h e g

Haute école de gestion
Genève

Structurer la veille en contexte humanitaire : proposition d'un modèle intégrant sécurité de l'information, protection des données et traçabilité des sources

mémoire réalisé par :

Charlotte CHUARD

Sous la direction de :

Stéphanie HAESEN

Genève, 15 juillet 2026

Information Science

Haute École de Gestion de Genève (HEG-GE)

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Déclaration

Ce mémoire est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre Bachelor of Science HES-SO en Information Science.

L'étudiant atteste avoir soumis son travail à un logiciel de détection de plagiat. Il accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le mémoire, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au mémoire, du juré et de la HEG.

« J'atteste que le présent travail a été réalisé en utilisant uniquement les sources citées dans la bibliographie, qu'il est le fruit de ma réflexion personnelle et a été rédigé de manière autonome. »

Fait à Genève, le 14 juillet 2026

Charlotte CHUARD

Remerciements

Je tiens à exprimer ma sincère reconnaissance à toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce travail.

Mes remerciements s'adressent d'abord à Madame Stéphanie Haesen, pour son accompagnement tout au long de ce projet et pour ses conseils avisés.

Je remercie chaleureusement Madame Lorraine Schilling, qui m'a encadrée durant le stage à l'origine de ce travail. L'idée de ce projet est née de cette expérience, et son soutien constant m'a été d'une aide précieuse jusqu'à son aboutissement.

Ma gratitude va également à Madame Lisa Ferreira, pour l'intérêt qu'elle a porté à ce travail et pour le temps qu'elle a consacré à m'aider dans mes recherches documentaires.

Je remercie mes amis, pour leur écoute, leur aide et leur relecture attentive de ce travail.

Enfin, je tiens à remercier l'ensemble des organisations qui ont participé, directement ou indirectement, à ce projet, et sans lesquelles cette recherche n'aurait pas été possible.

Résumé

En une décennie, la veille est devenue un instrument stratégique de l'action humanitaire, permettant d'anticiper les besoins, de coordonner les interventions et d'assurer la sécurité des équipes comme des populations assistées. Cette centralité s'accompagne d'une exposition accrue aux risques informationnels comme la désinformation, les cyberattaques ou le détournement de données sensibles. Or les dispositifs existants privilégient la rapidité de collecte au détriment de trois exigences essentielles : la sécurité de l'information, la protection des données et la traçabilité des sources, le plus souvent traitées de manière fragmentée. Ce travail vise à dépasser cette fragmentation en proposant un modèle conceptuel de veille qui intègre ces trois dimensions de façon cohérente et systématique, tout en restant adapté aux contraintes opérationnelles du secteur.

La démarche, hybride, combine recherche théorique et modélisation. Un état de l'art retrace l'évolution de la veille humanitaire, ses acteurs, ses plateformes et standards (HDX, KoBoToolbox, guidelines de gestion de l'information) et les cadres de sécurité, de protection et de traçabilité qui s'y appliquent. Un diagnostic empirique mixte confronte ensuite ce cadre au terrain : une enquête par questionnaire auprès de neuf répondants issus de huit organisations, des entretiens semi-directifs et deux études de cas documentées (cyberattaque contre le CICR en 2022, séisme en Turquie et en Syrie de 2023).

Le diagnostic dégage quatre constats : l'urgence opérationnelle prime systématiquement sur la procédure ; la désinformation est perçue comme un risque majeur mais reste rarement protocolarisée ; les outils tiers commerciaux dominent le stockage au détriment de la souveraineté des données ; et le budget conditionne fortement les choix technologiques. La maturité informationnelle apparaît par ailleurs davantage liée à la spécialisation des organisations qu'à leur taille.

Ces constats fondent le modèle TRIVAH (Traçabilité - Résilience Informationnelle - Veille Adaptée à l'Humanitaire). Guidé par huit principes directeurs, il s'organise autour de trois piliers (sécurité, protection, traçabilité) articulés dans un cycle en six phases, du cadrage à la destruction documentée des données. Une fiche d'identité informationnelle accompagne chaque information et matérialise les trois dimensions tout au long de son cycle de vie. Le modèle comprend en outre une classification de sensibilité à quatre niveaux, quatre protocoles de décision pour les situations de tension entre piliers et une grille d'auto-évaluation de maturité à cinq niveaux, dont un profil d'entrée à coût nul.

Sa pertinence est établie par une validation conceptuelle à trois niveaux (confrontation à des cas réels, benchmark et mise en regard de l'enquête), sa mise à l'épreuve en conditions réelles restant une perspective ouverte. Au-delà du modèle, le travail documente des pratiques rarement rendues publiques et propose des outils directement mobilisables par les praticiens.

Mots-clés : veille humanitaire ; gestion de l'information ; sécurité de l'information ; protection des données ; traçabilité des sources ; gouvernance informationnelle ; désinformation ; éthique humanitaire ; intelligence informationnelle ; organisations humanitaires internationales ; modèle conceptuel ; TRIVAH.

Table des matières

Déclaration i
Remerciements ii
Résumé iii
Table des matières iv
Liste des tableaux vi
Liste des figures vii
Liste des acronymes viii
1. Introduction 1
1.1 Problématique 1
1.2 Questions de recherche 1
1.3 Objectifs du travail 2
1.4 Positionnement du travail 3
1.5 Méthodologie 3
2. Contexte général 9
2.1 Évolution du secteur humanitaire 9
2.2 Importance stratégique de la veille 10
3. Cadre théorique 12
3.1 La veille : définitions et modèles 12
3.2 La veille humanitaire : état de l'art 15
3.3 Gestion de l'information humanitaire 18
3.4 Sécurité de l'information humanitaire 19
3.5 Protection des données humanitaires 21
3.6 Traçabilité et fiabilité des sources 23
4. Terrain professionnel 26
4.1 Présentation du terrain documentaire 26
4.2 Études de cas humanitaires documentées 30
4.3 Enquête auprès des organismes 32
4.4 Résultat d'analyse 34
5. Proposition d'un modèle conceptuel de veille humanitaire 40
5.1 Objectifs du modèle 40
5.2 Principes directeurs 40
5.3 Structure du modèle 41
5.4 Le cycle de veille intégré TRIVAH 46
5.5 Matrice des risques par phase 47
5.6 Grille d'auto-évaluation de maturité 48
5.7 Protocoles de décision en cas de conflit entre piliers 51

5.8 Innovations par rapport à l'existant 53
5.9 Déclinaison par contexte opérationnel 54
5.10 Limites et conditions de mise en œuvre 55
6. Validation conceptuelle du modèle 57
6.1 Validation par confrontation aux études de cas 57
6.2 Validation par benchmark 59
6.3 Mise en regard avec les résultats de l'enquête 61
6.4 Synthèse de la validation 62
7. Discussion 64
7.1 Apports du modèle 64
7.2 Limites du travail 64
7.3 Conditions de mise en œuvre en pratique 66
7.4 Réflexion critique 66
7.5 Perspectives de recherche 67
8. Conclusion 69
8.1 Synthèse des résultats 69
8.2 Réponse à la problématique 69
8.3 Contributions du travail 70
8.4 Ouverture 70
Bibliographie 71
Utilisation d'outils assistés par l'intelligence artificielle 76
Annexe 1 : Questionnaire 77
Annexe 2 : Guide d'enquête 91
Annexe 3 : Guide d'entretien 97
Annexe 4 : Matrices d'analyse 98
Annexe 5 : Schémas du modèle proposé 103
Annexe 6 : Guide de recommandation 104

Liste des tableaux

Tableau 1 : Canaux de diffusion du questionnaire et résultats observés 4
Tableau 2 : Typologie des motifs de refus et de non-réponse 5
Tableau 3 : Liste comparative des plateformes d'information humanitaire 14
Tableau 4 : Analyse comparative des outils de veille humanitaire 29
Tableau 5 : Profil des répondants 32
Tableau 6 : Finalités du monitoring déclarées par les répondants 34
Tableau 7 : Niveaux de maturité auto-évalués par organisation 36
Tableau 8 : Synthèse des résultats de l'enquête par dimension 38
Tableau 9 : Mesures de sécurité par niveau de sensibilité 42
Tableau 10 : Le cycle de veille intégré 46
Tableau 11 : Matrice des risques 47
Tableau 12 : Grille d'auto-évaluation de maturité 48
Tableau 13 : Déclinaison contextuelle du modèle TRIVAH 54
Tableau 14 : Application du modèle TRIVAH au cas CICR 2022 57
Tableau 15 : Application du modèle TRIVAH au cas séisme Turquie-Syrie 2023 58
Tableau 16 : Benchmark comparatif 59
Tableau 17 : Mise en regard des constats 61

Liste des figures

Figure 1 : Analyse d'outils 29
Figure 2 : Classification de sensibilité 42
Figure 3 : Analyse d'impact relative à la protection des données systématisée 44
Figure 4 : Pilier sécurité 49
Figure 5 : Pilier protection 50
Figure 6 : Pilier traçabilité 50
Figure 7 : Cas 1, protocole TRIVAH 51
Figure 8 : Cas 2, protocole TRIVAH 52
Figure 9 : Cas 3, protocole TRIVAH 52
Figure 10 : Cas 4, protocole TRIVAH 53
Figure 11 : Séquence recommandée 56

Liste des acronymes

Organisations et institutions :

- **ACAPS** : Assessment Capacities Project.
- **CICR** : Comité international de la Croix-Rouge.
- **FICR / IFRC** : Fédération internationale des sociétés de la Croix-Rouge et du Croissant-Rouge.
- **HCR / UNHCR** : Haut-Commissariat des Nations Unies pour les réfugiés.
- **IASC** : Inter-Agency Standing Committee
- **MSF** : Médecins Sans Frontières.
- **OCHA** : Bureau de la coordination des affaires humanitaires des Nations Unies.
- **OIG** : Organisation Intergouvernementale.
- **ONG** : Organisation Non Gouvernementale.
- **PAM / WFP** : Programme alimentaire mondial.
- **UNDRR** : Bureau des Nations Unies pour la réduction des risques de catastrophes.
- **UNICEF** : Fonds des Nations Unies pour l'enfance.
- **UNOSAT** : Centre satellitaire des Nations Unies.

Concepts techniques et outils humanitaires :

- **AAP** : Accountability to Affected Populations
- **APT** : Advanced Persistent Threat
- **BIMS** : Biometric Identity Management System
- **CHS** : Core Humanitarian Standard (norme humanitaire fondamentale).
- **HDX** : Humanitarian Data Exchange (plateforme de partage de données d'OCHA).
- **HXL** : Humanitarian Exchange Language (standard de balisage sémantique).
- **IM** : Information Management
- **IoT** : Internet of Things
- **mVAM** : mobile Vulnerability Analysis and Mapping (analyse de la vulnérabilité par téléphonie mobile du PAM).
- **OPSEC** : Operational Security
- **OSINT** : Open Source Intelligence
- **PRIMES** : Population Registration and Identity Management EcoSystem (Écosystème de gestion des identités du HCR).
- **SDC** : Statistical Disclosure Control (Contrôle de la divulgation statistique pour l'anonymisation).

Rôles professionnels :

- **CDO** : Chief Digital Officer
- **DPO** : Data Protection Officer
- **MEAL** : Monitoring, Evaluation, Accountability and Learning
- **RSSI** : Responsable de la sécurité des systèmes d'information.

Autres termes techniques et informatiques :

- **API** : Application Programming Interface
- **CATI / IVR** : Computer Assisted Telephone Interviewing / Interactive Voice Response
- **CISA** : Cybersecurity and Infrastructure Security Agency
- **DPIA** : Data Protection Impact Assessment
- **EDI** : Échange de données informatisé
- **EXIF** : Exchangeable Image File Format
- **MFA** : Multi-Factor Authentication
- **NLP** : Natural Language Processing
- **RGPD** : Règlement Général sur la Protection des Données.
- **RFID** : Identification par radiofréquence
- **UAV** : Unmanned Aerial Vehicle

1. Introduction

En une décennie, la gestion de l'information est devenue un enjeu central de l'action humanitaire. Les organisations qui interviennent en contexte de crise s'appuient désormais sur des dispositifs de veille pour anticiper les besoins, coordonner leurs réponses et préserver la sécurité de leurs équipes comme des populations qu'elles assistent. Cette montée en puissance de l'information s'accompagne toutefois d'une vulnérabilité nouvelle : les données humanitaires, souvent sensibles, circulent dans un environnement marqué par la désinformation, les cybermenaces et le risque de détournement à des fins de surveillance ou de répression.

Dans ce contexte, la veille ne peut plus être pensée comme une simple activité de collecte. Elle engage des exigences de sécurité de l'information, de protection des données et de traçabilité des sources qui, aujourd'hui encore, sont le plus souvent traitées séparément. C'est à cette fragmentation que le présent travail s'intéresse, en cherchant à comprendre comment ces trois dimensions peuvent être articulées au sein d'un dispositif de veille cohérent, sans sacrifier la réactivité qu'impose le terrain.

Ce premier chapitre expose la problématique et les questions de recherche qui structurent le travail, précise ses objectifs et son positionnement, puis détaille la méthodologie mixte adoptée pour y répondre.

1.1 Problématique

Si la veille est aujourd'hui reconnue comme un outil stratégique essentiel pour les organisations humanitaires, sa mise en œuvre soulève de nombreux défis informationnels. Les dispositifs existants privilégient souvent la rapidité de collecte et la couverture des sources, au détriment de questions essentielles telles que la traçabilité de l'information, la fiabilité des sources, la sécurisation des flux informationnels et la protection des données sensibles.

