noirs (black spots). Voici quelques exemples :

- **NetHope**³⁶⁹ fournit des moyens permettant une connectivité dans divers contextes d'urgence. Conjointement avec l'agence USAID, NetHope offre une connexion Internet à haut débit dans des zones rurales au Moyen-Orient, en Afrique (Botswana, Ghana, Kenya, Libéria, Nigéria et Zambie), en Asie (Cambodge et Indonésie) et aux Caraïbes (Jamaïque).
- L'**Emergency Telecommunications Cluster (ETC)** est un réseau d'organisations qui collaborent afin de fournir des services de communication partagés dans des situations d'urgence humanitaire. L'ETC est l'un des 11 groupes formés par l'Inter-Agency Standing Committee (IASC, Comité permanent interinstitutions)³⁷⁰.
- L'initiative **Connectivity for Refugees** du HCR aide les personnes déplacées et les communautés d'accueil à bénéficier d'une connectivité, en adoptant une approche fondée sur les droits humains et centrée sur l'inclusion dans les systèmes nationaux.
- Initiatives du secteur privé :
 - **Loon**³⁷¹ est une initiative lancée à l'origine par Google pour connecter les individus ; l'idée est de lâcher des ballons contenant les composants essentiels des tours de communication pour assurer un accès Internet dans les zones non couvertes par les réseaux actuels. Le projet vise à élargir la portée de la 4G haut débit sans fil (ou Long Term Evolution, LTE) en collaborant avec les opérateurs de réseau mobile.
 - **Facebook Connectivity**³⁷² est également partie prenante dans de nombreuses initiatives, par exemple l'application Free Basics, qui vise à offrir un accès Internet gratuit partout dans le monde, et High Altitude Connectivity, qui favorise l'utilisation de systèmes de connectivité par des plateformes de haute altitude (HAPS) et des technologies satellite pour offrir une connectivité aux zones reculées, et ce à moindre coût.
 - **Tactical Operations (TacOps) de CISCO**³⁷³ déploie une variété de technologies et d'équipements réseau pour fournir, à la suite de catastrophes, des moyens de télécommunication gratuits aux organisations humanitaires et à leurs bénéficiaires. Par exemple, après le séisme de magnitude 8.1 qui s'est produit au Népal en 2015, Cisco TacOps est arrivé sur place 72 heures après la catastrophe pour rétablir les communications.

³⁶⁹ <https://nethope.org>.

³⁷⁰ <https://www.etcluster.org>.

³⁷¹ <https://loon.com>.

³⁷² <https://connectivity.fb.com>.

³⁷³ https://www.cisco.com/c/fr_fr/index.html.

15.1.2 CONTEXTE OPÉRATIONNEL

Lors de la mise en œuvre d'un programme centré sur la connectivité comme forme d'aide, il est important de garder à l'esprit que les crises sont des situations complexes et que les circonstances et les personnes touchées diffèrent d'une crise à l'autre. De la même façon, les programmes de connectivité varient selon le contexte. Pour certains, l'objectif sera de renforcer la résilience du réseau existant en prévision de futures catastrophes naturelles ou urgences. Pour d'autres, l'accent sera mis sur la fourniture d'une connectivité dans des zones blanches (c'est-à-dire desservies par aucun réseau). Les modalités pratiques différeront inévitablement, mais les organisations devront tenir compte de certains facteurs communs, quel que soit le type de programme mis en œuvre. Le premier est l'environnement réglementaire, qui déterminera ce que l'organisation peut et ne peut pas faire. Le second est la présence d'organisations commerciales et non commerciales offrant déjà une connectivité dans la zone. En effet, les organisations humanitaires collaborent souvent avec des entités du secteur privé sur tout ou partie de la chaîne de connectivité et, puisque ces partenariats sont devenus de plus en plus courants, les organisations des deux secteurs ont élaboré des lignes directrices sur les modalités de cette collaboration³⁷⁴.

Lorsqu'elles envisagent un partenariat avec d'autres entités (voir section 15.1.3 ci-dessous), les organisations humanitaires ont intérêt à toujours évaluer les risques qu'il comporte. Pour ce faire, elles peuvent effectuer une analyse d'impact relative à la protection des données (AIPD) – qui ne se limite pas aux questions de protection des données (voir section 15.2 ci-dessous) et vise à garantir que le partenariat ne portera pas préjudice aux personnes touchées.

15.1.3 MULTIPLES PARTIES PRENANTES ET PARTENARIATS

Les organisations humanitaires ne disposent pas toujours de l'expertise, la technologie ou l'équipement nécessaires pour mettre en œuvre un programme à elles seules. Cela signifie que, si elles veulent atteindre leurs objectifs, elles devront potentiellement travailler en partenariat avec un ou plusieurs fournisseurs de technologies ou de connectivité. Il peut s'agir d'organismes à but non lucratif, d'entreprises privées (par exemple des opérateurs de télécommunications ou des sociétés de technologies) et d'ONG qui offrent des solutions de connectivité dans des situations d'urgence.

En plus de tenir compte des autres parties impliquées, il est aussi important de comprendre que la fourniture de connectivité peut être un processus sur plusieurs niveaux. Comme mentionné plus haut, il en existe deux : communautaire et individuel. Au niveau individuel, les bénéficiaires portent une plus grande

³⁷⁴ Voir, par exemple : GSM Association (GSMA), « Humanitarian Connectivity Charter » : <https://www.gsma.com/mobilefordevelopment/mobile-for-humanitarian-innovation/humanitarian-connectivity-charter>.

responsabilité quant à leurs choix de connectivité, puisque les opérateurs peuvent collecter des données directement auprès d'eux.

Une fois la connectivité établie, des services supplémentaires (aussi appelés « over-the-top ») sont proposés, comme des services de médias sociaux associés à un contrat de téléphonie, des portefeuilles mobiles ou l'argent mobile. Certains fournisseurs de ces services peuvent offrir leurs produits directement aux personnes qui bénéficient d'une assistance humanitaire. Bien que les bénéficiaires agissent ici comme des consommateurs, ils sont en réalité plus vulnérables qu'un consommateur normal. Il y a également des parties moins visibles qui sont impliquées dans les programmes de connectivité, comme les fournisseurs d'infrastructures et ceux qui travaillent sur le réseau de raccordement pour offrir une connectivité aux organisations humanitaires ou aux fournisseurs de services (comme les fournisseurs de bande passante). Les fournisseurs peuvent aussi appliquer l'inspection approfondie des paquets (DPI – *deep packet inspection*)³⁷⁵ au réseau comme couche de protection supplémentaire. La DPI consiste à filtrer les paquets indésirables (unités de données envoyées d'un point d'origine à un point de destination sur Internet), tels que les virus ou logiciels malveillants. Néanmoins, il est important de souligner qu'une DPI permet d'identifier l'expéditeur ou le destinataire d'un contenu composé de paquets spécifiques, ce qui signifie qu'elle peut aussi être utilisée à des fins de suivi et de surveillance.

Toutes ces organisations et entités opérant à différents niveaux du programme de connectivité – raccordement, infrastructures, services « over-the-top » et accès au dernier kilomètre – peuvent collecter des données sur les utilisateurs ou avoir accès à ces dernières, du moment que des données et métadonnées supplémentaires sont générées et traitées à chaque niveau de connectivité. Ce traitement par différentes entités est nécessaire d'un point de vue technique, car il faut en général que plusieurs entités connaissent l'origine et la destination d'un message pour pouvoir l'envoyer d'un point à un autre³⁷⁶. Ces métadonnées (comme les extrémités d'une connexion, les « Likes » et les visites) peuvent être accessibles à tout ou partie des entités de la chaîne de connectivité, qui peuvent ainsi extraire des informations sur les urgences humanitaires et les individus impliqués en ayant recours à des moyens que les bénéficiaires et les organisations humanitaires peuvent difficilement envisager³⁷⁷.

³⁷⁵ Pour en savoir plus sur l'inspection approfondie des paquets, voir : TechTarget – SearchNetworking, « deep packet inspection (DPI) » : <https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI>.

³⁷⁶ CICR et Privacy International, 2018, p. 22-23.

³⁷⁷ *Ibid.*, p. 23.

EXEMPLES D'OPÉRATEURS DE CONNECTIVITÉ QUI COLLECTENT DES DONNÉES DIRECTEMENT AUPRÈS DES BÉNÉFICIAIRES :

Un opérateur de réseau mobile national a généralement accès aux informations suivantes à des fins de facturation : les identifiants uniques pour la carte SIM et l'appareil (numéros IMSI et IMEI) ; l'heure et le lieu des transactions (appels et messages) ; et les données obtenues lors de l'enregistrement de la carte SIM³⁷⁸, qui peuvent varier grandement d'un pays à l'autre et selon le type de carte SIM achetée (prépayée ou postpayée). Néanmoins, la tendance générale est l'enregistrement obligatoire pour tous les types de cartes, ce qui contraint les utilisateurs à fournir des données personnelles³⁷⁹, comme une copie de leur document d'identité, leur numéro d'identification national et leur date de naissance. Dans certains cas, l'identité de l'individu est également vérifiée grâce à une base de données d'identité nationale (en Inde et au Pakistan) ou il devra fournir ses empreintes digitales ou une photographie (au Nigéria par exemple)³⁸⁰. Des recherches³⁸¹ ont montré que les réfugiés et autres personnes déplacées éprouvent la plupart du temps des difficultés à se procurer des cartes SIM via les moyens légaux habituels et se tournent finalement vers des solutions alternatives, officielles ou non, qui présentent un certain nombre de défis en termes de circulation des données.

Dans ce contexte, les organisations humanitaires ne contrôlent pas l'ensemble de la chaîne de connectivité et ne peuvent donc pas garantir la protection des individus contre le détournement de leurs données et métadonnées. Les risques pouvant résulter de cette absence de contrôle devraient être évalués au moyen d'analyses d'impact relatives à la protection des données (voir section 15.2 ci-dessous) lorsque les organisations humanitaires et leurs partenaires jouent un rôle actif dans l'amélioration de la connectivité offerte aux communautés touchées. Pour limiter les risques, certaines organisations humanitaires fournissent aux personnes touchées des informations et des recommandations sur la sécurité numérique³⁸². Néanmoins, lorsque les risques sont trop élevés, les organisations humanitaires n'ont parfois pas d'autre choix que de renoncer à mettre en œuvre un programme de connectivité.

³⁷⁸ *Ibid.*, p. 71.

³⁷⁹ K. P. Donovan et A. K. Martin, « The rise of African SIM registration: The emerging dynamics of regulatory change », *First Monday*, vol. 19, n° 2 (26 janvier 2014) : <http://firstmonday.org/ojs/index.php/fm/article/view/4351> ; voir aussi l'arrêt de la Cour européenne des droits de l'homme (CEDH) rendu dans l'affaire Breyer c. Allemagne (requête n° 50001/12), 30 janvier 2020.

³⁸⁰ GSMA, *Mandatory registration of prepaid SIM cards: Addressing challenges through best practice*, 2016 : [uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf](https://www.gsma.com/regulatory/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf).

³⁸¹ HCR, « Displaced and Disconnected », 2019 : <https://www.unhcr.org/innovation/displaced-and-disconnected/>.

³⁸² Pour en savoir plus sur la sécurité des données, voir [section 2.8 : Sécurité des données et sécurité du traitement](#).

15.2 ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES

Une analyse d'impact relative à la protection des données (AIPD)³⁸³ vise à détecter, évaluer et gérer les risques que présente un projet, une politique, un programme ou une autre initiative pour les personnes dont les données personnelles sont traitées. Elle doit mener à la mise en place de mesures permettant d'éviter de tels risques, de les minimiser, de les transférer ou de les partager. Avant de mettre en œuvre des programmes technologiques impliquant le traitement de données personnelles, les organisations humanitaires devraient effectuer une AIPD pour en évaluer les conséquences possibles, comme l'utilisation illicite des données des bénéficiaires par des partenaires ou l'ingérence du gouvernement dans le réseau.

Avant d'accepter un partenariat dans le cadre d'un programme de connectivité, une organisation humanitaire devrait évaluer les partenaires potentiels et leurs politiques en matière de protection de la vie privée, ainsi que les obligations légales auxquelles ils sont soumis, afin d'être pleinement au fait de la manière dont ils traitent les données des bénéficiaires. Une fois que l'organisation a acquis une vision claire de l'environnement de connectivité, des parties prenantes et des services fournis, elle peut élaborer des lignes directrices ou des critères standard concernant les services requis, y compris les caractéristiques techniques et les exigences en matière de respect de la vie privée. Cela facilitera son interaction avec les partenaires et permettra de parvenir plus rapidement à un accord en cas de situation d'urgence.

Il est également important de rappeler que les bénéficiaires d'une aide humanitaire sont particulièrement vulnérables et que le risque de leur porter préjudice est élevé. C'est pourquoi une AIPD devrait tenir dûment compte des autres droits fondamentaux des personnes concernées³⁸⁴. Comme les organisations humanitaires agissent conformément aux principes humanitaires, il convient également de tenir compte des droits et libertés de tous les membres d'un groupe ou d'une communauté donnée lors de la mise en œuvre de programmes de connectivité, y compris les droits qui ne sont pas liés à leurs données. Par exemple, une AIPD peut examiner des

³⁸³ Voir [chapitre 5 : Analyses d'impact relatives à la protection des données](#).