Dans un contexte international marqué par la désinformation, les cybermenaces et les risques d'exploitation des données humanitaires (tels que la surveillance ciblée de populations vulnérables ou le détournement tactique de métadonnées à des fins de répression politique ou militaire), l'absence d'un cadre conceptuel intégré peut fragiliser la qualité des analyses produites et, par conséquent, les décisions opérationnelles qui en découlent. La littérature professionnelle montre par ailleurs que les approches actuelles abordent fréquemment la veille, la sécurité de l'information et la protection des données de manière fragmentée.

1.2 Questions de recherche

Dès lors, la question centrale de ce travail est la suivante :

Comment structurer un dispositif de veille menée par les organisations humanitaires qui intègre de manière cohérente et systématique les exigences de sécurité de l'information, de protection des données et de traçabilité des sources, tout en restant adapté aux contraintes opérationnelles du secteur humanitaire ?

Cette problématique appelle une réflexion conceptuelle approfondie, appuyée sur l'analyse des pratiques documentées et des cadres de référence existants.

1.3 Objectifs du travail

Le but de ce travail est de proposer un modèle conceptuel de veille intégrant les dimensions de sécurité de l'information, de protection des données et de traçabilité des sources. Par traçabilité, il convient d'entendre ici l'implémentation de protocoles visant à documenter l'origine de l'information, ses modalités de collecte ainsi que l'intégralité de son cycle de vie, incluant les étapes de traitement et de validation. Cette approche permet d'identifier des axes d'amélioration vis-à-vis des dispositifs existants. Afin de garantir la pertinence de ce travail, une série d'objectifs et de sous-objectifs a été définie ; celle-ci permet de délimiter le périmètre de l'étude et de répondre aux exigences académiques et opérationnelles fixées.

1.3.1 Dresser un état de l'art de la veille humanitaire

- Réaliser une revue systématique de la littérature scientifique et des publications professionnelles afin de définir les fondements et les spécificités de la veille dans le secteur humanitaire.
- Identifier les cadres théoriques existants et les concepts clés liés à la veille en contexte de crise.

1.3.2 Réaliser un diagnostic des pratiques informationnelles actuelles

- Conduire une étude empirique mixte :
  - Volet quantitatif : collecter des données via une enquête par questionnaire auprès d'un échantillon diversifié d'organisations humanitaires.
  - Volet qualitatif : approfondir l'analyse par des entretiens semi-directifs avec des experts et professionnels du domaine.
- Évaluer la maturité des dispositifs de veille existants et analyser les cadres méthodologiques actuellement employés.
- Synthétiser les forces, les faiblesses et les besoins non couverts par les pratiques actuelles (bilan de l'existant).

1.3.3 Élaborer un modèle conceptuel structuré de dispositif de veille intégrant les enjeux de gouvernance, de sécurité et d'éthique.

- Analyser la pertinence des systèmes de veille actuels au regard des contraintes spécifiques du terrain humanitaire.
- Déterminer les processus optimaux et les protocoles de sécurité indispensables au traitement de données sensibles.
- Formaliser un modèle conceptuel structuré intégrant les dimensions de gouvernance, de sécurité des données et d'éthique professionnelle.
- Discuter de la pertinence, des apports et des limites de ce modèle au regard des études de cas et des pratiques documentées
- Mener une réflexion critique sur la viabilité, les apports et les limites du modèle proposé face aux réalités opérationnelles documentées.

1.3.4 Formuler des recommandations stratégiques et opérationnelles

- Élaborer un guide de bonnes pratiques destiné aux professionnels de l'information en milieu humanitaire.
- Produire un livrable de synthèse regroupant les conclusions de l'enquête, des pistes de réflexion stratégiques et des préconisations concrètes pour l'implémentation d'un système de veille robuste.

1.4 Positionnement du travail

Ce projet adopte une approche hybride, articulant recherche théorique et modélisation pratique. La démarche méthodologique se décompose comme suit :

- Phase exploratoire (théorie) : une enquête quantitative, diffusée via un questionnaire auprès de diverses ONG ou organisations internationales ou régionales, permettra d'établir un état des lieux des pratiques de veille actuelles. Cette phase sera complétée par une approche qualitative sous forme d'entretiens semi-directifs avec des chargés de veille ou autres responsables ayant un lien avec la veille, visant à approfondir la compréhension des mécanismes de veille.
- Phase de modélisation (pratique) : l'analyse des données recueillies servira de base à l'élaboration d'un modèle conceptuel. Ce dernier visera à formaliser des bonnes pratiques et des protocoles de veille adaptés aux contraintes de sécurité et de confidentialité propres au milieu humanitaire.

1.5 Méthodologie

Afin de répondre à la problématique posée, ce travail adopte une démarche méthodologique structurée en trois phases majeures, s'étendant sur cinq mois. Cette approche mixte, combinant recherche documentaire et investigation empirique, garantit la validité scientifique du modèle proposé.

1.5.1 Phase de recherche

La première phase est consacrée à la construction d'un socle théorique robuste permettant d'ancrer la problématique dans la littérature existante et de délimiter le périmètre du travail.

1.5.1.1 Recherche documentaire

Cette étape consiste en une exploration systématique des ressources académiques et de la littérature grise, tel que les guides institutionnels. Elle vise à identifier les théories de la gestion de l'information, les normes de protection des données applicables au secteur humanitaire et les cadres de cybersécurité existants. Les bases de données bibliographiques spécialisées (LISTA, Web of Science), le catalogue de l'Humanitarian Library et le corpus documentaire du CICR, en particulier son *Handbook on Data Protection in Humanitarian Action*, constituent les sources primaires de cette phase. Le contact de spécialistes de l'information au sein d'organisations humanitaires a permis d'identifier des ressources de littérature grise non référencées dans les bases de données académiques conventionnelles. La recherche a été conduite de manière itérative, chaque lecture nourrissant de nouvelles pistes bibliographiques par la méthode boule de neige.

1.5.1.2 Cadrage du projet

Parallèlement à la recherche documentaire, l'élaboration du cahier des charges permet de définir les limites du sujet, les livrables attendus et le calendrier du travail, assurant ainsi la cohérence de la démarche avec les exigences académiques de la HEG. Cette étape a également donné lieu à la conception des instruments de collecte : le questionnaire (annexe 1), le guide d'enquête (annexe 2) et le guide d'entretien (annexe 3), élaborés de manière itérative et affinés progressivement au fil du travail, en particulier les deux guides.

1.5.2 Phase d'analyse

La deuxième phase constitue le cœur empirique du travail. Elle mobilise une approche mixte articulant un volet quantitatif par questionnaire et un volet qualitatif par entretiens semi-directifs. Ces deux modalités sont complémentaires : le questionnaire fournit une vue d'ensemble statistique des pratiques, tandis que les entretiens permettent de saisir les nuances opérationnelles, les tensions organisationnelles et les besoins non captés par les données chiffrées.

1.5.2.1 Volet quantitatif : enquête par questionnaire

Un questionnaire en ligne de 66 questions a été conçu (cf. Annexe 1 : Questionnaire). Il couvre six axes thématiques : gouvernance informationnelle, pratiques de monitoring, outils mobilisés, traçabilité des sources, sécurité de l'information et perspectives d'évolution. Les questions combinent items à choix unique, choix multiple, échelles de Likert et questions ouvertes permettant aux répondants d'expliciter leurs pratiques au-delà des catégories prédéfinies.

La diffusion a mobilisé six canaux distincts, dont les caractéristiques et les résultats sont détaillés dans le tableau ci-dessous.

Tableau 1 : Canaux de diffusion du questionnaire et résultats observés

Canal de diffusion	Modalité	Résultat observé
Courriel direct	Envoi personnalisé à des responsables d'information, chefs de projet, DPO et responsables MEAL d'organisations identifiées via LinkedIn, sites institutionnels et réseaux professionnels	Taux de réponse faible (~10-15 %) ; plusieurs non-réponses, refus motivés par le contexte sécuritaire ou l'absence de profil interne compétent
Formulaire en ligne institutionnel	Diffusion via les pages de contact des organisations humanitaires	Peu de retours ; majoritairement sans suite
LinkedIn (profil personnel)	Publication d'une annonce de recherche ciblant les professionnels de l'information humanitaire	Quelques partages ; plusieurs prises de contact informelles mais peu de conversions en réponses
SwissLib (liste de diffusion) et réseaux d'associations	Annonce diffusée auprès de la communauté des professionnels suisses de l'information et de la documentation	Pertinence variable ; aucune réponse
Contacts de contacts (bouche-à-oreille)	Recommandations et mises en relation par des personnes ayant répondu ou ayant connaissance du projet	Canal le plus efficace ; à l'origine de plusieurs réponses qualitatives et des entretiens
Relances multiples	Rappels envoyés après 2 et 4 semaines aux organisations contactées n'ayant pas répondu	Effet limité ; quelques réponses tardives obtenues

© Charlotte Chuard 2026

Au total, un peu plus de 50 organisations ont été sollicitées (cf. Annexe 2 : Guide d'enquête). Le taux de réponse effectif est faible, ce qui constitue une limite méthodologique reconnue (cf. chapitre 1.5.3). Neuf réponses exploitables ont été collectées, issues de huit organisations distinctes. Une organisation a été représentée par deux répondants aux profils complémentaires, permettant de croiser des perspectives internes différenciées. Conformément aux engagements pris lors de la diffusion du questionnaire et par souci de protection des organisations participantes, l'ensemble des résultats est présenté de manière anonymisée : chaque organisation est désignée par un code neutre (Org. A à Org. H) dans l'analyse.

Les motifs de refus ou de non-réponse, lorsqu'ils ont été explicités, ont été systématiquement documentés car ils constituent en eux-mêmes une information utile sur les contraintes du terrain. Le tableau suivant en propose une typologie.

Tableau 2 : Typologie des motifs de refus et de non-réponse

Motif de refus / non-réponse	**Explication**	**Profil type concerné**
Contexte sécuritaire ou politique	L'organisation ne peut pas exposer ses pratiques informationnelles dans un contexte de conflit actif ou sous contrainte politique	Organisations actives en zones de conflit armé (Sahel, Moyen-Orient, Ukraine)
Absence de profil compétent en interne	Aucune personne au sein de l'organisation ne se considère suffisamment spécialisée pour répondre à des questions sur la veille informationnelle sécurisée	Principalement petites ONG opérationnelles
Questionnaire trop spécifique	La veille au sein de l'organisation est principalement commerciale ou stratégique (marketing, fundraising) et ne correspond pas au périmètre du questionnaire	ONG à forte composante de communication
Manque de temps / de ressources	Personnel trop sollicité ; questionnaire jugé long pour une période de terrain chargée	Organisations en réponse d'urgence active
Non-réponse sans motif explicité	Aucun retour malgré relances	Environ 30 % des organisations contactées

© Charlotte Chuard 2026

Ces résultats révèlent une réalité structurelle du secteur : la veille informationnelle sécurisée est un domaine suffisamment spécialisé pour que de nombreuses organisations ne disposent pas en interne de personnel capable ou autorisé à se prononcer sur leurs propres pratiques. Ce "silence" confirme que la veille humanitaire sécurisée est un domaine encore peu formalisé

et hautement sensible. Loin d'affaiblir la pertinence du travail, il en renforce au contraire la nécessité.

1.5.2.2 Volet qualitatif : entretiens semi-directifs

Afin d'approfondir les résultats du questionnaire et de saisir les dimensions non quantifiables des pratiques de veille, trois entretiens semi-directifs ont été conduits avec des professionnels de la veille, de la gestion de l'information et de la sécurité des données dans des organisations humanitaires ou proches du secteur. Ces entretiens ont été obtenus à l'issue de contacts approfondis : environ une dizaine de demandes avaient été adressées, la plupart sans réponse, soulignant à nouveau la difficulté d'accès au terrain.

Les entretiens, d'une durée de 30 à 45 minutes, se sont déroulés en présentiel ou à distance selon les disponibilités et contraintes des interlocuteurs. Ils ont été conduits sur la base d'un guide semi-directif (cf. Annexe 3 : Guide d'entretien) structuré autour de cinq thématiques : le but de la veille au sein de l'organisation et son articulation avec la mission opérationnelle ; les outils mobilisés et les critères ayant guidé leur choix ; les limites concrètes des pratiques actuelles, notamment face à la tension entre rapidité et fiabilité de l'information ; les manques perçus comme prioritaires en matière de ressources, de compétences ou de cadre ; et, en clôture, une projection libre sur un système de veille idéal, sans contrainte de faisabilité immédiate. Ce dernier axe visait explicitement à faire des entretiens un moment de validation participative du modèle en construction, en recueillant les attentes des praticiens dès la phase d'élaboration plutôt qu'en les confrontant à un modèle déjà figé.

Les entretiens ont été enregistrés avec l'accord des participants, transcrits et analysés par codage thématique. Les verbatim sont utilisés dans l'analyse de manière anonymisée. Aucun nom, prénom ou identifiant organisationnel n'apparaît dans le présent travail.

1.5.2.3 Traitement et analyse des données

Les données quantitatives issues du questionnaire ont été exportées depuis Google Forms et traitées dans Microsoft Excel. Le traitement comprend : le calcul de fréquences et de pourcentages pour les questions fermées ; la réalisation de diagrammes de répartition illustrant les résultats par dimension thématique (cf. Annexe 4 : Matrices d'analyse) ; la construction d'un tableau comparatif des outils déclarés par organisation (cf. Tableau 4); et l'élaboration d'une matrice de maturité (cf. chapitre 4.4.2) croisant les organisations et les cinq dimensions d'évaluation retenues.

Les données qualitatives issues des entretiens ont fait l'objet d'une analyse de contenu thématique, structurée autour des mêmes axes que le questionnaire pour permettre une mise en regard des deux sources. Les éléments convergents et divergents entre les réponses au questionnaire et les entretiens sont explicitement identifiés dans l'analyse (cf. chapitre 4). Toutes les organisations et tous les participants sont présentés de manière anonymisée dans l'ensemble du document, conformément aux engagements pris lors de la collecte des données.

1.5.3 Phase de finalisation

La troisième phase est celle de la synthèse et de la production intellectuelle. Elle repose sur l'articulation des résultats empiriques et du cadre théorique pour aboutir à la proposition du modèle conceptuel TRIVAH et à la rédaction du mémoire.

Sur la base de l'analyse conduite dans les phases précédentes, un modèle de dispositif de veille sécurisée est élaboré. Ce modèle, nommé TRIVAH (Traçabilité - Résilience Informationnelle - Veille Adaptée à l'Humanitaire), intègre les processus de veille avec des protocoles de sécurité et de traçabilité, articulés autour de trois piliers et d'un cycle en six phases. Sa conception s'appuie directement sur les besoins et les lacunes identifiés dans l'enquête empirique, ainsi que sur les bonnes pratiques documentées lors de l'analyse des dispositifs existants. Le modèle comprend en outre une grille d'auto-évaluation de maturité à dix-huit critères et cinq niveaux et quatre protocoles de décision formalisant les arbitrages entre piliers lorsqu'ils entrent en tension. Il est conçu pour être adopté progressivement, selon un profil d'entrée adapté au niveau de ressources de chaque organisation, en cohérence avec les besoins exprimés par les répondants de l'enquête.

Avant d'être présenté comme proposition finale, le modèle fait l'objet d'une validation conceptuelle en trois volets : une confrontation rétrospective à des études de cas humanitaires, un benchmark comparatif avec cinq cadres de référence du secteur et une mise en regard systématique avec les résultats de l'enquête. Cette démarche de validation ne constitue pas un test en conditions opérationnelles réelles mais permet d'établir la cohérence interne du modèle et sa pertinence apparente au regard des données disponibles.

Parallèlement à la rédaction du mémoire, les résultats du travail sont traduits en un guide de recommandation (cf. Annexe 6 : Guide de recommandation) à destination directe des organisations humanitaires. Conçu comme un outil de transfert de connaissances vers la pratique professionnelle, ce guide reprend les conclusions de l'enquête et les principes du modèle TRIVAH sous une forme accessible, différenciée selon la taille et le niveau de maturité des organisations, sans présupposer de compétences techniques avancées. Il constitue le livrable opérationnel du travail, distinct du mémoire académique qui en est la base scientifique.

La rédaction du mémoire s'étend sur trois mois permettant d'articuler progressivement le cadre théorique, les résultats, la proposition du modèle, sa validation et les perspectives ouvertes par le travail. Une phase de relecture et de finalisation précède le dépôt final.

Le cycle se clôture par une soutenance orale de ce travail en proposant des pistes de réflexions sur le sujet.

1.5.4 Limites méthodologiques

Plusieurs limites inhérentes à la démarche adoptée méritent d'être explicitées, dans un souci de transparence scientifique.

1.5.4.1 Taille de l'échantillon

Avec neuf réponses issues de huit organisations, l'échantillon de l'enquête ne peut prétendre à la représentativité statistique du secteur humanitaire dans son ensemble. Les résultats doivent être lus comme des indicateurs qualitatifs et des tendances, non comme des données généralisables à l'ensemble du secteur. Cette limite est assumée et partiellement compensée par la diversité des profils représentés (types d'organisations, tailles, mandats, zones d'intervention) et par la triangulation avec les données qualitatives des entretiens et l'analyse documentaire.

1.5.4.2 Biais de sélection

Les organisations ayant répondu sont a priori celles dont le personnel est suffisamment sensibilisé aux enjeux de veille informationnelle pour se sentir légitime à répondre. Les organisations les moins matures sur ces questions sont probablement sous-représentées dans l'échantillon, ce qui tend à produire une image du secteur légèrement plus favorable que la réalité. Par ailleurs, la concentration géographique des répondants en Suisse et en Europe occidentale limite la portée des conclusions pour les pratiques dans les pays du Sud global (Boniface 2025).

1.5.4.3 Confidentialité et désirabilité sociale

Les thèmes abordés comme la sécurité des données, les incidents et les pratiques de surveillance, sont sensibles. Certains répondants peuvent avoir atténué ou omis des informations jugées compromettantes pour leur organisation, même sous garantie d'anonymat. Les entretiens semi-directifs permettent partiellement de contourner ce biais, la dynamique conversationnelle favorisant une expression plus nuancée que le questionnaire auto-administré.

1.5.4.4 Accès limité aux pratiques internes

Les données collectées reposent sur des déclarations et auto-évaluations, non sur une observation directe des pratiques. L'écart entre pratiques déclarées et pratiques effectives, bien documenté dans la littérature sur les méthodes d'enquête, constitue une source d'incertitude résiduelle que le présent travail ne peut entièrement éliminer.

2. Contexte général

2.1 Évolution du secteur humanitaire

L'action humanitaire traverse actuellement une période de mutation profonde, marquée par une transformation numérique qui redéfinit les modalités d'assistance et de protection. Ce changement de paradigme, amorcé de manière accélérée au cours de la dernière décennie, n'est pas un simple effet de mode technologique mais répond à des impératifs opérationnels croissants.

2.1.1 L'évolution technologique du secteur

Historiquement centrée sur la présence physique, l'aide humanitaire intègre désormais massivement les technologies de l'information pour gagner en efficacité et en rapidité. Cette évolution est portée par plusieurs facteurs clés :

- L'expansion de la connectivité : une majorité croissante de populations touchées par des crises est désormais connectée, utilisant des smartphones comme outils de survie pour accéder à l'information, aux services et maintenir des liens familiaux.
- La complexité des crises : face à des conflits de plus en plus fragmentés et prolongés, les organisations utilisent la « proximité numérique » pour pallier les difficultés d'accès physique sur le terrain.
- L'optimisation de l'aide : l'usage de la biométrie pour l'enregistrement, des transferts monétaires numériques (Cash and Voucher Assistance) et de l'intelligence artificielle pour l'analyse prédictive permet de mieux cibler les besoins et de limiter les fraudes.

2.1.2 La montée des risques informationnels

Si le numérique offre des opportunités sans précédent, il expose également les organisations et les bénéficiaires à une nouvelle gamme de menaces. La donnée est devenue une ressource aussi précieuse que risquée, faisant de l'espace numérique un nouveau champ de bataille.

- L'augmentation de la surface d'attaque : en numérisant leurs activités, les organisations humanitaires augmentent leur vulnérabilité face aux opérations cyber hostiles. Le piratage sophistiqué visant un prestataire tiers au CICR en 2022, compromettant les données de plus de 500 000 personnes vulnérables, a marqué un tournant dans la prise de conscience du secteur.
- La dépendance envers des tiers : le secteur dépend désormais d'un réseau complexe de prestataires privés (services cloud, télécoms, plateformes financières) qui ne partagent pas nécessairement les principes humanitaires de neutralité et d'impartialité.
- Surveillance et détournement de finalité : les traces numériques laissées par les bénéficiaires peuvent être exploitées par des acteurs étatiques ou des groupes armés à des fins de surveillance, de discrimination ou de répression (phénomène de *function creep*) (Koops 2021, p. 41), transformant des données collectées pour l'aide en outils d'oppression.

2.1.3 La protection des données comme nouvel impératif humanitaire

Dans ce paysage hyperconnecté, la protection des données personnelles est passée d'une fonction administrative de conformité à un pilier fondamental de l'action humanitaire. Elle est intrinsèquement liée au principe de *Do No Harm*, qui est une approche analytique développée

pour éviter que l'aide humanitaire ou le développement n'exacerbent les conflits locaux. La perte de contrôle sur les informations sur les données personnelles sensibles des populations en crise peut entraîner des conséquences physiques et psychologiques réelles, allant jusqu'à mettre des vies en danger.

Le défi actuel pour les organisations est donc de réussir leur mue numérique tout en préservant l'intégrité de l'espace humanitaire numérique, garantissant que les données confiées par les plus vulnérables ne soient utilisées que pour leur protection et leur assistance.

2.2 Importance stratégique de la veille

Dans un environnement marqué par l'instabilité et la complexité croissante des crises, la veille ne se limite pas à une simple recherche documentaire. Elle constitue un processus itératif et organisé de collecte, de traitement et de diffusion d'informations visant à réduire l'incertitude et à soutenir la prise de décision, qu'elle soit stratégique ou opérationnelle. Les quatre dimensions présentées ci-dessous ne constituent pas une typologie normalisée : elles résultent d'une synthèse personnelle de la littérature consultée (notamment les travaux d'OCHA et de l'IASC sur la responsabilité et la coordination des données), organisée pour ce travail afin de structurer l'intérêt stratégique de la veille.

2.2.1 Le fondement de l'action humanitaire fondée sur des preuves

L'importance de la veille réside d'abord dans sa capacité à transformer des données brutes en un fondement solide pour une action dite « evidence-based ». Dans un secteur où les ressources sont limitées face à des besoins croissants, la veille permet :

- L'allocation optimale des ressources : elle aide à identifier avec précision les zones où les besoins sont les plus criants et à arbitrer entre différents programmes.
- La connaissance situationnelle : dans des contextes de conflits fragmentés, l'utilisation d'outils d'analyse de données et d'intelligence artificielle permet de détecter des schémas d'événements et de prévoir l'évolution des crises, comme les déplacements de population ou la propagation de maladies.

2.2.2 Un levier pour la coordination

Le secteur humanitaire est caractérisé par une multitude d'acteurs (ONG, agences onusiennes, États) opérant souvent de manière silotée. La veille partagée devient alors le « ciment de la coordination ». L'utilisation de plateformes de données communes et de standards (tels que ceux de l'IASC ou d'OCHA) permet d'éviter les doublons d'aide et d'harmoniser les efforts de réponse globale. Cette mutualisation de l'information est cruciale pour maintenir un standard élevé de responsabilité des données dans différents environnements opérationnels.

2.2.3 Maintenir la proximité et l'accès

La veille joue un rôle stratégique dans le maintien du lien avec les populations, particulièrement lorsque l'accès physique est entravé.

- La proximité numérique : elle permet aux organisations de rester « connectées » aux communautés via les réseaux sociaux ou les applications de messagerie, offrant ainsi une alternative indispensable à la présence physique pour évaluer les besoins en temps réel.

- La redevabilité envers les populations affectées (AAP) : un dispositif de veille efficace inclut des mécanismes de rétroaction rapide, permettant aux bénéficiaires de devenir des agents actifs de leur propre protection en signalant leurs besoins ou en exprimant leurs préoccupations.

2.2.4 La veille comme outil de gestion des risques

Enfin, la veille est un instrument de protection au sens large. En surveillant les menaces numériques (désinformation, surveillance, cyberattaques), les organisations peuvent anticiper les risques d'atteinte à la vie privée, à la dignité et à la sécurité des bénéficiaires. Elle permet d'appliquer concrètement le principe de *Do No Harm* dans l'espace numérique en s'assurant que la collecte de données ne crée pas de nouvelles vulnérabilités, comme le profilage malveillant ou le détournement de finalité (*function creep*).

En somme, la veille est devenue une capacité stratégique centrale qui conditionne non seulement l'efficacité logistique de l'aide, mais aussi la légitimité et la sécurité de l'action humanitaire dans le cyberespace.

3. Cadre théorique

3.1 La veille : définitions et modèles

La veille se définit comme un processus itératif et organisé de collecte, de traitement et de diffusion d'informations pertinentes visant à réduire l'incertitude et à soutenir la prise de décision stratégique ou opérationnelle. Dans le secteur humanitaire, elle s'inscrit dans une dynamique de gestion de crise où la réactivité et l'anticipation sont primordiales (Dubost et Denis 2020, p. 14). Elle ne se limite pas à une simple recherche documentaire, mais constitue un véritable outil de gestion des risques et de compréhension des contextes d'intervention complexes (Neuilly 2008, p. 61-74). La spécificité du secteur humanitaire réside dans la nature des données traitées, souvent personnelles, sensibles et relatives à des populations en situation de vulnérabilité extrême, ce qui impose des exigences de sécurité et de protection sans équivalent dans d'autres domaines de veille.

3.1.1 Veille stratégique

La veille stratégique consiste en une observation globale de l'environnement (politique, sécuritaire, technologique et juridique) pour anticiper les évolutions majeures pouvant impacter les missions humanitaires. Elle permet aux organisations d'identifier les crises émergentes avant qu'elles n'atteignent un point de rupture.

Elle vise la surveillance des signaux faibles et des tendances de fond. L'utilisation de listes de surveillance des crises, comme celle produite par l'International Rescue Committee (Reuters 2024), permet de prioriser les zones d'intervention selon l'aggravation prévisible des besoins. ACAPS complète cette approche par son « INFORM Severity Index », qui combine 31 indicateurs fondamentaux pour mesurer la sévérité des crises humanitaires à l'échelle mondiale, et par son «Global Humanitarian Access Index », publié semestriellement, qui évalue les obstacles à l'accès humanitaire dans plus de 80 pays (ACAPS [2026?]). Cette dimension stratégique est indissociable de la compréhension des acteurs et de la géopolitique du maintien de la paix (Tardy 2009, p. 35-53).