³⁸⁴ Voir Groupe de travail « Article 29 » sur la protection des données de l'UE, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 2017 : http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 ; et R. Gellert, « Understanding the notion of risk in the General Data Protection Regulation », *Computer Law & Security Review*, vol. 43, n° 2, 2018 : <https://doi.org/10.1016/j.clsr.2017.12.003>.

problèmes d'accès inégal au réseau³⁸⁵ ou d'exclusion potentielle de certains groupes ne sachant pas se servir des outils numériques. Il est également important de garder à l'esprit que les modèles commerciaux de certains partenaires des organisations humanitaires sont basés sur la monétisation des données, ce qui peut être contraire aux principes humanitaires. Les organisations peuvent aussi renoncer à collaborer avec certains partenaires du secteur privé en raison du risque réputationnel qu'une collaboration comporterait. Si l'AIPD indique qu'un programme de connectivité pourrait créer plus de problèmes qu'il n'en résoudrait, il peut s'avérer préférable de ne pas le mettre en œuvre.

15.3 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

Le responsable du traitement est la personne physique ou l'organisation qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles. Un sous-traitant, quant à lui, est la personne physique ou l'organisation qui traite les données personnelles pour le compte du responsable du traitement. Le chapitre 2 définit et examine plus en détail ces concepts.

Lorsque des organisations humanitaires élaborent et mettent en œuvre des programmes de connectivité, elles peuvent agir en tant que responsables du traitement ou en tant que sous-traitants, en fonction de leur rôle et de celui des autres partenaires dans un programme spécifique. Cette distinction est importante lors de l'attribution des responsabilités quant au traitement des données.

Comme les données sont collectées à différents niveaux d'un programme de connectivité, il convient de cartographier les flux de données à chacun de ces niveaux, en identifiant qui collecte les données, pour quelles finalités, quelle est leur durée de conservation et avec qui elles sont partagées. L'exercice de cartographie permettra d'identifier le rôle de chaque partie, y compris de l'organisation humanitaire, quant aux choix des modalités du traitement des données, et de définir ainsi si les parties agissent en tant que responsable du traitement ou sous-traitant.

385 Par exemple, les jeunes enfants et les personnes âgées peuvent ne pas bénéficier des programmes de connectivité ou des services d'accès qui exigent une connectivité, à cause de leur manque de compétences informatiques. De plus, « les femmes vivant dans des pays à revenu faible ou intermédiaire ont 10 % de moins de chances d'avoir un téléphone mobile et sont bien moins susceptibles que les hommes d'utiliser des services porteurs de transformations. Ces femmes ont aussi 26 % de moins de chances que les hommes d'utiliser l'Internet mobile et 33 % de moins de chances d'utiliser l'argent mobile. » Source : GSMA, *Connected Women: The Gender Analysis & Identification Toolkit. Estimating subscriber gender using machine learning*, 2018, p. 6 : <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/GSMA-Gender-Analysis-and-Identification-Report-GAIT-August-2018.pdf>.

Si une organisation humanitaire détermine l'objectif final (la finalité) du programme (par exemple, établir la connectivité) et choisit un partenaire spécifique pour sa mise en œuvre (les moyens), elle agit en tant que responsable du traitement. Dans ce cas, l'organisation doit assumer plusieurs obligations, notamment répondre aux demandes des personnes concernées souhaitant exercer leurs droits³⁸⁶. Les organisations humanitaires et les partenaires d'autres secteurs déterminent parfois ensemble les finalités et les moyens du programme, et agissent donc en tant que responsables conjoints. Dans ce cas, les responsables conjoints doivent définir leurs responsabilités respectives dans un accord écrit, y compris à qui incombe la gestion des demandes des personnes concernées.

15.4 PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

15.4.1 FONDEMENTS JURIDIQUES DU TRAITEMENT DES DONNÉES PERSONNELLES

Lorsque des données personnelles sont nécessaires pour pouvoir accéder aux services de connectivité, ou lorsqu'elles sont générées dans ce processus, il convient d'établir un fondement juridique approprié au traitement de ces données. Ces fondements juridiques sont énumérés au chapitre 3 de ce manuel, qui explique également les défis associés à l'utilisation du consentement comme base juridique dans un contexte humanitaire. En effet, on peut considérer que le consentement n'est pas toujours donné librement dans un contexte humanitaire, les bénéficiaires pouvant se sentir obligés de le donner lorsqu'il s'agit de la seule manière d'accéder à un service spécifique (dans ce cas, la connectivité). En outre, il peut s'avérer difficile d'obtenir un consentement véritablement éclairé en raison de la complexité qui caractérise la connectivité comme forme d'aide, si bien que les personnes concernées qui maîtrisent mal les outils numériques peuvent ne pas comprendre tous les aspects du traitement de leurs données. Les organisations humanitaires et les fournisseurs de services doivent dans ce cas chercher une autre base juridique pour la collecte et le traitement des données, par exemple :

- **Intérêt public** : ce peut être une option pour une organisation qui dispose d'un mandat spécifique pour établir la connectivité³⁸⁷.
- **Intérêt légitime de l'organisation humanitaire** : ce fondement peut aussi être envisagé lorsque l'établissement ou le rétablissement de la connectivité est en accord avec la mission de l'organisation, et lorsque cela pourrait aider les bénéficiaires à accéder à d'autres services essentiels ou améliorer la coordination des activités humanitaires. Néanmoins, cette base n'est applicable que si les droits et libertés des individus en question ne prévalent pas sur les intérêts poursuivis par l'organisation et les avantages attendus du traitement³⁸⁸.

³⁸⁶ Voir [section 2.11: Droits des personnes concernées](#).

³⁸⁷ Voir [chapitre 3: Fondements juridiques du traitement des données personnelles](#).

³⁸⁸ Voir [section 3.5: Intérêt légitime](#).

- **Obligation légale** : certaines juridictions exigent parfois que les utilisateurs des services de connectivité soient enregistrés. Le fondement juridique pour traiter les données des utilisateurs aux fins de l'enregistrement serait dans ce cas le respect d'une obligation légale³⁸⁹.

15.4.2 SÉCURITÉ DES DONNÉES

Les opérateurs de téléphonie mobile jouent un rôle important, car ils fournissent une infrastructure de connectivité essentielle. Dans des situations d'urgence, par exemple, le fait de pouvoir communiquer avec des ambulances et d'autres fournisseurs de soins de santé est vital pour répondre efficacement à un incident. Ces opérateurs doivent prendre des mesures de sécurité techniques et organisationnelles pour protéger les réseaux de communication et assurer la sécurité des données transmises. Ces mesures, qui varieront selon la gravité des risques, comprennent le chiffrement et d'autres moyens techniques de garantir la confidentialité, l'intégrité et la disponibilité des données collectées, ainsi que la résilience globale des services et des systèmes de traitement³⁹⁰.

Certaines métadonnées stockées sur les appareils personnels ne peuvent toutefois pas être chiffrées, et d'autres mesures de sécurité doivent dès lors être prises³⁹¹. Les organisations humanitaires et les individus devraient régulièrement revoir et mettre à jour les mesures de sécurité qu'ils prennent afin de tenir compte de l'évolution des nouvelles technologies et d'assurer un niveau de protection des données suffisant par rapport aux risques liés au traitement des données personnelles. Il faut aussi garder à l'esprit que certaines entités ou organisations peuvent être intéressées à accéder aux données et métadonnées générées par des programmes de connectivité, et ce à des fins non humanitaires, telles que le ciblage et l'exploitation commerciale ou la surveillance.

EXEMPLE :

L'Allemagne et le Danemark ont adopté des lois qui autorisent les autorités à procéder à une analyse détaillée des smartphones des demandeurs d'asile. Les données et métadonnées extraites de leurs appareils peuvent être utilisées pour « vérifier les allégations formulées dans leur demande d'asile ou pour obtenir de nouvelles informations sur leur identité, leur histoire, leur itinéraire, etc.³⁹² ». Des lois similaires ont été adoptées en Belgique et proposées en Autriche³⁹³. En pratique, ces lois impliquent que les données générées dans le cadre des programmes de connectivité peuvent en définitive être utilisées à des fins qui, quand bien même elles sont légitimes, sont contraires aux principes que respectent les organisations humanitaires.

³⁸⁹ Voir [section 3.7 : Respect d'une obligation légale](#).

³⁹⁰ Pour en savoir plus sur la sécurité des données, voir [section 2.8 : Sécurité des données et sécurité du traitement](#).

³⁹¹ CICR et Privacy International, 2018, p. 25.

³⁹² *Ibid.*, p. 62.

³⁹³ *Ibid.*, p. 62.

Les méthodes actuelles de surveillance sont parfois très sophistiquées et peuvent permettre d'obtenir une grande quantité de données et métadonnées sur les utilisateurs d'un réseau³⁹⁴. Cette situation est très préoccupante, car les métadonnées peuvent être utilisées pour en extrapoler des informations que les individus n'ont pas accepté de donner et pour anticiper leur comportement; les données générées dans le cadre de l'assistance humanitaire pourraient alors s'avérer des informations de grande valeur en situation de conflit.

Dans certains cas, une organisation humanitaire – selon son mandat – devra coopérer avec des autorités nationales ou étrangères dans le cadre d'un programme de connectivité. Ce type de coopération peut s'avérer être dans l'intérêt des bénéficiaires, comme lors du partage de données médicales avec les autorités de santé pour faciliter la fourniture d'une aide médicale et dans un objectif de santé publique. Les organisations humanitaires devraient faire preuve de transparence envers les bénéficiaires concernant une éventuelle coopération avec d'autres entités et leur indiquer clairement si leurs données risquent d'être partagées avec des autorités nationales ou étrangères.

Les organisations humanitaires devraient également négocier des mesures de sécurité avec leurs partenaires pour garantir le plus haut niveau de sécurité tout au long de la chaîne de connectivité, y compris pour les parties sur lesquelles l'organisation n'a pas de contrôle.

15.4.3 CONSERVATION DE DONNÉES

Les données personnelles ne doivent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles ont été collectées ou au respect des obligations légales applicables³⁹⁵. En conséquence, les données personnelles devraient toujours être supprimées ou anonymisées dès qu'elles ne sont plus nécessaires. Dans le cadre des programmes de connectivité, les divers partenaires peuvent toutefois avoir différents rôles, besoins et politiques, qui pourraient influencer la manière dont ils traitent les données, y compris la durée pendant laquelle ils les conservent. Là encore, il est important d'établir d'emblée, dans un accord écrit, les responsabilités de chaque partie et leurs politiques en matière de conservation des données. Cela permettra de faire en sorte que les organisations humanitaires soient pleinement au fait des données détenues par chaque partenaire à un moment donné et du lieu où elles sont stockées.

Les opérateurs de téléphonie mobile doivent souvent conserver les données de leurs utilisateurs pour une durée déterminée par la législation nationale. Un tel cadre

³⁹⁴ Voir, par exemple: B. Schneier, « China Isn't the Only Problem With 5G », Foreign Policy, 10 janvier 2020: <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/>.

³⁹⁵ Voir [section 2.7: Conservation des données](#).

permet par exemple aux autorités chargées de l'application des lois d'accéder aux données en cas de délit. Les organisations humanitaires devraient par conséquent déterminer quelles données sont véritablement nécessaires pour déployer le programme et, dans la mesure du possible, éviter de collecter des données inutiles. Moins on collectera de données, moins on en conservera.

15.4.4 INFORMATIONS

Dans les programmes de connectivité, il convient d'indiquer aux personnes concernées, dans un langage clair et facilement compréhensible, quelles données les concernant sont collectées, pour quelles finalités et par quels moyens. Cela est d'autant plus important lorsque les personnes concernées ne savent pas forcément que leurs données sont collectées, par exemple en cas de génération de métadonnées ou de déduction d'informations à partir de données explicitement fournies par la personne concernée ou de son comportement en ligne. Il convient également d'indiquer aux individus à qui ils peuvent s'adresser pour exercer leurs droits. Ces informations leur permettront de prendre des décisions éclairées concernant l'utilisation ou non d'un service spécifique, et de comprendre comment procéder lorsqu'ils souhaitent exercer leurs droits.

Dans un souci de transparence et de complète information, il est conseillé aux organisations humanitaires d'indiquer aux personnes concernées qui sont les tiers impliqués dans le programme, de quelles activités ils sont responsables et comment les contacter. Il convient également de les informer des conséquences négatives réelles ou potentielles et des risques associés à la prestation et l'utilisation de services de connectivité, ainsi qu'aux programmes de connectivité en général. Par exemple, il est utile de s'inspirer du modèle du HCR, qui informe les individus des risques pour la protection de la vie privée associés à la campagne El Jaguar³⁹⁶.