3.1.2 Veille opérationnelle

Contrairement à la veille stratégique, la veille opérationnelle se concentre sur le terrain et sur le cycle de vie immédiat des projets. Elle est orientée vers l'efficacité de l'action et la logistique.

Elle englobe le suivi en temps réel des flux d'aide, de la sécurité des personnels et de l'évolution des besoins des populations bénéficiaires (Masudin et al. 2021). Elle s'appuie fortement sur la gestion des données de terrain pour garantir la traçabilité des services logistiques (Masudin et al. 2021). Le HCR souligne que cette gestion des données opérationnelles est cruciale pour la coordination et la réponse immédiate en situation d'urgence (UNHCR 2025). Les outils de collecte comme KoBoToolbox (utilisé par plus de 32 000 organisations ; KoBoToolbox [2026?]) et les plateformes de gestion des bénéficiaires (SCOPE du PAM, PRIMES du HCR) constituent l'infrastructure technologique de cette veille opérationnelle. Le système mVAM du PAM et U-Report de l'UNICEF permettent de suivre l'évolution des besoins via la téléphonie mobile, y compris dans des zones à accès physique restreint.

3.1.3 Dispositifs de veille

Le dispositif de veille est l'architecture technique et humaine mise en place pour transformer des données brutes en renseignements exploitables. Dans le secteur humanitaire, ce dispositif doit impérativement intégrer des protocoles de protection des données afin de respecter le principe de *Do No Harm* (IASC 2023). Comme le souligne Marelli (2020, p. 367-387), la transformation numérique des organisations humanitaires a considérablement élargi leur surface d'exposition, rendant indispensable la définition d'un « cyber-périmètre » humanitaire.

3.1.3.1 Cycle

Le dispositif de veille repose sur un cycle structuré, calqué sur le cycle du « Data Management » humanitaire et formalisé par les « Data Responsibility Guidelines » d'OCHA (OCHA 2021, p. 28).:

1. Expression des besoins : identification des questions critiques (ex : accès aux zones de conflit, évolution des déplacements de population, risques sécuritaires). Les « Data Grids » (OCHA [2026?]b) de HDX permettent d'identifier les lacunes informationnelles structurelles.
2. Collecte : récupération de données via des capteurs humains (enquêtes KoBoToolbox, CATI, IVR), des systèmes biométriques (BIMS, SCOPE) (Açıkyıldız 2024b), des plateformes participatives (Ushahidi, U-Report), des sources OSINT (réseaux sociaux, imagerie satellitaire) et des capteurs IoT (stations météo, capteurs de débit).
3. Traitement et analyse : tri, nettoyage et interprétation des données. Les outils de Statistical Disclosure Control permettent l'anonymisation préalable au partage. PRIMES Analytics du HCR et les outils d'ACAPS fournissent des capacités analytiques structurées.
4. Diffusion : transmission de l'information aux décideurs sous forme de rapports, de tableaux de bord ou de jeux de données ouverts via HDX. ReliefWeb d'OCHA agrège les rapports et analyses de la communauté humanitaire mondiale.

3.1.3.2 Méthodes

Les méthodes de veille ont évolué avec la révolution numérique, intégrant des technologies de pointe qui font l'objet d'une analyse détaillée dans les sections suivantes. On peut identifier trois axes méthodologiques majeurs :

La veille via les réseaux sociaux et le crowdsourcing s'appuie sur ce que Santoni nomme le «territoire 2.0» (Santoni 2022, p. 72-94) et d'information géographique involontaire, montrant comment les réseaux sociaux transforment la gestion des crises en générant des flux d'information non structurés mais exploitables. Ushahidi, plateforme open source de cartographie participative déployée plus de 150 000 fois dans 160 pays, incarne cette approche. Les messageries (WhatsApp, Telegram) sont devenues des canaux de veille terrain incontournables, bien que leurs métadonnées posent des risques significatifs : même lorsque le contenu d'un message est chiffré, les métadonnées (identité des interlocuteurs, horodatage, fréquence des échanges, localisation approximative de l'émetteur) restent accessibles à l'opérateur de la plateforme et potentiellement à des tiers, permettant de reconstituer des réseaux de contacts et d'exposer l'identité de sources terrain.

La collecte biométrique et la gestion des bénéficiaires reposent sur l'utilisation des empreintes digitales et de l'iris pour identifier les bénéficiaires, via BIMS (HCR) et SCOPE (PAM), pose

des défis éthiques et sécuritaires majeurs. Plus de 37 millions de réfugiés avaient été enregistrés de manière biométrique dès 2020 (UNHCR 2025). La plateforme RedRose, utilisée par le CICR dans plus de 50 pays (RedRose [2026?]), complète cet écosystème avec ses fonctionnalités d'audit et de séparation des fonctions.

La mise en place de systèmes de traçabilité basés sur la blockchain vise à sécuriser la chaîne d'approvisionnement humanitaire (Saad et al. 2023). Le projet Building Blocks du PAM, plus grande initiative blockchain humanitaire au monde, a démontré son potentiel en Jordanie pour les transferts monétaires aux réfugiés syriens.

Tableau 3 : Liste comparative des plateformes d'information humanitaire

Outil	Organisation	Prix	Open Source	Offline
SCOPE (PAM)	PAM / WFP	Interne	Non	Oui
BIMS/PRIMES	HCR / UNHCR	Interne	Non	Oui
RedRose	Privé (Dublin)	Commercial	Non	Oui
LMMS	World Vision	Interne	Non	Oui
CATI	Variable	Variable	Certains	Non
U-Report	UNICEF	Gratuit	Oui	Non
mVAM	PAM / WFP	Interne	Non	Non
Device Magic	Privé	~25 $/mois	Non	Oui
RedSafe	CICR	Gratuit	Non	Oui
Ushahidi	ONG (Kenya)	Gratuit/Payant	Oui (AGPL)	Oui (app)
Blockchain (BB)	PAM / WFP	Interne	Non	Non
Drones	Variable	500-50k $	N/A	Oui
DPIA	Méthodologie	Gratuit	N/A	N/A
SDC	Méthodologie	Gratuit	Oui (R)	N/A

© Charlotte Chuard 2026

3.1.3.3 Bonnes pratiques

Les bonnes pratiques actuelles se concentrent sur la responsabilité des données (*Data Responsibility*). Par suite d'incidents majeurs comme la cyberattaque contre le CICR en 2022 (CICR 2022), le vol de 6,8 téraoctets de données de Save the Children par le groupe BianLian en 2023 (Powell 2023), le secteur a formalisé des standards stricts :

Le premier est la *privacy by design*, soit l'intégration de la cybersécurité et la protection des données dès la conception des outils de veille. Le « Handbook on Data Protection in

Humanitarian Action » du CICR (Marelli 2024) et l'ouvrage de Beduschi, Marelli et Martin (2025) fournissent le cadre de référence. Les conditions d'utilisation de KoBoToolbox d'OCHA exigent la conformité aux directives de responsabilité des données dès la conception des formulaires.

Le deuxième est la gouvernance éthique, qui suppose de suivre les directives de l'IASC sur la responsabilité des données et le *Sphere Handbook* (Sphere Association 2018) pour assurer un traitement transparent et sécurisé des informations. Le *Core Humanitarian Standard* (CHS), révisé en 2024, renforce les engagements de redevabilité envers les populations affectées.

Le troisième est la limitation de la collecte, qui exige de ne recueillir que les données strictement nécessaires (principe de minimisation) afin de réduire les risques en cas de fuite. Ce principe est d'autant plus crucial que des logiciels espions comme Pegasus (Amnesty International 2021) ont démontré la capacité de certains États à compromettre les terminaux mobiles des acteurs humanitaires, rendant toute donnée excédentaire un facteur de risque supplémentaire.

3.2 La veille humanitaire : état de l'art

La veille humanitaire s'est transformée au cours de la dernière décennie, passant d'une collecte d'informations artisanale et fragmentée à un écosystème numérique complexe. Rejali et Heiniger (2020, p. 2) soulignent que les technologies numériques jouent un rôle structurant tant sur le plan opérationnel que normatif, tandis que Meier (2011, p. 249-254) identifiait les prémices de cette reconfiguration. Cet état de l'art explore comment l'information est devenue un « bien humanitaire » à part entière, essentiel à la survie des populations et à l'efficacité des interventions (Greenwood 2017).

Elle se distingue de la veille stratégique classique par son objet : la protection de la vie et de la dignité humaine dans des contextes de vulnérabilité extrême. Elle peut être définie comme le processus systématique de collecte et d'analyse de données relatives aux risques de catastrophes, aux besoins des populations touchées et à l'accès humanitaire (UNDRR 2017). Elle ne se limite pas à l'observation des crises, mais inclut la surveillance de l'espace humanitaire, c'est-à-dire l'environnement politique et sécuritaire permettant l'action (Dachy 2004, p. 39-40). Dans un monde numérisé, cette veille intègre désormais la lutte contre les « informations préjudiciables » (mésinformation, discours de haine) qui peuvent mettre en péril les opérations et les populations (CICR 2020, p. 2). L'essor de ce que certains qualifient d'« humanitarisme de la quatrième révolution industrielle » (Searle 2025) accentue ces enjeux en introduisant des technologies puissantes mais porteuses de risques inédits (intelligence artificielle, blockchain, biométrie de masse) qui reconfigurent les flux d'information et les rapports de pouvoir au sein du système humanitaire.

3.2.1 Rôle

La veille remplit trois fonctions critiques qui structurent la réponse humanitaire moderne : l'anticipation, la décision et la coordination.

Grâce à l'analyse des risques, la veille permet de passer d'une logique de réaction à une logique proactive. Les organisations utilisent des indicateurs de vulnérabilité, comme l' « INFORM Severity Index » d'ACAPS (ACAPS [2026?]), pour prévoir l'impact des crises imminentes. La surveillance des mesures administratives, comme les restrictions

d'enregistrement imposées aux ONG, permet d'anticiper les entraves aux futures actions humanitaires. Les systèmes d'alerte précoce basés sur des capteurs IoT (stations météorologiques connectées, capteurs de niveau d'eau) automatisent la détection des signaux faibles environnementaux.

L'information traitée est le fondement de l'action humanitaire fondée sur des preuves. Le HCR utilise PRIMES Analytics pour transformer les données d'enregistrement et de distribution en intelligence décisionnelle. Le PAM s'appuie sur SCOPE et mVAM pour arbitrer entre zones d'intervention et types de programmes. Les analyses d'ACAPS, « CrisisInSight » fournissent une base factuelle indépendante pour les décisions d'allocation de ressources.

Dans un système fragmenté composé de multiples acteurs (États, agences onusiennes, ONG nationales et internationales), la veille partagée est le ciment de la coordination. Les *Data Grids* de HDX permettent d'éviter les doublons et d'harmoniser les efforts de réponse. Le système des clusters, avec ses responsables IM (*Information Management Officers*), structure la coordination informationnelle par secteur. Le projet Building Blocks du PAM illustre comment la blockchain peut faciliter la coordination inter-agences en permettant à plusieurs organisations de vérifier et enregistrer l'aide délivrée dans un registre commun.

3.2.2 Acteurs clés

La veille humanitaire repose sur un réseau d'acteurs aux rôles complémentaires, allant du plaidoyer politique à l'exécution technique.

3.2.2.1 OCHA

Le Bureau de la coordination des affaires humanitaires est le pilier central de la gestion de l'information. À travers le Centre for Humanitarian Data (La Haye), OCHA définit les standards de responsabilité des données, gère le Humanitarian Data Exchange (HDX) et maintient une instance de KoBoToolbox pour la collecte de données coordonnée. Le *Guidance Note on Data Security* (Centre for Humanitarian Data 2022) fournit les orientations de cybersécurité pour les opérations.

3.2.2.2 ACAPS et IFRC

ACAPS fournit quotidiennement des analyses indépendantes de plus de 150 crises dans 80 pays via sa plateforme « CrisisInSight », son « INFORM Severity Index » et son « Global Humanitarian Access Index ». L'IFRC s'appuie sur son réseau de volontaires et sur sa propre instance KoBoToolbox (hébergée à Francfort) pour une veille au plus près des communautés. Son Digital Expo présente les innovations technologiques du Mouvement.

3.2.2.3 ONG

Des acteurs comme Handicap International, Acted ou Oxfam sont des producteurs de données de terrain essentiels. Ils effectuent une veille constante sur l'accès humanitaire et les droits humains. Dauvin et Siméant-Germanos (2002, p. 231) montrent que le travail des acteurs des ONG, du siège au terrain, repose sur des flux informationnels dont la qualité conditionne l'efficacité de l'intervention.

3.2.2.4 Les Clusters

Groupes de coordination sectoriels (santé, logistique, protection, abri), les clusters centralisent la veille thématique. Chaque cluster dispose d'*Information Management Officers* qui

coordonnent, standardisent et partagent les données entre les ONG participantes, offrant une vision consolidée de chaque secteur lors d'une urgence.

3.2.2.5 Acteurs technologiques et de niche

Des entités spécialisées surveillent les risques numériques. The Engine Room fournit des évaluations indépendantes des technologies utilisées en contexte de crise (The Engine Room [2026?]). Le Harvard Humanitarian Initiative développe KoBoToolbox. ACAPS et le Centre for Humanitarian Data publient des analyses prédictives. Ces acteurs sont devenus essentiels face à la multiplication des cyberattaques contre les humanitaires.

3.2.3 Méthodes actuelles

Les méthodes de veille humanitaire reposent aujourd'hui sur un triptyque composé de plateformes de partage de données, d'outils de collecte standardisés et de cadres normatifs guidant la gestion de l'information.