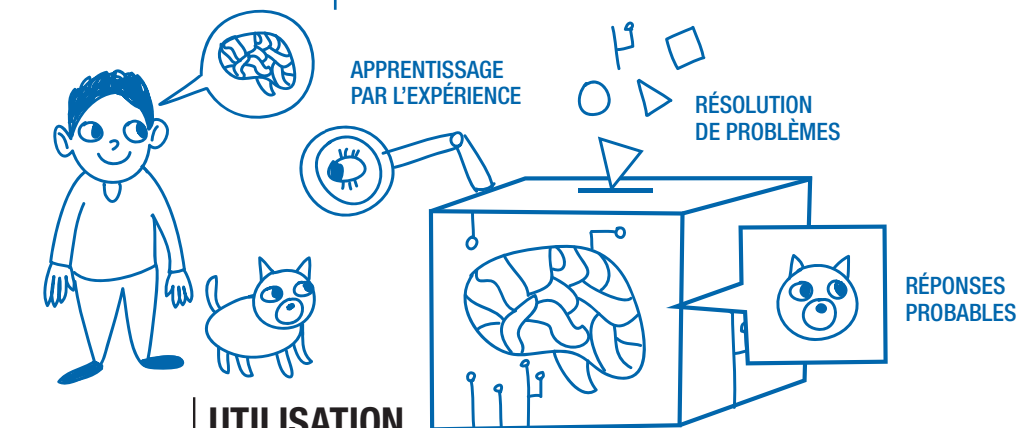
15.5 TRANSFERT INTERNATIONAL DE DONNÉES

Les données traitées en ligne traversent couramment les frontières, ce qui suscite des préoccupations en termes de protection des données personnelles dans le cadre des programmes de connectivité. Malgré l'existence de mécanismes juridiques reconnus, comme des clauses contractuelles, il peut être difficile pour les organisations humanitaires de s'en servir efficacement, du fait surtout qu'elles n'ont souvent pas le contrôle sur les solutions de connectivité. Ceci étant, les organisations devraient faire tout leur possible pour veiller à ce que le fournisseur prenne des dispositions pour encadrer le transfert des données³⁹⁷.

³⁹⁶ <https://www.facebook.com/ConfiaEnElJaguar/videos/874221649451680/>. Cette campagne vidéo donne des conseils sur la protection de la vie privée et la sécurité des profils sur les médias sociaux.

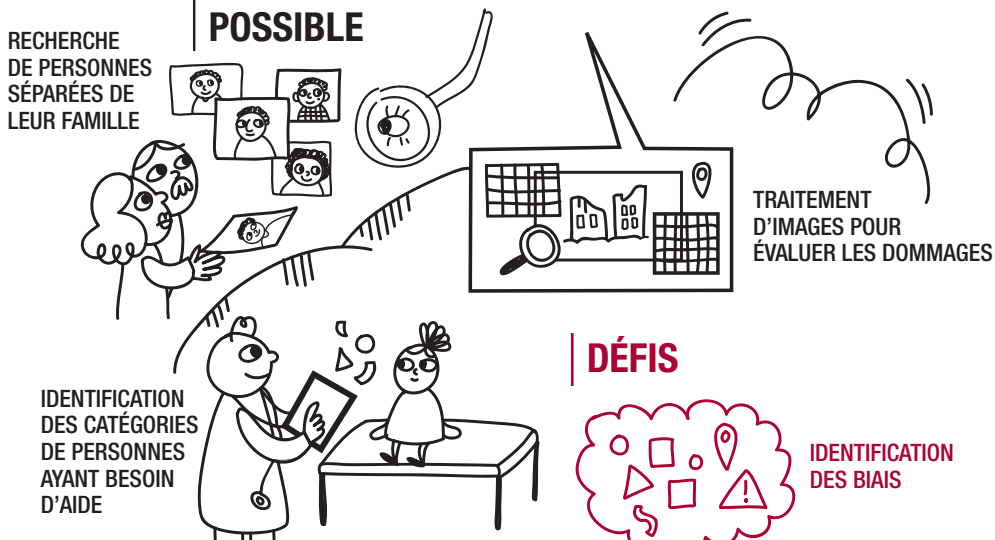
³⁹⁷ Voir [chapitre 4 : Transfert international de données](#).

INTELLIGENCE ARTIFICIELLE



RECHERCHE
DE PERSONNES
SÉPARÉES DE
LEUR FAMILLE

UTILISATION POSSIBLE



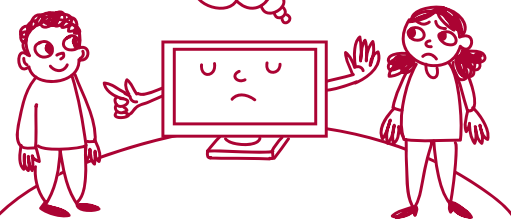
TRAITEMENT
D'IMAGES POUR
ÉVALUER LES DOMMAGES

IDENTIFICATION
DES CATÉGORIES
DE PERSONNES
AYANT BESOIN
D'AIDE

DÉFIS

IDENTIFICATION
DES BIAIS

DÉCISIONS BASÉES
SUR UNE ANALYSE
PILOTÉE PAR IA



COMPRÉHENSION
DES CONCLUSIONS

ATTAQUE CONTRE
L'INTÉGRITÉ DES DONNÉES



CHAPITRE 16

INTELLIGENCE ARTIFICIELLE ET APPRENTISSAGE AUTOMATIQUE³⁹⁸

398 Les auteurs souhaitent remercier Alessandro Mantelero (Politecnico di Torino) pour son aide à la rédaction de ce chapitre.

16.1 INTRODUCTION

Ce chapitre explore les défis liés à la protection des données qui résultent de l'utilisation des systèmes d'intelligence artificielle et d'apprentissage automatique dans le secteur humanitaire. Certains de ces défis concernent la prise de décisions automatisée, un sujet au cœur de nombreux débats, tandis que d'autres tiennent au fait que ces systèmes impliquent une utilisation massive de données, y compris de données personnelles. Les sections suivantes donnent d'abord une explication simple des technologies en question, puis identifient les défis qu'elles présentent en termes de protection des données, et enfin donnent des orientations aux organisations humanitaires pour répondre à certains de ces défis.

16.1.1 QUE SONT L'INTELLIGENCE ARTIFICIELLE ET L'APPRENTISSAGE AUTOMATIQUE ?

Bien qu'il n'y ait pas de définition universellement acceptée de ce terme, l'intelligence artificielle est généralement entendue comme un « ensemble de sciences, théories et techniques dont le but est de reproduire par une machine des capacités cognitives d'un être humain³⁹⁹ ». Dans sa forme actuelle, elle vise à permettre aux concepteurs de technologies de « confier à une machine des tâches complexes auparavant déléguées à un humain⁴⁰⁰ ».

L'apprentissage automatique est quant à lui une forme spécifique d'intelligence artificielle pouvant être définie comme l'étude d'algorithmes qui s'améliorent avec le temps dans de l'exécution d'une tâche spécifique à travers l'expérience accumulée sous forme de données lisibles par machine⁴⁰¹. Un algorithme reçoit de plus en plus de données représentant le problème qu'il tente de résoudre et « apprend » de ces données. Il existe cependant d'autres techniques d'intelligence artificielle qui dépendent moins des données, car elles « apprennent » d'une autre manière⁴⁰².

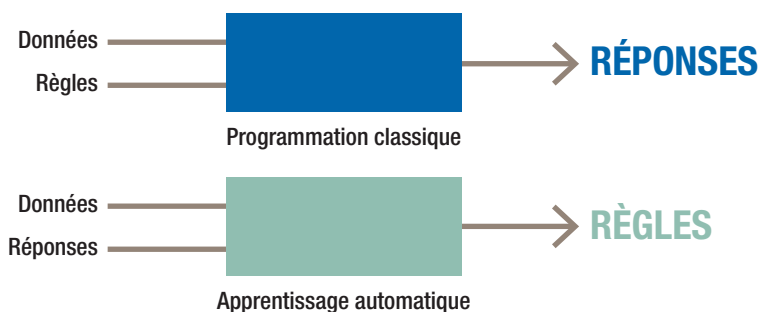
Quelle que soit leur méthode d'apprentissage, toutes les formes d'intelligence artificielle ont un point commun : elles ne sont pas un ensemble de règles qu'une machine doit suivre pour exécuter une tâche spécifique, mais plutôt un ensemble de règles à partir duquel la machine doit générer des stratégies ou des solutions pour exécuter cette tâche, comme l'illustre le modèle suivant :

399 Conseil de l'Europe (CdE), Glossaire, entrée Intelligence artificielle : <https://www.coe.int/fr/web/artificial-intelligence/glossary>.

400 *Ibid.*

401 T. Mitchell, *Machine Learning*, McGraw-Hill, New York, 1997, p. 2.

402 Les réseaux bayésiens et les moteurs de règles sont deux exemples de ces méthodes. Ils ne seront toutefois pas abordés dans ce chapitre.



Source : F. Chollet, *Deep Learning with Python*, Manning Publications, 2017.

L'apprentissage automatique est la forme d'intelligence artificielle qui a attiré la grande majorité des investissements réalisés dans l'intelligence artificielle ces dernières années. C'est pourquoi, dans ce chapitre, le terme « intelligence artificielle » sera utilisé pour désigner aussi bien les solutions d'intelligence artificielle que celles d'apprentissage automatique. Si un point fait référence à une technique spécifique, cela sera clairement indiqué.

16.1.2 COMMENT FONCTIONNENT L'INTELLIGENCE ARTIFICIELLE ET L'APPRENTISSAGE AUTOMATIQUE ?

Il existe de nombreuses techniques d'intelligence artificielle. Certaines traitent des données personnelles, tandis que d'autres ne le font pas. La plupart des solutions, en particulier celles qui utilisent l'apprentissage automatique, fonctionnent toutefois comme suit :

1. Les données sélectionnées supposées contenir des motifs récurrents ou des similarités spécifiques (données d'apprentissage) sont saisies dans le système.
2. Les techniques d'intelligence artificielle identifient ces motifs et déterminent quelles caractéristiques sont pertinentes pour le classement de ces motifs ou similarités et pour la formulation de prédictions concernant de nouvelles données.
3. Un modèle est généré, qui a la capacité d'identifier des motifs lorsqu'il traite de nouvelles données en vue d'établir des prédictions ou des classements⁴⁰³.

⁴⁰³ Autorité norvégienne de protection des données, *Artificial intelligence and privacy*, 2018, p. 7 : <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

Contrairement à la plupart des types d'intelligence artificielle, certains n'ont besoin que de quantités limitées de données pour fonctionner. Pour comprendre les principales implications en termes de protection des données détaillées à la section 16.3, il est important de comprendre les différentes méthodes d'apprentissage des solutions d'intelligence artificielle :

- **Apprentissage supervisé** : dans ce modèle, les données d'apprentissage sont étiquetées (l'analyste attribue une « classe » à chaque échantillon de données). Par exemple, on attribue aux échantillons d'images d'animaux une étiquette, telle que « chien », « chat » ou « perroquet » et on les transmet ensuite au système. En règle générale, l'objectif final est de faire en sorte que l'algorithme parvienne à classer de nouvelles images (non vues) dans l'une des classes apprises. Ce type d'apprentissage peut également être utilisé, entre autres, pour prédire une valeur basée sur différents paramètres (ou caractéristiques), par exemple évaluer le prix d'une maison en fonction du nombre de pièces, de la superficie et/ou de l'année de construction. Dans les deux cas, il s'agit d'identifier la fonction mathématique capable de distribuer au mieux les données dans les bonnes classes ou d'évaluer correctement les valeurs.
- **Apprentissage non supervisé** : dans ce modèle, aucune étiquette n'est transmise au système. L'idée est que l'algorithme découvre des similarités ou des motifs dans un jeu de données et crée lui-même les étiquettes (ou classes). Il existe différentes méthodes permettant de classer les données dans des « clusters ». Il n'y a pas de bonnes ou de mauvaises réponses.
- **Apprentissage par renforcement** : cette approche ne nécessite que peu ou pas de données d'apprentissage. Elle est fondée sur une méthode de récompenses positives et négatives où « le système reçoit un signal de récompense lorsqu'il accomplit ce que le concepteur souhaite ou lorsqu'il franchit une étape qui rapproche le processus de l'objectif décrit par le concepteur. Lorsque le système se trompe (échoue à se rapprocher efficacement de l'objectif souhaité), il n'est simplement pas récompensé⁴⁰⁴ ».

Lorsqu'une solution est soumise à un apprentissage selon l'une des méthodes susmentionnées⁴⁰⁵, elle génère un modèle qui sera utilisé pour analyser ou prédire des données nouvelles ou non vues. Les modèles produits par l'intelligence artificielle peuvent être statiques ou dynamiques. Les modèles statiques n'évoluent pas au fil du temps et appliquent toujours le modèle conçu à partir des données d'apprentissage, ce qui permet au concepteur de contrôler entièrement le modèle,

⁴⁰⁴ Ibid., p. 18.

⁴⁰⁵ Ce chapitre n'aborde pas toutes les méthodes d'apprentissage possibles de l'intelligence artificielle. Pour en savoir plus sur les méthodes qui ne sont pas mentionnées ici (comme les réseaux neuronaux), voir par exemple : L. Hardesty, « Explained: Neural networks », MIT News, 14 avril 2017 : <http://news.mit.edu/2017/explained-neural-networks-deep-learning-0414> ; et Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning*, 2018 : https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf.

mais empêche la solution de se perfectionner au fil du temps. En revanche, les modèles dynamiques utilisent les données pour s'adapter aux changements et perfectionner leurs résultats⁴⁰⁶.

Comme la plupart des solutions d'intelligence artificielle apprennent à partir des données qui leur sont fournies pendant l'apprentissage (et également pendant le déploiement, dans le cas des modèles dynamiques), les modèles générés conservent une partie des données utilisées pour leur conception ou leur amélioration. Dans certains cas, si des parties malveillantes attaquaient le système et réussissaient à en prendre le contrôle, elles pourraient alors accéder aux données d'apprentissage (ou aux données utilisées pendant le déploiement de la solution, dans le cas des modèles dynamiques). La section 16.3.5 ci-après traite de la sécurité des données et donne plus de détails sur les attaques possibles contre les solutions d'intelligence artificielle.

16.1.3 INTELLIGENCE ARTIFICIELLE DANS LE SECTEUR HUMANITAIRE

Le nombre d'applications reposant sur l'intelligence artificielle dans notre quotidien a grandement augmenté en raison du développement récent de la capacité de traitement et de la multiplication des données disponibles⁴⁰⁷. Par exemple, l'intelligence artificielle est utilisée dans les assistants numériques à commande vocale, dans les systèmes de reconnaissance biométrique qui autorisent le déverrouillage des téléphones et l'accès à des bâtiments, dans les applications d'aiguillage du trafic, dans les systèmes de recommandation d'achat ou de consultation sur les plateformes en ligne, et dans de nombreuses autres fonctions des outils et services en ligne et des appareils dits « intelligents ». Cette technologie peut aussi être utilisée pour une grande variété de tâches, comme le diagnostic médical, la reconnaissance d'images, les prévisions boursières et les jeux vidéo.

L'intelligence artificielle peut également faciliter l'action humanitaire et les activités qui lui sont associées ou qui présentent des caractéristiques semblables, et les rendre plus efficaces et efficientes. Voici certaines de ces applications, existantes et potentielles :

- **Lecture de l'opinion publique** – En Ouganda, le programme de l'ONU Global Pulse a mené un projet pilote pour la mise au point « d'une solution pour rendre les textes des émissions radio publiques lisibles par une machine grâce à l'utilisation de technologies de reconnaissance vocale et d'outils de traduction

⁴⁰⁶ Pour en savoir plus, voir : Autorité norvégienne de protection des données, 2018, p. 10.

⁴⁰⁷ Centre for Information Policy Leadership, *First Report: Artificial Intelligence and Data Protection in Tension*, 2018, p. 4 : https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf.

qui transforment les contenus radiophoniques en texte⁴⁰⁸ ». Cette solution, conçue par Pulse Lab Kampala, vise à identifier des tendances au sein de différents groupes de population, en particulier ceux des zones rurales. L'idée derrière cette initiative est que la lecture de ces tendances pourrait aider le gouvernement et les acteurs du développement à mieux comprendre les besoins du pays dans ce domaine, qui pourront ainsi être pris en compte lors de la mise en œuvre des programmes de développement.

- **Identification et localisation des enfants disparus** – Selon certaines sources⁴⁰⁹, le *National Tracking System for Missing & Vulnerable Children* (système de suivi national pour les enfants disparus et vulnérables) de l'Inde a identifié près de 3 000 enfants portés disparus après seulement quatre jours d'essai d'un nouveau système de reconnaissance faciale qui compare les visages des individus disparus aux photographies des enfants vivant dans des foyers et des orphelinats.
- **Suivi des attaques contre les civils et des violations des droits humains** – Le projet « Decode the Difference » d'Amnesty International⁴¹⁰ a fait appel à des bénévoles pour comparer les images d'un même lieu à des moments différents en vue d'identifier les bâtiments endommagés, pouvant servir à démontrer l'existence d'attaques systématiques contre des civils. À l'avenir, ces données pourraient être utilisées pour former des outils d'apprentissage automatique à l'analyse d'images, ce qui permettrait d'accélérer le processus et d'augmenter la capacité du système.
- **Prévention et diagnostic des maladies** – « Depuis les années 1990, on utilise l'IA [intelligence artificielle] pour diagnostiquer différents types de maladies, telles que le cancer, la sclérose en plaques, les affections pancréatiques et le diabète⁴¹¹. » Plus récemment, Microsoft a lancé le projet « Premonition », qui vise à détecter les agents pathogènes avant qu'ils ne provoquent une épidémie. Le projet déploie des robots dont l'objectif est de surveiller la présence de moustiques dans une zone, d'établir des prédictions sur leurs mouvements

⁴⁰⁸ UN Global Pulse, « Making Ugandan Community Radio Machine-readable Using Speech Recognition Technology », 2016, disponible à l'adresse suivante : <https://www.unglobalpulse.org/projects/radio-mining-uganda>.

⁴⁰⁹ A. Cuthbertson, « Indian police trace 3,000 missing children in just four days using facial recognition technology », *The Independent*, 24 avril 2018 : <https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html> ; voir aussi : *The Times of India*, « Delhi: Facial recognition system helps trace 3,000 missing children in 4 days », 22 avril 2018 : http://timesofindia.indiatimes.com/articleshow/63870129.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. Pour consulter le site Web officiel du système, voir : <https://trackthemissingchild.gov.in/trackchild/index.php/index.php>.

⁴¹⁰ Amnesty International, « Amnesty Decoders » : <https://decoders.amnesty.org/>.

⁴¹¹ H. M. Roff, « Advancing Human Security through Artificial Intelligence », *Chatham House*, 2017, p. 5 : <https://www.chathamhouse.org/publication/advancing-human-security-through-artificial-intelligence>.

et de capturer des espèces ciblées. Grâce à des techniques d'apprentissage automatique, les moustiques capturés sont étudiés pour analyser les agents pathogènes qu'ils pourraient transporter après avoir piqué certains animaux⁴¹².

16.1.4 DÉFIS ET RISQUES LIÉS À L'UTILISATION DE L'INTELLIGENCE ARTIFICIELLE

Malgré leur potentiel, les applications de l'intelligence artificielle peuvent présenter des défis et des risques. Outre les préoccupations relatives à la protection des données (voir la section 16.3 ci-dessous), toutes les utilisations évoquées ci-dessus présentent des défis pratiques liés à leur mise en œuvre. Par exemple, le logiciel de reconnaissance d'images fondé sur l'intelligence artificielle qui permet d'identifier les personnes disparues risque de produire trop de faux positifs. Ces fausses correspondances pourraient non seulement susciter une certaine confusion auprès des personnes chargées des recherches, mais aussi donner de faux espoirs aux familles. D'autres systèmes pourraient être plus précis, mais ne pas détecter des correspondances positives (ce que l'on appelle un faux négatif). Si les faux négatifs ne représentent pas un problème très important pour des applications commerciales, ils peuvent avoir de graves conséquences dans le secteur humanitaire. Si une organisation n'identifie pas un enfant qui a perdu le contact avec ses parents, cette erreur peut affecter l'ensemble de la famille.

Comme relevé ci-dessus, l'intelligence artificielle peut comporter des risques pour les bénéficiaires. Par exemple, si elle est utilisée pour identifier la bonne population cible pour un programme humanitaire spécifique et que la solution n'identifie pas correctement les individus, certaines personnes qui auraient dû bénéficier du programme peuvent s'en trouver exclues. C'est ce qui s'est produit en Suède, où des milliers de personnes sans emploi se sont vu refuser à tort des allocations par un système gouvernemental fondé sur l'intelligence artificielle⁴¹³.

Comme la plupart des organisations humanitaires choisissent des solutions disponibles sur le marché plutôt que de concevoir leurs propres modèles, le risque que les algorithmes produisent des résultats inattendus ou déraisonnables est bien réel. De même, le fait que les organisations se retrouvent captives de leurs fournisseurs est problématique, car un changement de solution peut s'avérer onéreux. Les organisations peuvent également être ciblées par des initiatives commerciales dont le but principal est d'accéder aux vastes jeux de données qu'elles possèdent et de les exploiter, avec parfois à la clé un risque élevé de nuire aux personnes et aux communautés concernées.

⁴¹² Microsoft, « Microsoft Premonition » : <https://www.microsoft.com/en-us/research/project/project-premonition/>.

⁴¹³ T. Wills, « Sweden: Rogue algorithm stops welfare payments for up to 70,000 unemployed », Algorithm Watch, 25 février 2019 : <https://algorithmwatch.org/en/rogue-algorithm-in-sweden-stops-welfare-payments/>.

Les biais représentent un autre risque pour l'efficacité de l'intelligence artificielle, en particulier dans certains contextes humanitaires spécifiques (voir la section 16.3.2.2 ci-dessous). Comme la plupart des solutions (mais pas la totalité) apprennent à partir de grandes quantités de données, il est important de sélectionner un jeu de données adapté à l'objectif visé. En outre, lorsque la solution est utilisée pour identifier des tendances ou faire des prédictions concernant des individus ou des communautés spécifiques, le jeu de données d'apprentissage comportera très certainement des données personnelles.

Comme pour bon nombre d'autres technologies, le principe « à données inexactes, résultats erronés⁴¹⁴ » s'applique également à l'intelligence artificielle : l'utilisation de données inadéquates, inexactes ou non pertinentes peut donc compromettre l'exactitude de la solution. C'est un aspect particulièrement problématique pour les organisations humanitaires, car il est extrêmement rare que les algorithmes disponibles sur le marché soient parfaitement adaptés à leurs contextes. Par exemple, si une organisation humanitaire souhaite concevoir un logiciel de reconnaissance faciale pour la recherche de personnes disparues, les jeux de données d'apprentissage devront être suffisamment vastes pour intégrer les caractéristiques physiques propres à chaque ethnie afin de maximiser la précision de la fonction de correspondance.

16.2 ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Une AIPD vise à identifier, évaluer et gérer l'impact qu'aura sur les personnes concernées et leurs données personnelles un projet, une politique, un programme ou une autre initiative impliquant le traitement de ces données⁴¹⁵. Elle doit permettre d'identifier les mesures à prendre afin de minimiser, éviter, transférer ou partager les risques associés aux activités de traitement des données. Une AIPD est un processus continu, qui doit accompagner un projet ou une initiative impliquant le traitement des données personnelles tout au long de son cycle de vie. Compte tenu de la transparence limitée qu'offre l'intelligence artificielle (comme expliqué plus en détail à la section 16.3.2.3 ci-dessous), une AIPD peut contribuer à accroître l'acceptation des bénéficiaires d'accepter et les amener à utiliser davantage les solutions d'intelligence artificielle mises en place par les organisations humanitaires. Comme l'utilisation de l'intelligence artificielle peut présenter des

⁴¹⁴ Selon le Free online dictionary of computing (<http://foldoc.org>), le concept de « données inexactes, résultats erronés » fait référence au fait que les « ordinateurs, contrairement aux êtres humains, traiteront les données absurdes sans se poser de questions et produiront un résultat lui aussi absurde ». L'expression est également employée pour évoquer les « échecs dans la prise de décisions par des êtres humains à cause de données erronées, incomplètes ou imprécises ».

⁴¹⁵ Voir le [chapitre 5 : Analyses d'impact relatives à la protection des données](#).

risques considérables en matière de protection des données personnelles, toute organisation qui envisagerait de mettre en œuvre une telle solution devrait effectuer une AIPD avant de prendre sa décision. Les implications éthiques de l'intelligence artificielle, dont il est question à la section 16.8 ci-dessous, devraient également être prises en compte dans une AIPD.

16.3 APPLICATION DES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES

Comme indiqué plus haut, la plupart des solutions d'intelligence artificielle doivent traiter de grandes quantités de données, aussi bien personnelles que non personnelles, pour pouvoir fonctionner correctement. Il peut toutefois être difficile de savoir quand les solutions d'intelligence artificielle traitent des données personnelles et donc quand les principes de protection des données sont applicables, car ces solutions sont toujours davantage capables « de rapprocher des données ou de reconnaître des tendances dans les données pouvant rendre identifiables des données non personnelles⁴¹⁶ ». Cela signifie que les solutions d'intelligence artificielle peuvent, dans certains cas, réidentifier des données pseudonymisées, c'est-à-dire les rendre identifiables en élargissant « les types et la demande de données collectées, par exemple à partir des capteurs des téléphones portables, des voitures et d'autres appareils », et en s'appuyant sur « des capacités de calcul toujours plus avancées pour analyser les données collectées » et parvenir à les combiner de sorte à pouvoir identifier des personnes de manière fiable⁴¹⁷. Comme pour les autres systèmes qui traitent des données personnelles, au moment de déterminer si et comment les principes de protection des données s'appliquent, il conviendra d'accorder une attention particulière à l'architecture de la solution et au contexte dans lequel elle sera utilisée.

16.3.1 LIMITATION DE LA FINALITÉ ET TRAITEMENT ULTÉRIEUR

Il est difficile d'appliquer le principe de limitation des finalités⁴¹⁸ aux solutions d'intelligence artificielle et d'apprentissage automatique, car ces technologies sont parfois capables de traiter des données d'une manière autre que celle prévue au départ et peuvent par conséquent servir une finalité non prévue à l'origine. Cela s'explique par la nature même de l'apprentissage automatique, qui consiste à tester et à découvrir des corrélations diverses au sein d'un jeu de données analysé. Ces solutions sont donc capables de déduire de nouvelles informations à partir des caractéristiques des données.

⁴¹⁶ Centre for Information Policy Leadership, 2018, p. 11.

⁴¹⁷ *Ibid.*, p. 11.

⁴¹⁸ Voir la [section 2.5.2: Principe de limitation des finalités](#).

EXEMPLE :

En 2012, des chercheurs ont constaté que lorsque les algorithmes d'intelligence artificielle analysaient les « Likes » d'une personne sur Facebook, sans autres informations sur cette personne, les solutions pouvaient « prédire automatiquement et précisément une variété d'attributs personnels très sensibles, notamment : l'orientation sexuelle, l'origine ethnique, les opinions politiques et religieuses, les traits de caractère, l'intelligence, le niveau de bonheur, l'utilisation de substances addictives, la séparation parentale, l'âge et le sexe⁴¹⁹ ». Plus particulièrement, la solution a correctement fait la distinction « entre hommes homosexuels et hétérosexuels dans 88 % des cas, entre Afro-Américains et Américains d'origine caucasienne dans 95 % des cas, et entre républicains et démocrates dans 85 % des cas⁴²⁰ ». Dans ce cas précis, il a été demandé à la solution d'étudier ces corrélations. Néanmoins, dans d'autres situations, les solutions d'intelligence artificielle peuvent réaliser de telles déductions de manière autonome et dévoiler des informations sensibles sur une personne même si ce n'était pas le but du concepteur.