3.2.3.1 Le Humanitarian Data Exchange (HDX) et les Data Grids

Lancé en juillet 2014 par OCHA, le HDX constitue la plateforme de référence pour le partage de données humanitaires en libre accès. À l'occasion de ses dix ans en 2024, HDX comptait plus de 18 000 jeux de données provenant de 254 localisations et 2 147 sources (OCHA [2026?]a), consultés par 1,4 million de personnes en 2021. La plateforme interdit expressément le partage de données personnelles ou d'informations permettant l'identification des individus. Les *Data Grids* offrent une vue structurée de la disponibilité des données par crise. En 2024, OCHA estimait que 70 % des données de crise pertinentes étaient disponibles à travers 23 opérations humanitaires (OCHA [2026?]b).

3.2.3.2 Le Humanitarian Exchange Language (HXL)

Le HXL a été développé comme un standard simple pour les données non structurées du secteur humanitaire, reposant sur l'ajout de hashtags sémantiques dans les tableurs (#inneed, #country, #adm1). Après plus d'une décennie d'utilisation facilitant l'interopérabilité entre des jeux de données produits dans des langues et contextes différents, le standard a été retiré du support actif le 31 janvier 2026, OCHA explorant de nouvelles approches. Le HXL reste disponible en tant que standard ouvert.

3.2.3.3 KoBoToolbox et la collecte standardisée

KoBoToolbox est développé par le Harvard Humanitarian Initiative en partenariat avec OCHA et l'IRC. L'outil prend en charge l'intégralité du cycle de collecte : conception de formulaires (avec plus de 20 types de questions, logique conditionnelle et validation intégrée), collecte sur le terrain (y compris en mode hors ligne avec géolocalisation et métadonnées photographiques), et analyse des données. L'IFRC dispose de sa propre instance (kobo.ifrc.org) hébergée à Francfort, le HCR maintient ses propres serveurs, et les conditions d'utilisation du serveur OCHA exigent la conformité aux *Data Responsibility Guidelines* et aux Principes de protection des données personnelles des Nations Unies (2018).

3.2.3.4 Les IM guidelines et standards professionnels

Les *Data Responsibility Guidelines* d'OCHA, les directives de l'IASC et le *Guidance Note on Data Security* encadrent la gestion de l'information. Le *Sphere Handbook* et le CHS (2024) fournissent le cadre éthique et qualitatif. ACAPS complète l'écosystème par son INFORM Severity Index et son Global Humanitarian Access Index.

3.3 Gestion de l'information humanitaire

3.3.1 Cycle de vie des données

La gestion de l'information dans le secteur humanitaire s'articule autour d'un cycle de vie des données qui structure l'ensemble des opérations informationnelles, de la collecte initiale à l'archivage ou à la destruction. Les « Data Responsibility Guidelines » (OCHA 2021) et les « Operational Guidance on Data Responsibility in Humanitarian Action » du Comité permanent interorganisations (IASC 2023) formalisent ce cycle en identifiant les étapes clés : la planification et la conception de la collecte, la collecte proprement dite, le traitement et l'analyse, le partage et la diffusion, la conservation et, enfin, la destruction. À chaque étape correspond un ensemble de responsabilités spécifiques en matière de qualité, de sécurité et de protection des données.

Le HCR a structuré son approche de la gestion des données et de l'information (UNHCR 2025) autour de l'écosystème PRIMES, qui intègre l'enregistrement biométrique via BIMS (Biometric Identity Management System), la gestion de cas via proGres, les transferts monétaires via CashAssist et l'intelligence décisionnelle via PRIMES Analytics, qui a officiellement remplacé Dataport en avril 2025. Cet écosystème illustre une approche intégrée du cycle de vie des données, où l'information biographique, biométrique et transactionnelle circule entre différents outils interconnectés tout au long de l'intervention humanitaire.

Du côté du Programme alimentaire mondial (PAM), la plateforme SCOPE couvre l'ensemble du cycle opérationnel, de l'enregistrement biométrique des bénéficiaires (empreintes digitales, iris, photos) à la réconciliation des distributions, en passant par l'authentification, la gestion des transferts et le suivi des distributions. Sa capacité à fonctionner en mode déconnecté avec synchronisation ultérieure répond aux contraintes de connectivité des terrains humanitaires, un enjeu récurrent dans la gestion du cycle de vie des données.

Pour la collecte de données sur le terrain, KoBoToolbox s'est imposé comme l'outil de référence. L'IFRC dispose de sa propre instance hébergée sur Amazon Web Services à Francfort, tandis que l'UNICEF a déployé U-Report, un outil de messagerie sociale comptant des millions d'utilisateurs, pour des sondages rapides via SMS et réseaux sociaux. Le PAM utilise mVAM pour l'analyse de la vulnérabilité alimentaire à distance, et Device Magic est l'application mobile institutionnelle du CICR pour la saisie de données terrain via formulaires numériques.

3.3.2 Gouvernance de l'information

La gouvernance de l'information humanitaire repose sur un ensemble de mécanismes institutionnels visant à garantir la qualité, la cohérence et la responsabilité dans le traitement des données. Les directives opérationnelles sur la responsabilité des données (IASC 2023) établissent le cadre de cette gouvernance en définissant les rôles et responsabilités des différents acteurs impliqués dans le traitement de l'information. Le système des clusters, coordonné par OCHA, structure la gouvernance de l'information par secteur d'intervention, chaque cluster disposant de responsables de gestion de l'information chargés de la coordination, de la standardisation et du partage des données au sein de leur domaine.

Les plateformes de gestion des bénéficiaires incarnent des modèles de gouvernance distincts. SCOPE (PAM) fonctionne comme un système propriétaire interne, avec des rôles d'accès strictement contrôlés et des comptes utilisateurs gérés centralement. PRIMES (HCR) adopte

une approche d'écosystème interopérable, permettant l'accès contrôlé à des partenaires gouvernementaux et humanitaires tout en maintenant une gouvernance centralisée des données biométriques. RedRose, plateforme commerciale utilisée par le CICR, l'IFRC, le NRC et d'autres dans plus de 50 pays, intègre des fonctionnalités de séparation des fonctions et des journaux d'audit, instaurant une gouvernance fondée sur la redevabilité et la traçabilité des actions.

3.3.3 Standards et principes professionnels

Plusieurs cadres normatifs structurent les pratiques de gestion de l'information humanitaire. Le « Sphere Handbook » (Sphere Association 2018), dans sa quatrième édition publiée en 2018, constitue l'un des outils les plus largement reconnus et utilisés au niveau international pour la délivrance d'une réponse humanitaire de qualité. Composé de la Charte humanitaire, des Principes de protection, du Core Humanitarian Standard (CHS) et de standards minimaux dans quatre domaines vitaux, il fournit un cadre de référence que les ONG nationales et internationales, les agences des Nations Unies et les autorités gouvernementales utilisent pour planifier, mettre en œuvre et évaluer les opérations humanitaires. La deuxième édition du CHS (2024), renforce les neuf engagements visant à garantir que les organisations soutiennent les personnes affectées par les crises dans le respect de leurs droits et de leur dignité.

Le Humanitarian Data Exchange (HDX), lancé par OCHA en juillet 2014, est devenu la plateforme de référence pour le partage de données humanitaires en libre accès. Comptant plus de 18 000 jeux de données provenant de 254 localisations et 2 147 sources, HDX applique le standard HXL, un langage simple de balisage sémantique qui facilite la validation, le nettoyage et la fusion des données. Les « Data Grids » offrent une vue structurée de la disponibilité des données par crise, permettant d'identifier les lacunes informationnelles. HDX interdit expressément le partage de données personnelles ou d'informations permettant l'identification des individus, toutes les données devant être suffisamment agrégées ou anonymisées. Les conditions d'utilisation du serveur KoBoToolbox d'OCHA exigent de même que toutes les données soient gérées conformément aux Data Responsibility Guidelines et aux Principes de protection des données personnelles des Nations Unies (2018).

La protection générale de l'information (PGI) s'inscrit dans une approche transversale visant à intégrer les considérations de protection dans tous les secteurs de la réponse humanitaire. Les principes directeurs d'OCHA en matière de gestion de l'information (OCHA IM) fournissent des orientations pratiques pour les responsables de l'information sur le terrain, tandis que le Centre for Humanitarian Data, basé à La Haye, publie des travaux sur la responsabilité des données, l'alphabétisation numérique et l'analyse prédictive. L'UNDRR (2017) intègre ces préoccupations dans sa définition de l'information sur les risques de catastrophe, soulignant l'importance d'une gestion structurée de l'information pour l'alerte précoce et la réduction des risques.

3.4 Sécurité de l’information humanitaire

3.4.1 Les risques informationnels

L'environnement informationnel dans lequel opèrent les organisations humanitaires est traversé par des risques multiformes. Marelli (2020) identifie la nécessité de définir un « cyber-périmètre » humanitaire et de développer des stratégies de cybersécurité adaptées à ces

organisations qui doivent concilier ouverture opérationnelle et protection des données. L'entretien avec van Solinge et Marelli (CICR 2020, p. 31-33) met en lumière la double menace de la désinformation et de la manipulation de l'information, qui affectent directement les opérations de terrain et la confiance des populations assistées.

Santoni (2022) analyse le concept de « territoire 2.0 » et d'information géographique involontaire, montrant comment les réseaux sociaux numériques génèrent des flux d'information non structurés pouvant être exploités pour la veille mais aussi manipulés à des fins de désinformation. L'utilisation massive de messageries grand public (WhatsApp, Telegram, Viber, Facebook Messenger) par les organisations humanitaires et les populations affectées amplifie ce risque : si le contenu des messages peut être chiffré de bout en bout (WhatsApp, Signal), les métadonnées (qui communique avec qui, quand, depuis où) demeurent accessibles aux plateformes et, potentiellement, aux États. Le rapport d'Amnesty International (2021) sur le logiciel Pegasus a démontré l'ampleur des capacités de surveillance étatique, rappelant que des canaux de communication considérés comme sécurisés peuvent être compromis au niveau des terminaux eux-mêmes.

3.4.1.1 Les cyberattaques : incidents majeurs

La cyberattaque contre le CICR en janvier 2022 constitue un cas paradigmatique. Qualifiée de « menace persistante avancée » (APT) comparable à des opérations étatiques, elle a ciblé les serveurs du programme de rétablissement des liens familiaux, compromettant les données personnelles de plus de 515 000 personnes (CICR 2022) vulnérables issues d'au moins 60 sociétés nationales de la Croix-Rouge et du Croissant-Rouge dans le monde. L'attaque a exploité une vulnérabilité non corrigée dans un logiciel d'authentification, permettant aux attaquants de compromettre des identifiants administrateur et de se déplacer latéralement dans les systèmes du CICR. L'organisation a été contrainte de mettre hors ligne les systèmes compromis, paralysant temporairement sa capacité à réunir les familles séparées, en moyenne douze réunifications quotidiennes. Robert Mardini, directeur général du CICR, a qualifié cet acte d'« affront à l'humanité », appelant à ce que la protection de la mission humanitaire du Mouvement s'étende explicitement aux actifs et infrastructures numériques.

En septembre 2023, Save the Children International a été victime du groupe de rançongiciel BianLian (Powell 2023), qui a revendiqué le vol de 6,8 téraoctets de données incluant des fichiers RH internationaux, des données personnelles, plus de 800 gigaoctets de documents financiers ainsi que des courriels et des données médicales. Cet incident, le troisième subi par l'organisation en quelques années (après la brèche Blackbaud en 2020), illustre une tendance structurelle : les organisations humanitaires, en raison de la nature sensible et du volume des données qu'elles détiennent, constituent des cibles privilégiées pour les cybercriminels, comme l'a noté la CISA américaine dans son avis conjoint sur BianLian.

3.4.2 Confidentialité, intégrité, disponibilité

La sécurité de l'information repose sur trois exigences fondamentales (la confidentialité, l'intégrité et la disponibilité) qui prennent un sens particulièrement concret en contexte humanitaire, où les conséquences d'une défaillance ne se mesurent pas en pertes financières mais en risques pour des personnes vulnérables.

La confidentialité, soit la garantie que l'information n'est accessible qu'aux personnes autorisées, est l'enjeu le plus immédiatement compréhensible dans ce secteur. Lorsque les

données concernent des personnes recherchées, des victimes de violences ou des membres de groupes ethniques ciblés, une fuite peut entraîner des conséquences directes sur leur sécurité physique : persécutions, détentions arbitraires, représailles. La difficulté est encore plus grande avec les données biométriques, comme les empreintes digitales ou les images de l'iris, collectées par des systèmes comme BIMS (HCR) ou SCOPE (PAM). Contrairement à un mot de passe que l'on peut changer après une compromission, ces données sont permanentes : une fois exposées, elles le restent à vie.

L'intégrité, soit la garantie que l'information n'a pas été modifiée ou falsifiée, est un enjeu moins visible mais tout aussi critique. Dans un contexte humanitaire, une liste de bénéficiaires ou un registre de distribution altérés peuvent avoir des effets directs sur le terrain : l'aide est détournée vers des personnes non éligibles ou, à l'inverse, des personnes vulnérables en sont privées. La manipulation des données n'est donc pas seulement un problème technique, c'est une atteinte à l'équité de l'intervention humanitaire elle-même.

La disponibilité, soit la garantie que l'information reste accessible quand on en a besoin, est soumise à des pressions particulières dans les environnements où opèrent les organisations humanitaires : connexion internet instable ou inexistante, coupures d'électricité fréquentes, risque de confiscation des équipements par des acteurs armés. C'est pour répondre directement à cette réalité que des outils comme SCOPE, KoBoToolbox ou RedRose ont été conçus pour fonctionner sans connexion et se synchroniser une fois la connectivité rétablie, une fonctionnalité qui, dans d'autres secteurs, serait un simple confort, mais qui devient ici une condition d'opérabilité.