Le principe de limitation des finalités exige des organisations qu'elles établissent un objectif bien précis pour le traitement des données personnelles et qu'elles déterminent les moyens et les informations nécessaires pour l'atteindre. Dans le cas de l'intelligence artificielle, elles doivent cependant évaluer également le risque que la solution produise un résultat indésirable. Si l'on peut s'attendre à ce que la solution traite des données personnelles d'une manière incompatible avec la finalité définie, dévoile des informations ou établisse des prédictions non désirées, il convient d'en tenir compte lors de sa conception et de la sélection du jeu de données d'apprentissage. L'objectif ultime est d'éviter autant que possible les résultats indésirables et toute forme non souhaitée de traitement ultérieur.

16.3.2 TRAITEMENT ÉQUITABLE ET LICITE

16.3.2.1 Licéité

Si la solution d'intelligence artificielle est censée traiter des données personnelles dans le cadre de son déploiement ou de son apprentissage, il convient de définir un fondement juridique pour ce traitement. Compte tenu de la complexité des systèmes d'intelligence artificielle, il peut s'avérer particulièrement difficile d'identifier et de justifier une base juridique appropriée. Le chapitre 3 présente différentes possibilités et souligne les limites de l'utilisation du consentement comme fondement juridique dans l'action humanitaire. En particulier, la question du retrait du consentement est pertinente dans l'optique du développement et du perfectionnement des solutions

⁴¹⁹ M. Kosinski, D. Stillwell et T. Graepel, « Private traits and attributes are predictable from digital records of human behavior », *PNAS*, vol. 110, n° 15, 2013, p. 1 : <https://www.pnas.org/content/pnas/early/2013/03/06/1218772110.full.pdf>.

⁴²⁰ *Ibid.*, p. 1.

d'intelligence artificielle. Dans le cas de l'intelligence artificielle, il est en outre difficile d'envisager un consentement réellement libre et éclairé, notamment pour les raisons suivantes : « longueur et caractère excessivement technique des notices d'information sur le traitement des données, *lock-in* (dépendance) social et technique, conception peu claire des interfaces et sensibilisation insuffisante des intéressés⁴²¹. »

Comme indiqué au début de ce chapitre, les modèles produits par l'intelligence artificielle peuvent être statiques ou dynamiques. Ces deux types de modèles ont des implications différentes en termes de protection des données. Les modèles statiques traitent des données personnelles uniquement pour exécuter la tâche attribuée au système, tandis que les modèles dynamiques traitent des données pour atteindre le résultat souhaité, mais également pour perfectionner le système en vue d'obtenir des résultats plus précis. Par conséquent, la finalité et le fondement juridique du traitement des données seront différents pour chacun des modèles.

Par exemple, si une organisation humanitaire choisit un modèle dynamique, elle doit identifier un fondement juridique approprié pour traiter les données personnelles nécessaires à l'entraînement de son algorithme en vue d'atteindre un objectif clairement défini. Il y a lieu de définir un fondement juridique également pour le traitement de nouvelles données personnelles, une fois l'entraînement du système terminé. Enfin, l'organisation doit identifier un fondement juridique pour traiter des données personnelles dans le but d'améliorer le modèle dynamique.

Dans le cas des modèles dynamiques, y compris les solutions commerciales développées par des sociétés de technologies, il faut garder à l'esprit que toutes les données transmises au système pendant son développement et son déploiement seront utilisées pour son perfectionnement. Cela peut poser d'autres défis liés au consentement : en effet, même si les bénéficiaires ont accepté que leurs données personnelles soient traitées à des fins humanitaires spécifiques, ils ne s'attendent peut-être pas à ce qu'elles soient utilisées pour la mise au point d'une solution d'intelligence artificielle⁴²². Dans ce cas, si le consentement est le fondement juridique pour le traitement des données, il convient d'indiquer aux personnes concernées, dans un langage facilement compréhensible, les raisons pour lesquelles leurs données sont nécessaires, à quoi elles serviront et comment elles influenceront la solution. Les personnes concernées devront également être informées des risques éventuels, tels qu'une réidentification par la solution (comme indiqué à la section 16.3.1) ou le fait que des tiers pourraient obtenir l'accès à leurs données en cas d'attaque (voir ci-dessus). Ce faisant, les organisations pourront s'assurer que le consentement des personnes concernées est pleinement éclairé.

⁴²¹ A. Mantelero, *Intelligence artificielle et protection des données: enjeux et solutions possibles*, Conseil de l'Europe, 2019, p. 7 : <https://rm.coe.int/intelligence-artificielle-et-protection-des-donnees-enjeux-et-solution/168091f8a5>.

⁴²² Future of Privacy Forum, 2018, p. 8.

Au vu de ce qui précède, le consentement peut ne pas toujours constituer un fondement juridique approprié pour l'utilisation de l'intelligence artificielle dans le secteur humanitaire. Bien que la fourniture d'une assistance ou de services vitaux puisse justifier l'invocation de l'intérêt vital⁴²³ ou de l'intérêt public⁴²⁴ comme fondement juridique légitime du traitement des données personnelles, ce n'est pas toujours le cas du développement de solutions d'intelligence artificielle. Pour déterminer si l'amélioration de solutions d'intelligence artificielle est acceptable au regard du fondement juridique choisi, l'organisation devrait vérifier si le traitement ultérieur des données pour le perfectionnement de la solution est compatible avec la finalité initiale pour laquelle les données personnelles ont été recueillies.

16.3.2.2 Loyauté et biais

Le principe de loyauté⁴²⁵ exige que toutes les activités de traitement de données respectent les intérêts des personnes concernées et que les responsables du traitement prennent des mesures pour empêcher toute discrimination arbitraire à l'encontre des individus⁴²⁶. Le problème des biais discriminatoires dans l'intelligence artificielle est largement reconnu et débattu.

EXEMPLE :

Un exemple bien connu est celui d'une solution d'intelligence artificielle développée aux États-Unis pour prédire les taux de récidive dans des affaires criminelles, afin d'aider les juges dans leurs décisions concernant la possibilité d'une libération sous caution des personnes condamnées. La solution a évalué à tort les prévenus noirs comme étant presque deux fois plus susceptibles de récidiver que les blancs⁴²⁷.

Pour minimiser le risque de biais discriminatoires, les concepteurs d'intelligence artificielle doivent « adopter une approche [intégrant les] droits de l'homme dès la conception (*by-design*) et éviter tout biais potentiel, y compris les biais non intentionnels ou cachés, ainsi que les risques de discrimination ou d'autres effets négatifs sur les droits humains et libertés fondamentales des personnes concernées⁴²⁸ ».

Les biais des solutions d'intelligence artificielle peuvent provenir de l'utilisation de jeux de données biaisés durant la phase d'apprentissage, de biais systémiques

⁴²³ Voir la [section 3.3 : Intérêt vital](#).

⁴²⁴ Voir la [section 3.4 : Motifs importants d'intérêt public](#).

⁴²⁵ Voir la [section 2.5.1 : Principes de licéité, de loyauté et de transparence du traitement](#).

⁴²⁶ Autorité norvégienne de protection des données, 2018, p. 16.

⁴²⁷ J. Angwin *et al.*, « Machine Bias », ProPublica, 23 mai 2016 : <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

⁴²⁸ CdE, *Lignes directrices sur l'intelligence artificielle et la protection des données*, 2019, p. 2 : <https://rm.coe.int/lignes-directrices-sur-l-intelligence-artificielle-et-la-protection-de/168091ff40>.

au sein de la société, ou même des choix des concepteurs quant à la pondération de certaines caractéristiques dans chaque jeu de données. En outre, lorsqu'il y a des biais historiques dans la société, il peut être difficile d'obtenir des données non biaisées pour l'entraînement de la solution. Dans ce cas, la solution risque tout simplement de renforcer les biais systémiques contenus dans le jeu de données. Il est par conséquent important qu'un modèle soit entraîné au moyen de données correctes et pertinentes ; ce modèle doit aussi apprendre à quelles caractéristiques accorder de la valeur, de sorte à ne pas attribuer une importance trop élevée à des facteurs discriminatoires qui pourraient être présents dans les données. Lorsqu'il y a un risque de discrimination arbitraire, les informations relatives à l'origine raciale ou ethnique, aux opinions politiques, aux croyances religieuses ou philosophiques et à l'orientation sexuelle, ainsi que toute autre information pouvant être source de discrimination, ne devraient pas être traitées ou devraient être protégées de façon à éviter toute pondération disproportionnée⁴²⁹.

Cela dit, le fait que les modèles d'intelligence artificielle ne doivent pas mettre en valeur certaines catégories de données ne signifie pas que leur suppression du jeu de données permettra nécessairement d'éliminer le risque de biais. Le système pourrait en effet corrélérer d'autres caractéristiques, comme l'origine ethnique ou le sexe, et le modèle pourrait alors acquérir des biais à travers ces caractéristiques corrélées, que l'on appelle dans ce contexte « proxy⁴³⁰ ». Par ailleurs, comme la caractéristique discriminatoire principale a été retirée du jeu de données, il pourrait être plus difficile de repérer et de corriger ces biais.

EXEMPLE :

Une autre étude s'est penchée sur la solution prédictive américaine mentionnée plus haut et a conclu que dans 70 % des cas, l'algorithme avait établi une prédiction de récidive correcte malgré le biais évident. Cette seconde étude n'a cependant pas intégré l'origine raciale dans le jeu de données, soulignant « la difficulté de trouver un modèle qui ne crée pas de proxy pour l'origine raciale ou d'autres facteurs éliminés, comme la pauvreté, le chômage ou la marginalisation sociale⁴³¹ ».

Par conséquent, lors de la sélection d'un jeu de données d'apprentissage, le concepteur de solutions d'intelligence artificielle, qu'il agisse en tant que responsable du traitement indépendant, sous-traitant ou responsable conjoint avec une organisation humanitaire, doit évaluer la qualité, la nature et l'origine des données personnelles utilisées et évaluer les risques éventuels pour les individus et les groupes découlant de l'utilisation de données décontextualisées pour la création

⁴²⁹ Autorité norvégienne de protection des données, 2018, p. 16.

⁴³⁰ Centre for Information Policy Leadership, 2018, p. 14.

⁴³¹ Future of Privacy Forum, 2018, p. 15.

de modèles décontextualisés⁴³². Pour ce faire, les responsables du traitement peuvent d'une part intégrer dans le processus continu d'AIPD (voir section 16.2) des « évaluations fréquentes des ensembles de données qu'ils traitent afin de vérifier s'il n'y a pas de biais » et d'autre part « élaborer des moyens de traiter tout élément préjudiciable, y compris toute dépendance excessive à l'égard des corrélations⁴³³ ». Comme indiqué à la section 2 ci-dessus, la non-mise en œuvre de ces mesures a des conséquences tant juridiques qu'éthiques.

16.3.2.3 Transparence

Au même titre que la loyauté, la transparence est un aspect crucial de la protection des données. Selon ce principe, le traitement des données personnelles doit être transparent⁴³⁴ pour les personnes concernées, qui doivent recevoir lors de la collecte de leurs données à tout le moins un minimum d'informations concernant leur traitement⁴³⁵. Néanmoins, la transparence peut se révéler un principe difficile à appliquer dans le cadre de l'intelligence artificielle, car ces solutions sont fondées sur des technologies avancées qui peuvent être compliquées à comprendre et à définir en termes simples⁴³⁶. Par ailleurs, de nombreux modèles d'apprentissage automatique intègrent des réseaux multicouches dont les résultats reposent sur un processus interne qui ne peut être ni reproduit ni compris d'un point de vue mathématique, même par les spécialistes des données et les concepteurs de solutions eux-mêmes⁴³⁷. Cette architecture multicouche est couramment appelée « boîte noire », car il est souvent impossible pour ceux qui utilisent la solution de comprendre comment elle est parvenue à la conclusion ou la prédiction formulée (par exemple, de savoir quelles caractéristiques se sont vu attribuer une plus grande pondération dans le processus). Autrement dit, dans la plupart des cas, la logique derrière le choix de la pondération n'est pas transparente ni compréhensible par les êtres humains en raison de l'extrême complexité de l'intelligence artificielle. Il est donc difficile de savoir si le choix des caractéristiques est exhaustif et si leur pondération est raisonnable.

L'une des mesures proposées pour pallier ces problèmes de transparence dans les applications d'intelligence artificielle consiste à expliquer le raisonnement qui sous-tend les solutions, autrement dit : « [d]onner des informations sur le type de données de départ et les résultats attendus, expliquer les variables et les pondérations opérées ou apporter un éclairage sur l'architecture analytique⁴³⁸. »

⁴³² CdE, 2019, p. 2.

⁴³³ Groupe de travail « Article 29 » sur la protection des données de l'UE, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, 2018, p. 28 : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

⁴³⁴ Voir la [section 2.5.1: Principes de licéité, de loyauté et de transparence du traitement](#).

⁴³⁵ Voir la [section 2.10: Information](#).

⁴³⁶ Autorité norvégienne de protection des données, 2018, p. 19.

⁴³⁷ Future of Privacy Forum, 2018, p. 17.

⁴³⁸ Mantelero, 2019, p. 12-13.