3.4.3 Sécurité opérationnelle (OPSEC)

La sécurité opérationnelle (OPSEC) dans le domaine humanitaire vise à protéger les informations sur les processus, les mouvements et les plans des organisations qui, si elles étaient révélées, pourraient compromettre les opérations ou mettre en danger le personnel et les bénéficiaires. Dans les zones de conflit, les données de géolocalisation collectées par les appareils mobiles, les photos avec métadonnées EXIF ou les publications sur les réseaux sociaux peuvent révéler involontairement la position de convois, d'entrepôts ou de refuges. L'application RedSafe du CICR, qui offre un « coffre-fort numérique » chiffré pour les documents personnels sur smartphone, illustre une réponse à ce besoin de protection des données en transit. Cependant, le risque de confiscation de téléphone par des forces armées demeure, rappelant que la sécurité technologique ne se substitue pas à la sécurité physique.

Les capteurs IoT déployés dans les contextes humanitaires (capteurs thermiques dans les camps, capteurs de débit sur les pompes à eau, stations météorologiques connectées) présentent des vulnérabilités OPSEC spécifiques. Souvent faiblement sécurisés, ces dispositifs peuvent être compromis pour surveiller les mouvements dans un camp ou identifier des schémas d'activité. Le « Guidance Note on Data Security in Operational Data Management » du Centre for Humanitarian Data fournit des orientations pratiques sur la sécurisation de ces flux de données opérationnels.

3.5 Protection des données humanitaires

3.5.1 Principes du CICR

L'ouvrage collectif dirigé par Beduschi, Marelli et Martin (2025) constitue la référence actualisée sur la protection des données dans l'action humanitaire, analysant les défis posés

par un monde de plus en plus orienté par les données. Le « Handbook on Data Protection in Humanitarian Action » du CICR (Marelli 2024), fruit d'une collaboration entre le Brussels Privacy Hub et le bureau de protection des données du CICR, fournit des directives opérationnelles concrètes organisées autour de principes fondamentaux : licéité et loyauté du traitement, limitation des finalités, proportionnalité et minimisation, qualité et sécurité des données, droits des personnes concernées. Ce Handbook fait figure de référence sectorielle, utilisé tant pour la formation du personnel que pour l'évaluation des projets technologiques.

Hayes (2017) alerte sur les tensions entre protection des données et politiques migratoires à l'ère de la surveillance de masse et du « big data », appelant à une application rigoureuse du principe de *Do No Harm* dans le traitement des données de personnes déplacées. Marelli (2023) analyse par ailleurs les interactions complexes entre les organisations internationales et les régulations nationales de protection des données, révélant un paysage juridique fragmenté qui constitue un défi majeur pour les opérations transfrontalières. Les organisations humanitaires opèrent souvent dans des juridictions où la législation sur la protection des données est inexistante, insuffisante ou, au contraire, instrumentalisée à des fins de contrôle. Une situation qui rend d'autant plus nécessaire l'existence de cadres internes robustes.

3.5.2 Privacy by design

Le principe de privacy by design est d'intégrer la protection de la vie privée dès la conception des systèmes et des processus et de trouver des applications concrètes dans l'écosystème technologique humanitaire. Les conditions d'utilisation du serveur KoBoToolbox d'OCHA illustrent cette approche en exigeant que toutes les données collectées soient gérées conformément aux directives de responsabilité des données dès la phase de conception des formulaires. L'IFRC, dans sa politique de confidentialité pour sa propre instance KoBoToolbox hébergée à Francfort, distingue clairement entre les données contrôlées par l'IFRC (analytiques de site et données d'inscription) et les données traitées pour le compte des utilisateurs enregistrés, ces derniers conservant la pleine propriété de leurs données applicatives.

Le HDX intègre le privacy by design en interdisant structurellement le partage de données personnelles sur la plateforme et en exigeant une agrégation ou une anonymisation suffisante de tous les jeux de données partagés. La proposition d'identité numérique préservant la vie privée pour la distribution d'aide humanitaire, présentée lors du IEEE Symposium on Security and Privacy de 2023, illustre les recherches de pointe visant à concevoir des systèmes d'authentification qui ne nécessitent pas la centralisation de données biométriques sensibles. Le projet Building Blocks du PAM, plus grande initiative blockchain humanitaire au monde, tente de concilier traçabilité des transactions et protection des données en séparant les données personnelles (stockées hors chaîne) des métadonnées transactionnelles (inscrites sur la blockchain).

3.5.3 Minimisation des données, consentement et sensibilité accrue

Les travaux d'Açıkyıldız (2024b) mettent en évidence la diversité des approches biométriques adoptées par les organisations humanitaires, montrant que des organisations confrontées à des données similaires aboutissent à des usages très différents selon leurs cultures institutionnelles et leurs mandats. Dans une seconde étude (Açıkyıldız, 2024a), le même auteur explore les implications de ces pratiques biométriques sur la relation de pouvoir entre

organisations et bénéficiaires, soulignant la connaissance intime que ces systèmes confèrent aux organisations sur les populations assistées.

Le consentement éclairé constitue un défi structurel en contexte humanitaire. Lorsque l'enregistrement biométrique dans BIMS est un prérequis pour la demande d'asile et la réception de l'aide, la notion de consentement « libre » devient problématique. Plus de 37 millions de réfugiés avaient fourni leurs données biométriques à BIMS dès 2020, un enregistrement souvent présenté comme une condition sine qua non de l'accès aux services. Le *Signal Code* développé par Greenwood (2017) propose une approche fondée sur les droits humains de l'information en situation de crise, articulant le droit à l'information, le droit à la vie privée et le droit à la protection. Les méthodes de SDC (k-anonymité, l-diversité, bruit statistique) permettent de réduire le risque de réidentification lors du partage de données, bien que l'expertise statistique nécessaire ne soit pas toujours disponible dans les équipes de terrain. L'analyse d'impact relative à la protection des données (DPIA/AIPD) est de plus en plus systématisée avant tout déploiement technologique, constituant un outil de gouvernance préventive au service de la minimisation des données.

3.6 Traçabilité et fiabilité des sources

3.6.1 Confiance, validation, chaîne de traitement

La traçabilité des sources constitue un pilier fondamental de tout dispositif de veille humanitaire. Masudin et al. (2021) démontrent l'impact de la traçabilité des systèmes d'information sur la performance logistique humanitaire, établissant un lien direct entre la qualité de la chaîne de traitement de l'information et l'efficacité de la réponse. Saad et al. (2023) analysent les apports de la blockchain pour la traçabilité de la chaîne d'approvisionnement humanitaire, mettant en évidence la transparence accrue, la réduction des coûts de transaction et l'immutabilité des registres comme facteurs de confiance.

La chaîne de traitement de l'information désigne le processus documenté par lequel une donnée est collectée, transmise, traitée, analysée et diffusée, en garantissant à chaque étape son intégrité et son authenticité. Les plateformes comme RedRose matérialisent cette chaîne grâce à leurs journaux d'audit complets qui enregistrent chaque action effectuée dans le système (par qui, quand et sur quelles données). La technologie blockchain, telle qu'implémentée par le projet Building Blocks du PAM en Jordanie, offre une forme particulièrement robuste de traçabilité : chaque transaction d'aide est inscrite dans un registre distribué et immuable, permettant une vérification a posteriori de l'intégrité de l'ensemble de la chaîne. Cette approche a permis au PAM d'éliminer les frais de transaction payés aux intermédiaires financiers.

Cependant, comme le montre la recherche critique, l'immutabilité de la blockchain entre en tension avec le droit à l'effacement consacré par le RGPD, et les métadonnées de transaction, même pseudonymisées, peuvent être corrélées avec des identités connues dans le contexte restreint d'un camp de réfugiés. La confiance dans les systèmes de traçabilité repose donc non seulement sur leurs propriétés techniques, mais aussi sur la gouvernance et les cadres éthiques qui encadrent leur utilisation.

3.6.2 Méthodes de vérification

L'OSINT est devenu un outil central de la veille humanitaire. Il permet la surveillance en temps quasi réel de l'émergence des crises via les réseaux sociaux, les médias en ligne, l'imagerie

satellitaire et les données géospatiales ouvertes. Les organisations humanitaires l'utilisent pour cartographier les dynamiques de conflit, identifier les menaces potentielles, vérifier les conditions d'accès humanitaire, planifier des itinéraires sécurisés et suivre les mouvements de population. The Engine Room, à travers sa bibliothèque d'outils technologiques pour les droits humains, fournit des ressources méthodologiques précieuses pour naviguer dans cet écosystème.

Ushahidi, plateforme open source de crowdsourcing née au Kenya en 2008 et déployée plus de 150 000 fois dans 160 pays (Ushahidi [2026?]), illustre à la fois le potentiel et les limites de la collecte participative d'informations. Sa capacité à agréger des données multi-sources (SMS, e-mail, web, réseaux sociaux) sur une carte interactive en fait un outil directement pertinent pour la veille situationnelle. L'intégration récente de l'intelligence artificielle pour la traduction, la géolocalisation automatique et l'assignation de formulaires renforce ses capacités analytiques. Cependant, la vérification des informations crowdsourcées reste un défi fondamental : chaque rapport doit être authentifié, contextualisé et, si possible, corroboré par des sources indépendantes.

La triangulation constitue la méthode de référence pour la validation de l'information en contexte humanitaire. Elle consiste à croiser systématiquement une information donnée avec au moins deux sources indépendantes provenant de canaux différents. Dans la pratique, cela signifie confronter les témoignages directs (collectés via CATI, IVR ou formulaires KoBoToolbox) avec les données issues de l'imagerie satellitaire ou des drones (UAV), les rapports publiés sur ReliefWeb ou HDX, les signalements crowdsourcés via Ushahidi, et les analyses des réseaux sociaux. Les données de téléphonie mobile, analysées par des organisations comme Flowminder, offrent une source complémentaire pour le suivi des mouvements de population, bien que leur utilisation soulève des questions éthiques relatives au consentement et au profilage.

La validation croisée s'appuie également sur des outils spécifiques de vérification du contenu numérique. L'analyse forensique d'images et de vidéos (recherche d'images inversée, vérification des métadonnées EXIF, analyse de la cohérence d'éclairage et des repères géographiques) permet de détecter les contenus manipulés ou les deepfakes. La matrice d'évaluation de la validité des sources et de la crédibilité de l'information, graduée de A1 (source fiable, information confirmée par des sources indépendantes) à F6 (fiabilité inconnue, validité indéterminable) et inspirée du système de cotation du renseignement militaire (dit « système de l'OTAN » / Admiralty Code) (Irwin, Mandel 2019), constitue un outil de classification standardisé applicable au contexte humanitaire. L'imagerie satellitaire, fournie gratuitement par UNOSAT et le « Disaster Charter » pour les analyses humanitaires, ou commercialement par Maxar et Airbus, offre une source de vérification particulièrement robuste, bien que limitée par la couverture nuageuse et la résolution temporelle.

L'essor de ce que certains auteurs qualifient d'« humanitarisme de la quatrième révolution industrielle » (Searle 2025) soulève toutefois une mise en garde : la sophistication croissante des outils OSINT et des plateformes d'analyse ne doit pas faire oublier que la collecte de données à elle seule ne produit pas d'intelligence opérationnelle. Comme le souligne la recherche sur l'OSINT en contexte de crise, le surinvestissement dans la collecte et le traitement au détriment de l'expertise contextuelle, de la connaissance des dynamiques

conflictuelles et de la sensibilité aux biais cognitifs constitue un risque réel. L'outil détecte le signal ; c'est l'être humain qui détermine sa signification.

4. Terrain professionnel

4.1 Présentation du terrain documentaire

4.1.1 Sélection des organisations

Le terrain documentaire de ce travail s'articule autour d'un corpus d'organisations sélectionnées pour la diversité de leurs mandats, de leurs échelles d'intervention et de leur niveau de maturité informationnelle. Les organisations retenues sont :

- OCHA et son Centre for Humanitarian Data,
- ACAPS
- CICR
- MSF
- FICR
- CartONG[1]

Ces acteurs ont été complétés par des systèmes d'alerte précoce (FEWS Net, INFORM Risk Index) et des outils de géotraçage, dont l'usage est documenté dans la littérature grise humanitaire.

4.1.2 Justification du choix

Ce choix repose sur trois critères complémentaires. Premièrement, la représentativité sectorielle : les organisations retenues couvrent l'ensemble du spectre humanitaire, des agences de coordination onusiennes aux ONG médicales de terrain, en passant par les acteurs du Mouvement international de la Croix-Rouge. Deuxièmement, la disponibilité et la qualité documentaire : ces organisations publient régulièrement des rapports, des guides méthodologiques et des jeux de données ouverts permettant une analyse rigoureuse de leurs pratiques informationnelles. Troisièmement, la pertinence au regard de la problématique : les organisations sélectionnées sont précisément celles dont les dispositifs de veille, de protection des données et de traçabilité sont les mieux documentés dans la littérature professionnelle et académique.