Cette approche, appelée « interprétabilité », est centrée sur la compréhension des conséquences qu'a une modification des paramètres d'entrée sur ceux de sortie, sans nécessairement expliquer tout le raisonnement de la machine sur les différentes couches. Dans le cas des boîtes noires, l'interprétabilité est cependant difficile à réaliser la plupart du temps. Il est donc important de faire preuve de transparence envers les personnes concernées à propos des inconnues et des zones d'incertitudes.

16.3.3 MINIMISATION DES DONNÉES

Le principe de minimisation des données exige des organisations qu'elles limitent le traitement des données personnelles au minimum nécessaire en termes de quantité et d'étendue pour atteindre les finalités du traitement⁴³⁹. Dans le cas de l'intelligence artificielle, il peut néanmoins être difficile de savoir à l'avance ce qui est nécessaire⁴⁴⁰, car ces solutions identifient des caractéristiques et des tendances de manière autonome; il n'est donc pas simple de déterminer quel type et quelle quantité de données seront nécessaires à l'exécution d'une tâche spécifique. Puisque les techniques telles que l'apprentissage automatique requièrent de grandes quantités de données pour produire des résultats utiles, seul un certain degré de minimisation sera possible⁴⁴¹. Ces solutions doivent en effet être entraînées à l'aide d'un jeu de données suffisamment large et représentatif, sans quoi elles risquent de produire des résultats biaisés⁴⁴².

Malgré la contradiction apparente entre l'intelligence artificielle et le principe de minimisation des données, il existe diverses mesures d'atténuation. En voici quelques-unes, avec leurs limites éventuelles :

- Adopter des techniques qui rendent plus difficile l'identification des individus à partir des données, par exemple en limitant la quantité et la nature des informations utilisées. Cette approche peut ne pas convenir à certaines solutions d'intelligence artificielle, qui doivent traiter de grandes quantités de données pour fonctionner correctement. De plus, la complexification de l'identification ne peut garantir à elle seule le respect du principe de minimisation des données.
- Utiliser des « données synthétiques » comme données d'apprentissage. Les données synthétiques sont « un jeu de données artificiel qui intégrant des données sur des individus non réels, mais qui reproduit dans les caractéristiques et les liens proportionnels tous les aspects statistiques du jeu de données d'origine⁴⁴³ ». Cette technique présente toutefois des défis elle aussi, les données synthétiques étant obtenues à partir d'un jeu

⁴³⁹ Voir la [section 2.5.4: Principe de minimisation des données](#).

⁴⁴⁰ Centre for Information Policy Leadership, 2018, p. 14.

⁴⁴¹ Mantelero, 2019, p. 8.

⁴⁴² Centre for Information Policy Leadership, 2018, p. 13.

⁴⁴³ Future of Privacy Forum, 2018, p. 8.

de données réelles (nécessaire pour que les données synthétiques puissent être représentatives de la société et de la situation analysées et produire des résultats exacts). C'est pourquoi l'utilisation de jeux de données synthétiques comporte toujours un risque de réidentification.

- Adopter une approche progressive en recueillant ce que l'on pense être la quantité minimale de données requise pour obtenir les résultats prévus, puis en testant la solution pour analyser son fonctionnement. À la suite du test, il est possible d'ajouter des données si nécessaire et de tester à nouveau la solution jusqu'à obtenir les résultats souhaités. Cette approche réduit le traitement inutile de données et permet de faire en sorte que la solution soit entraînée à l'aide du jeu de données le plus petit possible, tout en rendant la réidentification plus difficile.

Malgré les défis que pose l'intelligence artificielle en termes de minimisation de données, ce principe n'interdit pas le traitement de données à grande échelle : il attire l'attention sur les risques élevés qu'il comporte et qui nécessitent la mise en œuvre de mesures appropriées en matière de sécurité et d'atténuation. Par ailleurs, comme indiqué précédemment, toutes les solutions d'intelligence artificielle n'ont pas nécessairement besoin de traiter de grandes quantités de données pour être précises. Par exemple, les solutions fondées sur l'apprentissage par renforcement peuvent être entraînées avec peu de données, voire aucune.

16.3.4 CONSERVATION DES DONNÉES

Les données personnelles ne doivent pas être conservées plus longtemps que nécessaire aux finalités pour lesquelles elles sont traitées⁴⁴⁴. Cependant, une fois la durée de conservation écoulée, les données personnelles sont effacées et ne peuvent donc plus être utilisées pour entraîner le système, le déployer ou assurer son suivi, trois processus susceptibles d'améliorer ses performances⁴⁴⁵. Si un modèle présente des biais, par exemple, il peut être utile d'avoir les données à disposition pour comprendre quelles caractéristiques ont été mal pondérées et entraîner de nouveau la solution afin d'obtenir des résultats plus justes. Malgré les avantages liés au stockage prolongé de données pour les solutions d'intelligence artificielle, les responsables du traitement doivent veiller à ne pas conserver les données personnelles plus longtemps que nécessaire et s'assurer que les données restent à jour tout au long de la période de conservation afin de réduire le risque d'inexactitudes⁴⁴⁶. Étant donné la large gamme d'utilisations possibles de l'intelligence artificielle dans le secteur humanitaire, il convient de définir des durées de conservation propres à chaque programme. À cet égard, les organisations humanitaires devraient déterminer et établir une durée de conservation initiale, par exemple une période de deux ans à des fins d'audit. Si les données sont encore

⁴⁴⁴ Voir la [section 2.7 : Conservation des données](#).

⁴⁴⁵ Centre for Information Policy Leadership, 2018, p. 15.

⁴⁴⁶ Groupe de travail « Article 29 » sur la protection des données de l'UE, 2018, p. 12.

nécessaires à l'issue de cette période initiale, les organisations doivent évaluer périodiquement les besoins de conservation et réfléchir à un fondement juridique autorisant la modification de la durée de conservation. Elles doivent également obtenir le consentement des personnes concernées, si leurs données sont conservées pour une durée plus longue que celle convenue au moment de la collecte.

16.3.5 SÉCURITÉ DES DONNÉES

La sécurité des données⁴⁴⁷ est un aspect essentiel de la mise en œuvre d'une solution d'intelligence artificielle, en particulier dans le secteur humanitaire. Les organisations humanitaires doivent être conscientes des risques liés à ces technologies et assurer le niveau de sécurité des données le plus élevé possible lors de leur utilisation. Les attaques perpétrées par des parties malveillantes rentrent généralement dans l'une des trois catégories suivantes :

- **attaques par inversion de modèle :** tentatives de déduire des informations sur les données d'apprentissage en inversant le modèle du système ;
- **attaques par empoisonnement :** tentatives de diminuer l'utilité du modèle ;
- **attaques par porte dérobée :** tentatives d'obtenir un accès non autorisé à la solution pour la modifier après l'apprentissage.

Pour ce qui est de l'inversion de modèle, il a été démontré que certains systèmes se souviennent de leurs jeux de données d'apprentissage. Par exemple, si le visage d'une personne est utilisé pour entraîner un système de reconnaissance faciale, une partie malveillante pourrait interroger le système de manière répétée, en changeant progressivement l'image d'entrée, afin de reconstituer le visage de manière suffisamment précise pour déterminer que la personne en question faisait partie du jeu d'apprentissage⁴⁴⁸.

Un autre type d'attaques délibérées consiste à ajouter du bruit aux données pour diminuer la qualité des résultats, ce qui peut parfois même conduire à des résultats inexploitable, comme des classifications ou des prédictions erronées.

Tous ces facteurs signifient qu'une sécurité inadéquate des données peut engendrer des risques importants pour les individus vulnérables dans le contexte de l'utilisation de l'intelligence artificielle. Compte tenu de ces risques, il est important de mettre en place des systèmes solides et sécurisés qui protègent efficacement les solutions contre tout accès non autorisé. Par exemple, il peut être utile de recourir à des techniques de pseudonymisation et de chiffrement. Bien que les techniques d'apprentissage des modèles à partir de données chiffrées n'en soient qu'à leurs

⁴⁴⁷ Voir la [section 2.8 : Sécurité des données et sécurité du traitement](#).

⁴⁴⁸ M. Fredrikson, S. Jha et T. Ristenpart, « Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures », *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, p. 1322-1333 : <https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf>.

débuts, les modèles statiques recevant des données d'entrée chiffrées et produisant des données de sortie chiffrées sont déjà couramment utilisés, malgré leurs limites. Le recours à la confidentialité différentielle⁴⁴⁹ devrait également être envisagé pour l'apprentissage des solutions d'intelligence artificielle.

16.4 DROITS DES PERSONNES CONCERNÉES

Les responsables du traitement doivent déterminer les moyens et les finalités du traitement et veiller à ce que les personnes concernées puissent exercer leurs droits⁴⁵⁰. Bien que ces obligations soient plus difficiles à respecter en cas d'utilisation de solutions d'intelligence artificielle, le choix de telles solutions pour atteindre un objectif particulier ne libère pas les responsables du traitement de leurs responsabilités. Les organisations humanitaires doivent donc mettre en place des procédures et des systèmes pour faire en sorte que chaque personne puisse exercer ses droits. Elles doivent également satisfaire aux principes de protection des données dès la conception et par défaut (voir la section 16.7 ci-dessous). Comme évoqué à la section 2.11 de ce manuel, l'exercice de ces droits peut toutefois être limité dans certaines circonstances.

16.4.1 DROIT À L'INFORMATION

Au même titre que pour les autres technologies, lors de l'utilisation de solutions d'intelligence artificielle, il convient d'indiquer aux personnes concernées⁴⁵¹ : l'identité du responsable du traitement, ses coordonnées et comment le contacter ; la finalité et le fondement juridique du traitement ; les catégories de données personnelles traitées ; leurs droits en tant que personnes concernées (en particulier leur droit d'accès aux données) ; et les mesures de protection liées au traitement des données. Les personnes concernées doivent en outre être informées de l'utilisation de l'intelligence artificielle, de son importance pour le traitement envisagé et des risques, règles et garanties associés au traitement des données⁴⁵².

449 « Les algorithmes dits différentiellement confidentiels résistent aux attaques adaptatives qui utilisent des informations auxiliaires. Ces algorithmes reposent sur l'intégration de bruit aléatoire dans l'ensemble de sorte que toutes les données acquises par un attaquant sont bruitées et imprécises ; il devient alors bien plus complexe de porter atteinte à la vie privée (si ce n'est impossible). » A. Elamurugaiyan, « A Brief Introduction to Differential Privacy », Medium, 31 août 2018 : <https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privacy-eacf8722283b>.

450 Voir la [section 2.11 : Droits des personnes concernées](#).

451 Voir la [section 2.10 : Information](#).

452 Autorité norvégienne de protection des données, 2018, p. 19.

16.4.2 DROIT DE SUPPRESSION

Les organisations doivent tenir dûment compte du droit à la suppression des données lors de la mise en œuvre de solutions d'intelligence artificielle⁴⁵³. Si une personne concernée demande la suppression de ses données, mais que ces dernières ont été utilisées pour entraîner une solution spécifique, celle-ci demeurera fondée sur ces données, même si les données elles-mêmes ont été supprimées. Par conséquent, même si une organisation supprime les données du jeu de données, la solution peut toujours contenir certaines caractéristiques de ces données (du moment qu'elles ont été analysées et comparées à d'autres dans le jeu de données pour créer la solution). Cela peut être problématique en cas d'attaques par inversion de modèle qui dévoileraient les données d'origine, comme expliqué plus haut.

Il convient dès lors de se demander si le fait de supprimer les jeux de données eux-mêmes, sans altérer la solution, constitue une limitation du droit de suppression et, le cas échéant, si cette limitation est justifiée par les circonstances. Indépendamment des défis associés à la suppression, « [l]e droit d'opposition devrait être garanti par rapport au traitement fondé sur des technologies qui influencent les opinions et le développement personnel des individus⁴⁵⁴ ». Néanmoins, il est important de souligner que des raisons valides peuvent limiter ce droit, comme indiqué à la section 2.11 de ce manuel.

16.4.3 DROITS RELATIFS À LA PRISE DE DÉCISIONS AUTOMATISÉE

Les personnes concernées ont le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, c'est-à-dire de « décisions prises par des moyens technologiques et sans aucune intervention humaine⁴⁵⁵ », lorsque ces décisions produisent des effets juridiques ou affectent de manière tout aussi significative les personnes en question.

EXEMPLE :

La prise de décision exclusivement automatisée peut concerner, entre autres, l'imposition d'amendes pour excès de vitesse sur la seule base des preuves fournies par les radars, le refus automatique d'une demande de crédit en ligne ou les pratiques de recrutement en ligne sans aucune intervention humaine⁴⁵⁶.

Ce droit s'explique par « la préoccupation liée aux biais des algorithmes ; la crainte de décisions automatisées incorrectes ou injustifiées fondées sur des données erronées ou incomplètes ; et la nécessité pour les individus de pouvoir obtenir

⁴⁵³ Voir la [section 2.11.4 : Droit de suppression](#).

⁴⁵⁴ CdE, 2019, p. 3.

⁴⁵⁵ *Ibid.*, p. 2.

⁴⁵⁶ *Ibid.*, p. 9.

réparation et contester une décision si un algorithme est incorrect ou injuste⁴⁵⁷ ». Ces préoccupations sont étayées par des exemples, tels que l'affaire des allocations en Suède (mentionnée plus haut), où à la suite de l'erreur d'une solution « des milliers de personnes sans emploi se sont vu refuser à tort des allocations⁴⁵⁸ ». Un problème semblable pourrait survenir dans le secteur humanitaire si des solutions d'intelligence artificielle prenaient des décisions relatives à la sélection des bénéficiaires ou à l'inclusion d'individus dans une population cible dans le cadre d'un programme d'aide. Les bénéficiaires doivent toujours être en droit d'exiger qu'un être humain supervise ces décisions les concernant.

Il convient de souligner que « [p]our qu'il y ait intervention humaine, le responsable du traitement doit s'assurer que tout contrôle de la décision est significatif et ne constitue pas qu'un simple geste symbolique⁴⁵⁹ ». C'est d'autant plus important que ceux qui prennent des décisions risquent de se fier aveuglément aux suggestions d'une solution d'intelligence artificielle, sous prétexte que les algorithmes mathématiques sont théoriquement infaillibles. La présence d'un intervenant humain n'est donc pas en soi suffisante⁴⁶⁰. Il faut aussi que l'intervenant soit capable de réfuter la décision ou la suggestion de la machine.

De la même manière, les intervenants ne comprennent parfois pas entièrement comment le système est parvenu à une décision ou a établi une suggestion spécifique et peuvent donc avoir des difficultés à déterminer si cette dernière est erronée (voir la section 16.3.2.3 sur la transparence ci-dessus). Ils devraient toujours pouvoir examiner l'intégralité des faits et des informations et prendre une décision de manière indépendante, sans tenir compte des résultats donnés par la solution d'intelligence artificielle. Ce n'est toutefois pas toujours simple, car une solution d'intelligence artificielle est capable de traiter bien plus d'informations qu'une personne dans la même situation. Dans ce cas, il peut être judicieux de créer une équipe pluridisciplinaire, composée de spécialistes du secteur et de concepteurs de technologies.

Certains individus, indépendamment de leur niveau d'expertise, peuvent être réticents à l'idée de réfuter les décisions automatisées d'une intelligence artificielle, vu la précision de cette technologie. Par conséquent, il faut aussi réfléchir aux modalités de l'intervention humaine pour que le contrôle de la décision soit « effectué par une personne qui a l'autorité et la compétence pour modifier la décision⁴⁶¹ ». Les organisations doivent donc déterminer si les bénéficiaires accepteraient de faire l'objet de décisions prises de manière automatisée s'ils

⁴⁵⁷ Centre for Information Policy Leadership, 2018, p. 16.

⁴⁵⁸ Wills, 2019.

⁴⁵⁹ Groupe de travail « Article 29 » sur la protection des données de l'UE, 2018, p. 21.

⁴⁶⁰ Mantelero, 2019, p. 11.

⁴⁶¹ Groupe de travail « Article 29 » sur la protection des données de l'UE, 2018, p. 27.

avaient le droit d'exiger une intervention humaine. À défaut, l'intérêt même de l'utilisation de cette technologie pourrait être remis en question.

Quoi qu'il en soit, il est essentiel que les bénéficiaires soient au fait de toute prise de décision automatisée les concernant, notamment de la logique qui sous-tend la solution d'intelligence artificielle ainsi que de l'importance et des conséquences prévues du traitement⁴⁶². Ils doivent aussi pouvoir s'opposer au traitement.

16.5 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

16.5.1 RESPECT DES OBLIGATIONS

Comme expliqué plus haut, l'intelligence artificielle connaît parfois des évolutions que les concepteurs ne peuvent pas entièrement comprendre en raison de l'effet « boîte noire » (voir la section 16.3.2.3). Cela peut soulever des questions concernant le principe de responsabilité du responsable du traitement. Pour mettre en œuvre ce principe, les responsables du traitement doivent respecter les exigences en matière de protection des données et pouvoir démontrer qu'ils ont pris des mesures techniques et organisationnelles adéquates et proportionnées dans le cadre de leurs opérations de traitement respectives⁴⁶³.

16.5.2 RESPONSABILITÉ

La prise de décision automatisée (voir ci-dessus) soulève des problèmes spécifiques en termes de responsabilité. Dans le domaine de la santé, par exemple, on considère souvent les machines comme plus précises que les humains dans le diagnostic de maladies, telles que certains types de cancers, ou l'analyse de radiographies. C'est pourquoi les médecins peuvent se sentir obligés de suivre les recommandations de la machine⁴⁶⁴. Dans ce cas, se pose la question de la responsabilité du diagnostic : qui est responsable, la machine elle-même (à supposer qu'elle soit dotée d'une personnalité juridique), ses concepteurs ou le médecin⁴⁶⁵ ? On peut se poser la même question lorsqu'une organisation humanitaire offre des services médicaux dans une situation d'urgence, par exemple si quelqu'un n'est pas diagnostiqué correctement pendant une épidémie de maladie contagieuse. Une solution pour les organisations pourrait être d'étendre aux algorithmes la logique de la responsabilité du fait des produits, en attribuant ainsi l'entière responsabilité à l'entreprise du concepteur⁴⁶⁶.

⁴⁶² Groupe de travail « Article 29 » sur la protection des données de l'UE, 2018, p. 25.

⁴⁶³ Voir la [section 2.9 : Le principe de responsabilité](#).

⁴⁶⁴ CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, 2017, p. 27 : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.

⁴⁶⁵ *Ibid.*, p. 27.

⁴⁶⁶ Mantelero, 2019, p. 19.

(bien que cette solution puisse être très difficile à négocier en pratique). D'un point de vue éthique, il est aussi important que les organisations comprennent quelles sont leurs propres responsabilités lors du choix d'une technologie et qu'elles les assument vis-à-vis des bénéficiaires.

16.6 TRANSFERT INTERNATIONAL DE DONNÉES

Les données personnelles et les autres types de données traitées par les solutions d'intelligence artificielle traversent couramment les frontières. Cela soulève des questions quant à la protection des données utilisées dans les applications d'intelligence artificielle lors d'un transfert international⁴⁶⁷. Malgré l'existence de mécanismes juridiques reconnus, ces derniers peuvent être pratiquement impossibles à mettre en œuvre dans le contexte de l'intelligence artificielle.

La détermination du droit et de la juridiction applicables peut également s'avérer complexe, du moment qu'une analyse de risque correcte et ciblée est impossible à réaliser – sauf si le choix de la juridiction et du droit est explicitement ancré dans la gouvernance de l'intelligence artificielle. Les principes décrits à la section 4.2 de ce manuel fournissent aux organisations humanitaires des recommandations plus précises sur les transferts internationaux de données dans le contexte de l'intelligence artificielle. La responsabilité du transfert des données est un élément clé à prendre en compte lorsque les organisations s'engagent dans des activités qui impliquent un transfert international de données.

16.7 PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT

La protection des données dès la conception et par défaut implique de concevoir une opération, un programme ou une solution de traitement en y intégrant d'emblée les principes clés de la protection des données de manière à offrir à la personne concernée les meilleures protections possible pour ses données. Ces principes clés de la protection des données sont les suivants :

- licéité, équité et transparence ;
- limitation des finalités ;
- minimisation des données ;
- exactitude ;
- durée de conservation limitée ;
- intégrité et confidentialité (sécurité) ;
- responsabilité.

⁴⁶⁷ Voir le [chapitre 4 : Transfert international de données](#).

Voir le chapitre 2 de ce manuel pour une description générale de ces principes, dont certains sont détaillés à la section 16.3 ci-dessus.

Certaines caractéristiques de l'intelligence artificielle peuvent poser problème pour la mise en œuvre de solutions conformes à la protection des données, comme l'explique la section 16.3 ci-dessus. La conception de solutions qui tiennent compte d'emblée de ces défis et risques est peut-être l'un des moyens les plus efficaces de les éviter ou de les atténuer. Par exemple, la plupart des technologies d'intelligence artificielle fonctionnent en traitant de grandes quantités de données pour apprendre à pondérer les caractéristiques pertinentes, identifier des tendances et entraîner des modèles pour les perfectionner. Ces données sont rarement anonymisées, car l'intelligence artificielle a souvent besoin de jeux de données détaillés pour fonctionner correctement. Cependant, plus l'on ajoute de caractéristiques uniques aux jeux de données, plus elles sont susceptibles d'identifier la personne à laquelle les données se rapportent, soit parce que le modèle déduit plus d'informations que prévu initialement (voir la section 16.3.1), soit parce que le système a subi une attaque délibérée (voir la section 16.3.5). En définitive, la décision d'utiliser ou non des technologies fondées sur l'intelligence artificielle impliquera toujours une mise en balance des avantages potentiels et des risques possibles pour les personnes concernées.

Les données synthétiques (voir plus haut) sont souvent proposées comme solution possible aux problèmes de réidentification. Cette solution n'est toutefois pas infaillible, car les données synthétiques sont issues d'un jeu de données réelles, et si plusieurs caractéristiques uniques du jeu de données d'origine sont conservées, des problèmes de réidentification peuvent toujours survenir. La possibilité de réidentifier des bénéficiaires à partir du modèle est très pertinente également pour le secteur humanitaire, où des individus ou organisations mal intentionnés peuvent tenter d'obtenir les données recueillies par les organisations humanitaires pour cibler des groupes ou personnes vulnérables ou leur nuire. Par ailleurs, la pseudonymisation, l'anonymisation (lorsqu'elle est possible) et les techniques de chiffrement peuvent contribuer à prévenir la réidentification et protéger l'identité des personnes concernées⁴⁶⁸. La combinaison du chiffrement avec la pseudonymisation ou l'utilisation de données synthétiques permet d'ajouter une couche de protection supplémentaire, puisque les attaquants qui réussissent à accéder au système ne peuvent « lire » aucune des informations obtenues sans la clé de déchiffrement.

Les données d'apprentissage doivent aussi se prêter à la finalité de la solution d'intelligence artificielle. Autrement dit, les données sélectionnées doivent être pertinentes pour la tâche envisagée, et des vérifications et mises à jour doivent être effectuées régulièrement pour identifier les données inexacts ou corrompus et les

⁴⁶⁸ Autorité norvégienne de protection des données, 2018, p. 18.

retirer du jeu de données, le cas échéant. L'ajout de nouvelles données est également possible pour éviter les biais (voir la section 16.3.2.2). Il est donc important que les organisations humanitaires collaborent avec les concepteurs pour s'assurer que la solution qu'elles acquièrent ou conçoivent sera applicable et adaptée aux besoins de l'organisation dans un contexte spécifique.

Les organisations humanitaires doivent également collaborer avec les concepteurs sur la question de « l'explicabilité », en particulier lorsqu'elles comptent utiliser des solutions d'intelligence artificielle pour soutenir leur processus décisionnel. Elles doivent être capables d'expliquer aux personnes concernées comment fonctionne la solution, quels en sont les risques éventuels et comment le système d'intelligence artificielle obtient des résultats ; elles doivent aussi connaître les dispositions qui ont été prises pour qu'un intervenant humain puisse examiner ces décisions et suggestions au besoin.

En conclusion, lorsque les organisations humanitaires choisissent de déployer des solutions fondées sur l'intelligence artificielle, elles sont encouragées à investir dans la protection des données dès la conception, qui doit être considérée comme une composante essentielle du processus de conception ou d'acquisition. Cet investissement est sans doute le moyen le plus efficace de garantir le respect des principes de protection des données.

16.8 PROBLÈMES ET CONSIDÉRATIONS ÉTHIQUES

Compte tenu de l'évolution rapide des technologies et du fait que les législations ont généralement un temps de retard par rapport aux changements sociétaux majeurs, il est probable que les lois actuelles ne couvrent pas encore toutes les considérations éthiques relatives aux solutions d'intelligence artificielle. Lorsque les organisations humanitaires décident de concevoir ou d'utiliser une solution de ce type, elles devraient bien entendu déterminer si celle-ci respecte la législation en matière de protection des données et les principes de protection des données dès la conception. Elles devraient aussi et avant tout s'intéresser aux éventuels effets négatifs qu'elle pourrait avoir sur les différents droits fondamentaux des personnes concernées, ainsi qu'aux conséquences éthiques et sociétales du traitement des données⁴⁶⁹.

Les outils fondés sur l'intelligence artificielle présentent de nombreux risques, tels que la présence éventuelle de biais discriminatoires, la difficulté d'établir les responsabilités, le risque d'imprécision du système et les atteintes possibles à la vie privée. De plus, certains concepteurs pourraient entraîner leurs systèmes à l'aide de données obtenues de manière illégale ou par des méthodes contraires à

⁴⁶⁹ A. Mantelero, « Artificial Intelligence and Big Data: A blueprint for a human rights, social and ethical impact assessment », *Computer Law & Security Review*, vol. 34, n° 4, 2018, p. 755 : <https://doi.org/10.1016/j.clsr.2018.05.017>.

l'éthique, par exemple en autorisant les utilisateurs à accéder à leur plateforme ou leurs services uniquement s'ils acceptent que leurs données soient utilisées pour entraîner un modèle d'intelligence artificielle. Cette pratique est d'autant plus préoccupante lorsque les utilisateurs de ces plateformes ou services font partie de groupes vulnérables et qu'ils doivent donner leur consentement pour accéder aux services alors même que l'entreprise ne fait pas preuve de transparence au sujet des données traitées. Pour assurer un déploiement éthique de l'intelligence artificielle, il faut toujours veiller à ce que les données utilisées aient été recueillies conformément aux normes reconnues en matière de droits humains et à ce que les identifiants de la personne et/ou du groupe aient été pseudonymisés.

Les évaluations des risques qui dépassent le périmètre traditionnel de la protection des données pour couvrir un éventail plus large d'intérêts, de normes et de droits éthiques (comme le droit à la non-discrimination⁴⁷⁰) sont d'une grande importance. Les intérêts sociétaux et l'éthique dépassent le cadre législatif, et les organisations doivent tenir compte d'un contexte plus large, notamment des nuances politiques et culturelles. Cela rend l'évaluation des valeurs éthiques plus complexe, plus dépendante du contexte et plus complète que l'évaluation de la seule conformité aux lois en matière de protection des données.