4.1.3 Limites et accès aux données

L'accès aux données documentaires présente plusieurs limites qu'il convient de signaler. En premier lieu, les publications institutionnelles reflètent la posture officielle des organisations et ne rendent pas nécessairement compte des pratiques effectives de terrain, qui peuvent en différer sensiblement. En second lieu, certaines informations relatives aux incidents de sécurité font l'objet d'une communication partielle ou différée, pour des raisons compréhensibles de réputation et de sécurité opérationnelle. Enfin, les données relatives aux dispositifs internes (procédures, protocoles, bases de données) sont rarement accessibles dans leur intégralité au regard de leur sensibilité. Le présent travail s'appuie donc essentiellement sur les sources publiées, complétées par les résultats de l'enquête (cf. chapitre 4.4).

[1] Organisation spécialisée dans l'information géographique humanitaire

4.1.4 Études de dispositifs existants

L'analyse documentaire porte sur six grandes catégories de dispositifs, dont les principales caractéristiques sont présentées ci-après. Pour chacun, l'accent est mis sur les pratiques de veille, les mécanismes de traçabilité et les enjeux de sécurité documentés.

4.1.5 HDX & HXL

Le Humanitarian Data Exchange (HDX), lancé en 2014, constitue la plateforme de référence pour le partage ouvert de données humanitaires. En 2024, elle recense plus de 18 000 jeux de données issus de 2 147 sources et couvrant 254 localisations géographiques. Le HDX repose sur le Humanitarian Exchange Language (HXL), un standard de balisage sémantique permettant d'homogénéiser des données provenant de sources hétérogènes. Son architecture intègre des règles strictes : interdiction de partager des données personnelles identifiables, obligation de conformité aux Data Responsibility Guidelines d'OCHA.

Sur le plan de la traçabilité, chaque jeu de données est associé à des métadonnées standardisées documentant l'organisation productrice, la date de mise à jour, la couverture géographique et la méthode de collecte. Les Data Grids offrent une vue structurée des lacunes informationnelles par crise. En matière de sécurité, la plateforme est hébergée par Amazon Web Services avec certification ISO 27001, et dispose d'une procédure de signalement des données sensibles publiées par erreur. La principale limite documentée réside dans la dépendance à un opérateur commercial américain, ce qui pose des questions de souveraineté des données pour les organisations opérant sous juridictions non conformes au droit américain.

4.1.6 ACAPS CrisisInSight

ACAPS produit quotidiennement des analyses indépendantes couvrant plus de 150 crises dans 80 pays via sa plateforme CrisisInSight. L'INFORM Severity Index et le Global Humanitarian Access Index, constituent les outils d'alerte précoce les plus systématisés du secteur. La méthodologie d'ACAPS se distingue par sa transparence : chaque analyse est accompagnée d'une documentation explicite des sources mobilisées, de la date de collecte et du niveau de confiance attribué à chaque donnée.

Le dispositif d'ACAPS illustre une pratique de traçabilité avancée rarement observée ailleurs dans le secteur : la publication des matrices d'évaluation et des processus de validation permet une vérification externe de la qualité analytique. En termes de sécurité, ACAPS opère avec une politique de non-collecte de données personnelles et limite ses sources aux informations publiquement disponibles, réduisant ainsi le risque d'exposition des populations.

4.1.7 IFRC Data Playbook

Le Data Playbook de la FICR constitue un dispositif de renforcement des capacités informationnelles des Sociétés nationales de la Croix-Rouge et du Croissant-Rouge à l'échelle mondiale. Il compile les bonnes pratiques en matière de collecte, de gestion et de protection des données, avec une attention particulière aux contraintes spécifiques des contextes à faibles ressources. Le Playbook intègre des modules sur le consentement éclairé, la minimisation des données et la gestion des données sensibles dans des environnements dégradés.

Ce dispositif illustre une approche pédagogique de la gouvernance informationnelle : plutôt que d'imposer un cadre normatif rigide, il propose des fiches pratiques adaptables aux réalités locales. Sa principale limite réside dans le fait qu'il constitue un cadre prescriptif sans mécanisme de vérification de son application effective par les Sociétés nationales.

4.1.8 Méthodes de monitoring

Pour exemple, une des organisations humanitaires internationales dispose d'une unité dédiée à la gestion de l'information, comprenant des fonctions d'archives, de documentation et de veille sur sources ouvertes, qui assure la veille contextuelle, sécuritaire et médiatique dans les zones d'intervention. Son dispositif de monitoring repose sur une combinaison de sources ouvertes (presse internationale et régionale, réseaux sociaux) et de remontées terrain, traitées par des analystes spécialisés par région. La réponse de cette organisation à l'enquête conduite dans le cadre de ce travail confirme une maturité intermédiaire : le monitoring est conduit de manière informelle sans service centralisé formalisé, malgré la taille importante de l'organisation.

Les pratiques documentées révèlent une tension caractéristique : l'urgence opérationnelle prime régulièrement sur les protocoles de traçabilité, conduisant à des pratiques de validation informelles. La classification des données intègre cependant une politique de gestion documentaire et un régime RGPD interne. L'absence de chiffrement systématique des données collectées et le recours à des prestataires tiers (Google/Microsoft) pour le stockage constituent les principales fragilités identifiées.

4.1.9 Systèmes d'alerte précoce

Le Famine Early Warning Systems Network (FEWS Net), financé par l'USAID, et l'INFORM Risk Index, développé conjointement par la Commission européenne et l'IASC, constituent deux dispositifs complémentaires d'anticipation des crises humanitaires. FEWS Net combine données satellitaires, relevés météorologiques, analyses de marchés et remontées terrain pour produire des projections de sécurité alimentaire sur trois à six mois. L'INFORM Risk Index agrège des indicateurs de risque, de vulnérabilité et de capacité de réponse pour 191 pays.

Ces systèmes illustrent la puissance de l'approche multi-source dans la veille humanitaire, mais également ses limites en matière de traçabilité : la multiplicité des contributeurs et des méthodes d'agrégation rend difficile la documentation précise de la chaîne de traitement pour chaque donnée. La question de la responsabilité analytique reste partiellement non résolue dans les modèles de gouvernance de ces dispositifs.

4.1.10 Outils de géotraçage

Les outils de géotraçage comme la cartographie participative (Ushahidi), l'imagerie satellitaire (UNOSAT, Planet Labs) ou les systèmes de localisation des bénéficiaires (SCOPE du PAM), constituent une catégorie particulièrement sensible du point de vue de la protection des données. Ces outils produisent des données de localisation dont le potentiel de réidentification est élevé, notamment lorsqu'elles sont croisées avec d'autres jeux de données.

La littérature professionnelle documente plusieurs incidents de détournement de données géolocalisées dans des contextes de conflit. En réponse, des standards de protection spécifiques ont été développés : agrégation géographique systématique avant partage (précision réduite au niveau du district plutôt que du village), suppression des coordonnées

exactes dans les exports HDX, et protocoles de consentement renforcés pour la collecte de données de localisation.

4.1.11 Analyse des outils

La figure ci-dessous détaille les différents outils analysés par fonctionnalités.

Figure 1 : Analyse d'outils

Fonctionnalité	SCOPE	BIMS/PRIMES	RedRose	LMMS	CATI	IVR	Device Magic	U-Report	mVAM	RedSafe	Messageries	Chatbots	Drones	Sat. imagery	Ushahidi	Big Data/IA	Blockchain	RFID	IoT capteurs	DPIA	SDC
COLLECTE																					
Enregistrement bénéficiaires	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	~	✗	✗	✗	✗	—	—
Enquêtes/formulaires	~	✗	✓	~	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	—	—
Collecte biométrique	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	~	✗	✗	✗	—	—
Crowdsourcing	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	~	✓	✗	✗	✓	~	✗	✗	✗	—	—
Géolocalisation	✓	✓	✓	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	—	—
SÉCURITÉ																					
Chiffrement données	✓	✓	✓	?	?	?	~	✗	?	✓	✓	?	?	?	?	?	✓	✗	?	—	—
Contrôle d'accès (rôles)	✓	✓	✓	?	?	?	✓	~	✓	✗	✗	?	—	—	✓	?	✓	✗	?	—	—
Authentification MFA	?	?	?	✗	✗	✗	✗	✗	✗	✗	✗	✗	—	—	✗	?	?	✗	✗	—	—
Audit logs	✓	✓	✓	?	✓	~	~	~	~	✗	✗	✓	✓	✓	✓	?	✓	✓	✓	✓	~
Plan réponse incidents	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	—	—
PROTECTION DONNÉES																					
Anonymisation intégrée	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	~	~	✗	✗	—	✓
Consentement géré	~	~	~	?	✓	~	?	~	?	—	✗	~	—	—	~	✗	—	—	—	✓	—
Droit effacement	?	?	?	?	?	?	?	?	?	✓	✗	?	—	—	✓	?	✗	—	?	✓	—
Minimisation données	✗	✗	✗	?	?	?	?	?	?	✓	✗	?	?	?	?	✗	?	—	?	✓	✓
TRAÇABILITÉ																					
Horodatage automatique	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	?	✓	✓	✓	—	—
Chaîne de custody	~	~	✓	✗	~	✗	✗	✗	✗	✗	✗	✗	✓	✓	~	✗	✓	✓	~	—	—
Registre immuable	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	—	—
Validation croisée	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	~	~	✓	✗	✗	✗	—	—
OPÉRATIONNEL																					
Mode offline	✓	✓	✓	✓	✗	✗	✓	✗	✗	✓	~	✗	✓	✓	✓	✗	✗	✓	~	—	✓
Multi-modalités paiement	✓	~	✓	✗	—	—	—	—	—	—	—	—	—	—	—	—	✓	—	—	—	—
Interopérabilité	✗	✓	✓	✗	?	?	✓	✓	✗	✗	✓	?	?	✓	✓	?	✓	✗	?	—	✓
Adapté urgence	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	~	✗	✓	✓	~	~

© Charlotte Chuard 2026

L'analyse comparative des dispositifs documentés et des réponses à l'enquête permet d'établir un panorama des outils mobilisés dans la veille humanitaire. Le tableau ci-dessous synthétise les principales catégories d'outils identifiées, en distinguant les organisations qui déclarent les utiliser dans l'enquête (cf. chapitre 4.4), les points forts relevés et les points de vigilance documentés.

Tableau 4 : Analyse comparative des outils de veille humanitaire

Outil / catégorie	Type	Coût	Org. déclarantes	Points forts	Points de vigilance
Stockage centralisé (cloud interne)	Gestion documentaire	Abonnement suite bureautique	Org. C, D, E, F, G	Accès par rôle, intégration écosystème	Souveraineté données, serveurs tiers
Agrégateurs de flux	Collecte & veille	Freemium à professionnel	Org. B, E, G	Veille multi-sources automatisée	Dépendance éditeur, biais de sélection
Social listening professionnel	Monitoring RS	Élevé	Org. E, F	Couverture médias structurée, analytics	Coût prohibitif petites structures

Outil / catégorie	Type	Coût	Org. déclarantes	Points forts	Points de vigilance
Business Intelligence (BI)	Visualisation & analyse	Abonnement suite bureautique ou standalone	Org. F, G	Tableaux de bord dynamiques	Compétences techniques requises
Analyse de réseaux	Cartographie d'acteurs	Gratuit (open source)	Org. E	Cartographie relationnelle	Courbe d'apprentissage importante
Veille basique automatisée (alertes mots-clés)	Alertes automatiques	Gratuit	Org. A	Accessibilité immédiate, zéro coût	Aucune traçabilité, biais algorithmique
Tableurs (Excel, Sheets)	Collecte & suivi manuel	Suite bureautique	Org. A, G, H	Universalité, accessibilité	Pas de traçabilité, risque d'erreurs humaines
Base de données relationnelle	Stockage structuré	Variable (compétences techniques)	Org. B	Requêtes avancées, intégrité des données	Ressources techniques nécessaires

© Charlotte Chuard 2026

Plusieurs enseignements transversaux ressortent de cette analyse. Premièrement, la domination des outils cloud commerciaux (Microsoft SharePoint, OneDrive, Google Drive) dans les pratiques de stockage documentaire est quasi universelle, y compris dans des organisations dont la taille et le mandat justifieraient des solutions plus souveraines. Cette situation crée une tension structurelle entre les exigences de confidentialité propres au secteur humanitaire et la réalité des pratiques. Deuxièmement, le fossé entre les organisations spécialisées dans le monitoring, dont les outils sont sophistiqués et nombreux, et les petites ONG opérationnelles, dont l'outillage se limite parfois à un tableur et une alerte Google, est considérable, et illustre l'importance d'une approche différenciée selon le niveau de maturité. Troisièmement, l'émergence de l'intelligence artificielle et du traitement automatique du langage dans trois organisations de l'échantillon annonce une transformation en cours des pratiques analytiques, qui devra être encadrée par des politiques spécifiques pour en maîtriser les risques de biais, de traçabilité et de confidentialité.

4.2 Études de cas humanitaires documentées

Deux études de cas illustrent concrètement les enjeux de la veille sécurisée dans des contextes opérationnels distincts. Elles sont issues de sources documentaires publiques et permettent de confronter les cadres théoriques aux réalités du terrain.

4.2.1 Cas 1 : la cyberattaque contre le CICR (janvier 2022)

4.2.1.1 Pratiques de veille observables

Le CICR gère, via son système ICRC Restores Families, les données de plus de 500 000 personnes vulnérables (détenus, migrants, personnes disparues). Ce dispositif s'appuie sur un réseau de bases de données centralisées, alimentées par des remontées terrain, issues de plus de 60 délégations. La collecte de données est structurée par des protocoles internes stricts, conformes au Handbook on Data Protection in Humanitarian Action.