De nombreux efforts ont été entrepris pour définir les principes éthiques applicables au développement de l'intelligence artificielle. On peut citer comme exemple les principes IA d'Asilomar⁴⁷¹ et la Déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle, adoptée lors de la 40^e Conférence internationale des commissaires à la protection des données et de la vie privée⁴⁷². Les chercheurs se penchent également sur les questions d'éthique dans le cadre de l'intelligence artificielle⁴⁷³, et certaines multinationales développent leurs propres ensembles de principes éthiques. Bien qu'il n'y ait pas aujourd'hui d'harmonisation entre ces initiatives ni d'ensemble unique de lignes directrices standard, les principes couvrant aussi bien l'éthique que le droit – comme la transparence, l'équité et la responsabilité (voir la section 16.3 ci-dessus) – semblent constituer une base commune.

Compte tenu de l'impact possible de l'intelligence artificielle, « le comité d'éthique fait l'objet d'une attention grandissante dans les cercles d'IA [intelligence artificielle]⁴⁷⁴ », car ils « peuvent apporter un concours précieux pour aider les

⁴⁷⁰ Mantelero, 2019, p. 14.

⁴⁷¹ Future of Life Institute, « Asilomar AI Principles » : <https://futureoflife.org/ai-principles/>.

⁴⁷² ICDPPC, Déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle : https://edps.europa.eu/sites/edp/files/publication/icdppc40th_ai-declaration_adopted_fr.pdf.

⁴⁷³ Voir par exemple la conférence de l'AMC sur l'équité, la responsabilité et la transparence (<https://www.fatml.org/>), qui a gagné en notoriété ces dernières années.

⁴⁷⁴ Mantelero, 2019, p. 16.

développeurs en intelligence artificielle à concevoir des algorithmes à vocation sociale, fondés sur les droits⁴⁷⁵ ». Pour ce qui est de la composition de ces comités, « [l]orsque les enjeux sociétaux sont considérables, une expertise juridique, éthique ou sociologique, outre des connaissances spécifiques au domaine concerné, est essentielle⁴⁷⁶ ». Les organisations humanitaires pourraient donc envisager la création d'un comité d'éthique pour faciliter la prise en compte de ces questions lors du déploiement de solutions d'intelligence artificielle.

En vue de garantir le respect des normes juridiques et éthiques, les organisations humanitaires devraient suivre les deux étapes ci-dessous.

- Tout d'abord, elles devraient répondre aux trois questions suivantes lors de l'AIPD :
 - Que faut-il faire concrètement ?
 - Qu'est-ce qui est autorisé d'un point de vue juridique ?
 - Qu'est-ce qui est possible d'un point de vue technique ?
- Ensuite, lorsqu'elles choisissent d'utiliser de nouvelles technologies, elles devraient réfléchir aux problèmes qui se posent et déterminer si l'intelligence artificielle peut les résoudre, à l'aide des questions suivantes :
 - Quels problèmes l'intelligence artificielle résout-elle ?
 - Quels problèmes ne résout-elle pas ?
 - Quels problèmes crée-t-elle ?
 - Quels résultats cette technologie permet-elle d'obtenir par rapport à d'autres technologies peut-être moins risquées ?

L'option zéro (ne pas utiliser l'intelligence artificielle) devrait toujours être envisageable, en particulier lorsque l'utilisation de l'intelligence artificielle serait légale, mais inacceptable sur le plan éthique. Par exemple, si la solution choisie par l'organisation n'est pas bien accueillie par les bénéficiaires visés par le programme, ce sentiment d'inconfort ou de méfiance peut être un motif suffisant pour renoncer au déploiement de la technologie.

⁴⁷⁵ *Ibid.*, p. 17.

⁴⁷⁶ *Ibid.*, p. 17.



ANNEXE I

MODÈLE DE RAPPORT D'AIPD

Page de couverture

- Analyse d'impact relative à la protection des données concernant [nom de l'activité]
- Personne à contacter, fonction et adresse électronique
- Date

Résumé

Une AIPD de plus de 20 pages doit contenir un résumé qui explique précisément pourquoi, pour qui et par qui elle a été entreprise, et présente les principaux constats et recommandations.

Introduction et vue d'ensemble de l'AIPD

L'introduction doit indiquer le périmètre de l'AIPD, en précisant également quand, pourquoi, pour qui et par qui elle a été réalisée. Elle doit donner des informations sur l'activité évaluée et présenter la méthodologie employée (par exemple, la méthode choisie pour dialoguer avec les parties prenantes).

Évaluation du seuil

Cette section doit énumérer les questions traitées par l'organisation humanitaire pour déterminer si une AIPD était nécessaire et son ampleur.

Description de l'activité ou du projet à évaluer

La description de l'activité à évaluer doit indiquer qui entreprend l'activité et quand elle doit être entreprise. Elle doit préciser qui sera touché par l'activité, mais aussi quelles personnes pourraient être intéressées ou touchées par celle-ci. La description doit donner des informations contextuelles sur la manière dont l'activité s'intègre avec les autres services ou activités de l'organisation humanitaire.

Flux d'informations

Cette section doit donner des informations détaillées au moins sur les points suivants :

- le type de données à recueillir,
- si des informations sensibles seront recueillies,
- comment les données seront recueillies,
- pour quelles finalités les données seront utilisées,
- comment et où les données seront stockées et/ou sauvegardées,
- qui aura accès aux données personnelles,
- si des données personnelles seront divulguées,
- si des données personnelles sensibles seront divulguées,
- si des données seront transférées à d'autres organisations ou pays.

Respect des lois, des règlements, des codes et des lignes directrices

Le rapport d'AIPD doit préciser les lois, les règlements, les codes de conduite et les lignes directrices que l'activité respecte ou devrait respecter. Au niveau mondial, les principes de protection de la vie privée énoncés dans la norme ISO/IEC 29100:2011

de l'Organisation internationale de normalisation (ISO)⁴⁷⁷ sont une référence utile dans une AIPD. En outre, le rapport d'AIPD doit indiquer comment il respecte les règles de confidentialité et les codes de conduite de l'organisation humanitaire et comment l'organisation humanitaire s'assure de ce respect.

Analyse des parties prenantes

Le rapport doit identifier les principales parties prenantes intéressées ou touchées par le traitement des données et exposer les critères retenus pour établir cette liste.

Impacts (risques) pour la protection des données

Cette section doit détailler les risques d'atteinte à la vie privée qui ont été identifiés en relation avec les principaux principes de protection de la vie privée énoncés dans la législation applicable ainsi que dans les règles de confidentialité et les codes de conduite de l'organisation humanitaire.

Évaluation des risques

Cette section doit préciser les modalités d'évaluation des risques et présenter les résultats de l'évaluation réalisée.

Questions organisationnelles

Le rapport d'AIPD doit comprendre une section décrivant comment la direction de l'organisation intervient dans les décisions relatives à la protection des données. Cette section comportera une analyse des aspects organisationnels directement ou indirectement affectés par l'activité de traitement des données. Par exemple, il peut apparaître que le traitement des données exige de mettre en place un mécanisme organisationnel pour garantir le respect du principe de responsabilité, c'est-à-dire qu'un haut dirigeant doit s'assurer que le programme n'a pas de répercussions négatives pour l'organisation humanitaire ou pour ses parties prenantes.

Au cours de l'AIPD, l'équipe de l'AIPD peut se rendre compte que l'organisation humanitaire a besoin de consacrer plus de temps à sensibiliser les employés au respect de la vie privée ou aux questions éthiques et d'accorder une place plus importante à la protection des données dans son organisation. Le rapport doit préciser quelles mesures elle envisage de prendre pour sensibiliser les employés à la protection des données et comment il serait possible de mieux les sensibiliser.

Le rapport doit indiquer comment l'organisation humanitaire détecte les incidents de protection des données, par exemple les atteintes à la protection des données, quelle suite elle donne à ces incidents (enquête, mesures) et comment elle en informe les parties touchées et comment elle en tire des leçons.

⁴⁷⁷ <https://www.iso.org/fr/standard/45123.html>.

Cette section doit aussi décrire comment l'organisation humanitaire répond aux demandes d'accès à des informations personnelles ou de correction ou rectification des informations qu'elle a recueillies, et préciser à qui les données sont transférées et quelles garanties elle exige avant d'effectuer un transfert.

Résultat des consultations

Le rapport doit indiquer les mesures prises par l'organisation humanitaire pour consulter les parties prenantes, pour recueillir leurs avis et leurs idées sur les impacts potentiels pour la protection des données, comment elles pourraient être affectées (en bien ou en mal) par le traitement des données et comment les incidences négatives pourraient être atténuées, évitées, minimisées, éliminées, transférées ou acceptées.

L'équipe chargée de l'AIPD doit préciser quelles techniques de consultation ont été déployées (enquêtes, entretiens, groupes de discussion, ateliers, etc.), quand les consultations ont été menées, les résultats de chaque consultation et si des divergences d'opinion ont été découvertes lorsque différentes techniques ont été utilisées.

L'AIPD doit préciser qui a été consulté et quels documents d'information l'organisation humanitaire a donnés aux parties prenantes, y compris les familles des personnes portées disparues.

L'AIPD doit indiquer si les consultations ont produit de nouveaux constats et quels efforts l'organisation humanitaire a faits pour tenir compte des vues et des idées des parties prenantes dans la conception de l'activité de traitement des données.

Recommandations

L'équipe chargée de l'AIPD doit énoncer ses recommandations pour éviter, minimiser, transférer ou partager les risques en matière de protection des données. Certains risques peuvent mériter d'être pris; l'AIPD doit alors expliquer pourquoi. L'AIPD doit préciser qui assumera le risque (l'organisation humanitaire, les parties prenantes ou d'autres?). Il faut également indiquer quels autres travaux sont nécessaires ou souhaitables pour mettre en œuvre ses recommandations (par exemple, l'AIPD doit mentionner la nécessité d'un suivi indépendant de ses recommandations par un tiers).

L'AIPD doit aussi formuler des recommandations sur l'opportunité ou non de rendre public le rapport d'AIPD. Il arrive dans certaines circonstances qu'il ne soit pas souhaitable de publier le rapport d'AIPD ou certaines de ses parties, par exemple pour des raisons de confidentialité ou de sécurité. Le rapport peut souvent être expurgé de certains passages, puis rendu public, ou les parties sensibles peuvent être regroupées dans une annexe confidentielle. Une autre solution consiste à établir un résumé du rapport.

ANNEXE II

PARTICIPANTS AUX ATELIERS

Tous les ateliers ont été coorganisés par le Brussels Privacy Hub et le CICR. Les représentants des organisations suivantes y ont participé :

- Barclays
- Commission de la protection de la vie privée (Belgique)
- Biometrics Institute
- Brussels Privacy Hub
- Croix-Rouge canadienne
- Cash Learning
- Conseil de l'Europe
- Conseil de l'UE
- Dalberg Data Insights
- Médecins sans frontières
- Autorité de surveillance de l'AELE
- Engine Room
- Commission européenne, DG ECHO
- Commission européenne, DG Justice
- Contrôleur européen de la protection des données
- European UAV-Knowledge Area
- Facebook
- Fairphone
- Association francophone des autorités de protection des données personnelles
- Commission Nationale de l'Informatique et des Libertés
- Gouvernement du Luxembourg
- GSMA
- Harvard Humanitarian Initiative
- Human Rights Watch
- ID2020
- Comité international de la Croix-Rouge
- Fédération internationale de la Croix-Rouge
- Organisation internationale pour les migrations
- UIT
- KU Leuven
- MasterCard
- Mercy Corps
- Microsoft
- MIT
- Croix-Rouge néerlandaise
- Croix-Rouge norvégienne
- Orange Business Services
- Oxford University
- Politecnico di Torino
- Privacy International
- Queen Mary University of London
- Ryerson University - Privacy by Design Centre of Excellence

- École Royale Militaire, Belgique
- Sensometrix
- SES
- Agence espagnole pour la protection des données
- Préposé fédéral à la protection des données et à la transparence
- École polytechnique fédérale de Lausanne
- UN Global Pulse
- Bureau du Rapporteur spécial de l'ONU sur le droit à la vie privée
- Haut Commissaire des Nations Unies pour les réfugiés
- Bureau de la coordination des affaires humanitaires des Nations Unies
- Université de Genève
- USAID
- VIVES University College
- Vrije Universiteit Brussel
- Programme alimentaire mondial
- World Vision International
- Yale University

Le CICR porte assistance aux personnes touchées par un conflit armé ou d'autres situations de violence partout dans le monde, mettant tout en œuvre pour améliorer leur sort et protéger leur vie et leur dignité, souvent en collaboration avec ses partenaires de la Croix-Rouge et du Croissant-Rouge. Il s'efforce en outre de prévenir la souffrance par la promotion et le renforcement du droit et des principes humanitaires universels.

 facebook.com/icrcfrancais

 twitter.com/cicr_fr

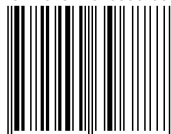
 instagram.com/icrc



CICR

Comité international de la Croix-Rouge
19, avenue de la Paix
1202 Genève, Suisse
T +41 22 734 60 01
shop.icrc.org
© CICR, mai 2021

ISBN 978-2-940396-88-7



9 782940 396887 >