4.2.1.2 Difficultés identifiées

En janvier 2022, le CICR a subi une cyberattaque sophistiquée ciblant un prestataire tiers hébergeant ses données. L'attaque a été conduite via une vulnérabilité non corrigée d'un logiciel commercial (CVE non divulguée). Les données de 515 000 personnes (CICR 2022) ont été compromises pendant plusieurs semaines avant détection. L'organisation a été contrainte de mettre hors ligne ses systèmes de localisation des personnes disparues, affectant directement ses opérations de réunification familiale.

4.2.1.3 Enjeux de sécurité et de traçabilité

Cet incident illustre trois vulnérabilités systémiques : la dépendance à des prestataires tiers dont le niveau de sécurité n'est pas directement contrôlable ; l'absence de détection précoce de l'intrusion, liée à des lacunes dans l'audit logging ; et la concentration de données hautement sensibles dans un système centralisé sans segmentation suffisante. Les données compromises incluaient des informations biométriques et des éléments permettant d'identifier des personnes en situation de protection, dont l'exposition peut entraîner des conséquences physiques graves dans des contextes de conflit.

4.2.1.4 Leçons tirées

En réponse, le CICR a publié en 2024 une version actualisée de son Handbook, intégrant des recommandations spécifiques sur la gestion des fournisseurs, l'audit régulier des accès tiers et la mise en place d'une architecture de données en couches limitant la propagation d'une compromission. Ce cas constitue un point de référence incontournable pour tout modèle de veille sécurisée dans le secteur humanitaire.

4.2.2 Cas 2 : séisme en Turquie et Syrie (février 2023)

4.2.2.1 Pratiques de veille observables

Le séisme de magnitude 7,8 du 6 février 2023, l'un des plus meurtriers de l'histoire récente avec plus de 56 000 victimes, a mobilisé un système d'information humanitaire d'une ampleur exceptionnelle. OCHA a activé son dispositif de veille en temps réel via ReliefWeb et HDX, permettant la publication de plus de 200 rapports de situation en 72 heures. Les clusters sectoriels ont déployé des outils de collecte KoBoToolbox pour cartographier les besoins dans les zones affectées. Des organisations comme CartONG ont mobilisé des équipes de cartographes bénévoles (OpenStreetMap) pour produire des cartes d'accès en temps réel.

4.2.2.2 Difficultés identifiées

La phase aiguë de la crise a révélé plusieurs points de friction documentés. En Syrie, l'accès humanitaire dans les zones contrôlées par des acteurs non étatiques a rendu la collecte de données dangereuse pour les informateurs de terrain, soulevant des questions éthiques quant à la protection des sources. La multiplication des acteurs, plus de 200 ONG déployées en deux

semaines, a généré une saturation informationnelle, avec des doublons de données et des estimations contradictoires de besoins. Les réseaux sociaux ont diffusé des informations non vérifiées sur des personnes disparues, créant un bruit informationnel considérable pour les équipes de veille.

4.2.2.3 Enjeux de sécurité et de traçabilité

La pression de l'urgence a conduit de nombreuses organisations à collecter et diffuser des données sans processus de validation formalisé, illustrant de manière aiguë la tension identifiée dans l'enquête entre rapidité opérationnelle et rigueur de traçabilité. Des données géolocalisées précises, publiées sans agrégation suffisante, ont posé des risques d'exposition pour des populations déjà vulnérables dans le contexte sécuritaire syrien.

4.2.2.4 Leçons tirées

Ce cas illustre la nécessité d'un dispositif de veille capable de fonctionner en mode dégradé, avec des ressources et une connectivité limitées, tout en maintenant des standards minimaux de validation et de protection des sources. Il souligne également l'importance d'une architecture informationnelle préétablie : les organisations dotées de protocoles clairs avant la crise ont pu les appliquer en situation d'urgence, tandis que celles dépourvues de tels cadres ont improvisé, au détriment de la qualité et de la sécurité des données.

4.3 Enquête auprès des organismes

4.3.1 Méthode

La méthodologie de collecte et d'analyse a été détaillée au chapitre 1.5 ; seuls les éléments propres à cette phase sont rappelés ici.

Neuf réponses exploitables ont été collectées, provenant de huit organisations distinctes. Une organisation a été représentée par deux répondants aux profils complémentaires permettant de croiser des perspectives internes différenciées au sein d'une même structure. Par souci de confidentialité et conformément aux engagements pris lors de la diffusion du questionnaire, les organisations sont désignées par des codes neutres (Org. A à Org. H) dans l'ensemble de l'analyse.

4.3.2 Profil des répondants

L'échantillon couvre un spectre organisationnel varié, représentatif de la diversité du secteur humanitaire et de développement. Le tableau ci-dessous synthétise les profils des répondants.

Tableau 5 : Profil des répondants

Code	Type	Taille	Secteur d'activité	Rôle du répondant
Org. A	ONG int.	< 50 emp.	Coopération au développement	Administration, communication & voyages de solidarité
Org. B	H2H	< 50 emp.	Monitoring de la violence	Direction
Org. C	OIG	> 1000 emp.	Droits de l'homme	Gestion de l'information / bibliothèque

Code	Type	Taille	Secteur d'activité	Rôle du répondant
Org. D	ONG int.	> 1000 emp.	Humanitaire	Responsable archives & documentation
Org. E (r.1)	Mvt. int.	> 1000 emp.	Humanitaire	Analyste information
Org. E (r.2)	Mvt. int.	> 1000 emp.	Humanitaire	Analyste
Org. F	ONG int.	> 1000 emp.	Services sociaux & action confessionnelle	Directeur numérique (CDO)
Org. G	ONG int.	50-250 emp.	Travail décent, démocratie & action humanitaire	Responsable MEAL & Qualité
Org. H	ONG int.	50-250 emp.	Santé / chirurgie (enfants & mères)	Responsable Audit & Contrôle interne, DPO

© Charlotte Chuard 2026

En termes de taille, 56 % des répondants appartiennent à des structures de plus de 1 000 employés, 22 % à des organisations de 50 à 250 employés et 22 % à des structures de moins de 50 personnes. La portée géographique est majoritairement internationale (78 % des répondants), reflétant la vocation globale du secteur humanitaire. Les rôles des répondants sont diversifiés (directeur, analyste information, responsable archives, DPO, Chief Digital Officer, responsable MEAL) ce qui garantit une diversité de points de vue au sein des organisations représentées.

4.3.3 Principales idées émergentes

Quatre tensions structurelles se dégagent de manière transversale de l'ensemble des réponses.

4.3.3.1 L'urgence opérationnelle prime systématiquement sur la procédure

67 % des répondants identifient ce facteur comme le principal obstacle à un monitoring plus sécurisé et mieux tracé. Dans des contextes de crise, les équipes terrain arbitrent de manière quasi systématique en faveur de la rapidité au détriment des protocoles de traçabilité et de validation, générant des angles morts durables dans la chaîne informationnelle. Ce constat confirme que la pression opérationnelle n'est pas un facteur exceptionnel mais une condition structurelle du secteur.

4.3.3.2 La désinformation est un risque majeur mais sous-protocolarisé

56 % des organisations considèrent la désinformation comme un risque central de leur activité de veille, mais seules deux disposent de protocoles spécifiques de vérification des informations sensibles. Une organisation se distingue en intégrant le monitoring de la désinformation comme objectif premier de son activité (Org. B), et non comme une difficulté

subie. Cette asymétrie entre la perception du risque et l'existence de réponses formalisées constitue une lacune systémique documentée.

4.3.3.3 Les outils tiers dominent au détriment de la souveraineté des données

La grande majorité des organisations stocke ses données sur des solutions cloud commerciales de type Google ou Microsoft, sans chiffrement additionnel. 56 % des répondants déclarent utiliser exclusivement des outils tiers commerciaux pour le stockage, et seuls 11 % chiffrent les données collectées. Ce constat prolonge l'analyse comparative des outils (cf. chapitre 4.1.11) et s'avère particulièrement préoccupant pour les organisations opérant dans des contextes de conflit, où les données de localisation ou d'affiliation peuvent mettre des vies en danger.

4.3.3.4 Le budget conditionne fortement les choix technologiques

L'ensemble des répondants confirment que les contraintes budgétaires influencent directement leurs décisions en matière d'outils de veille. Ce facteur explique la persistance de solutions rudimentaires (tableurs Excel, alertes par mots-clés) dans des organisations pourtant exposées à des risques informationnels élevés. Il justifie également l'intérêt pour des modèles open source et des approches modulaires ne nécessitant pas d'investissements technologiques importants pour être mis en œuvre.

4.4 Résultat d'analyse

4.4.1 Gouvernance et formalisation

L'analyse des réponses révèle un secteur dans lequel la formalisation des pratiques de monitoring est avancée sur le papier mais inégalement mise en œuvre dans les faits. 67 % des répondants déclarent disposer d'un service d'information formalisé au niveau de l'organisation entière, et 56 % d'une unité dédiée spécifiquement au monitoring. Ces chiffres, a priori encourageants, doivent être lus à la lumière d'une donnée complémentaire : un tiers seulement des organisations dispose d'un processus formalisé de validation de l'information avant diffusion interne. La formalisation du cadre organisationnel ne garantit donc pas la formalisation des processus opérationnels.

L'intégration du monitoring aux processus décisionnels est déclarée partielle ou totale pour 56 % des répondants. Cette proportion suggère que la veille reste dans certaines organisations une activité périphérique, mobilisée de manière ponctuelle (« ad hoc » dans les termes de deux répondants) plutôt qu'intégrée de façon systémique. La réflexion éthique sur les risques que le monitoring peut faire courir aux sources de terrain (principe *Do No Harm*) est présente pour 56 % des répondants, ce qui constitue un résultat positif mais souligne l'absence d'une telle réflexion chez un tiers des organisations enquêtées, y compris certaines opérant dans des contextes de conflit armé.

Tableau 6 : Finalités du monitoring déclarées par les répondants

Finalité du monitoring	Nombre de répondants	Pourcentage (n=9)
Analyse contextuelle et sécuritaire	8	89 %
Support aux décisions opérationnelles	8	89 %

Finalité du monitoring	Nombre de répondants	Pourcentage (n=9)
Support aux décisions stratégiques	7	78 %
Risk management et conformité	7	78 %
Anticipation des crises / early warning	7	78 %
Plaidoyer et communication publique	6	67 %
Sécurité du personnel	6	67 %
Fundraising / relations bailleurs	5	56 %

© Charlotte Chuard 2026

La finalité dominante est l'analyse contextuelle et sécuritaire (89 %), suivie du support aux décisions opérationnelles (89 %) et stratégiques (78 %), ce qui confirme la place centrale de la veille dans les processus de décision. La gestion des risques et la conformité arrivent en quatrième position (78 %), témoignant d'une intégration croissante des enjeux de compliance dans les pratiques de monitoring. Le fundraising apparaît comme la finalité la moins fréquemment déclarée (56 %), bien que ce résultat doive être interprété avec prudence, certains répondants ayant pu exclure cette dimension du périmètre de leur réponse.

4.4.2 Degré de maturité des organisations

L'analyse des auto-évaluations sur cinq dimensions (méthodologie et processus, sécurité de l'information, protection des données, traçabilité et qualité des sources, intégration de l'éthique) permet d'esquisser une typologie à trois niveaux de maturité.

Niveau 1 - Maturité avancée (Org. B) : Une organisation se distingue nettement par une approche systématisée, avec une grille OSINT formalisée, un processus de contrôle qualité multi-étapes impliquant plusieurs personnes et prenant plusieurs jours, et une auto-évaluation « très élevée » en méthodologie et en traçabilité. Cette organisation constitue une exception dans l'échantillon : son monitoring est une finalité en soi, non un outil accessoire. Sa spécialisation sectorielle dans le monitoring de la violence lui confère une expertise qui transcende sa petite taille (moins de 50 employés), confirmant que la maturité informationnelle est davantage corrélée à la spécialisation qu'à la taille organisationnelle.

Niveau 2 - Maturité intermédiaire-haute (Org. D, Org. E, Org. F) : Ces organisations présentent des pratiques robustes (cartographies de sources par région, outils professionnels de social listening, politique de sécurité formalisée, accès restreint par rôle) mais des lacunes persistantes en traçabilité documentaire systématique. Une grande organisation humanitaire (Org. D) illustre la limite de la corrélation taille-maturité : malgré plus de 1 000 employés, son monitoring reste conduit « ad hoc », sans service centralisé. Cette configuration s'explique par la culture organisationnelle avec la valorisation de l'expertise terrain au détriment de la formalisation, et par la priorité accordée à l'action opérationnelle.

Niveau 3 - Maturité faible à émergente (Org. A, Org. G, Org. H) : Ces organisations opèrent avec des ressources limitées et des pratiques peu formalisées. Une organisation (Org. H) s'auto-évalue uniformément « faible » sur toutes les dimensions et déclare n'utiliser que des tableurs Excel comme outil de monitoring. Ces organisations illustrent les défis des structures de taille moyenne confrontées à des exigences de conformité croissantes (RGPD, normes sectorielles) sans capacités internes suffisantes pour les satisfaire. Leur situation plaide pour des approches modulaires et accessibles, adaptées à des contextes de faibles ressources.

Tableau 7 : Niveaux de maturité auto-évalués par organisation

Code	Méthodologie & processus	Sécurité information	Protection des données	Traçabilité & sources	Éthique & valeurs
Org. B	Très élevé	Élevé	Élevé	Très élevé	Élevé
Org. E (r.1)	Élevé	Moyen	Moyen	Moyen	Élevé
Org. E (r.2)	Moyen	Élevé	N/A	N/A	Élevé
Org. D	Moyen	Moyen	Élevé	Moyen	Élevé
Org. F	Moyen	Élevé	Élevé	Moyen	Moyen
Org. A	Moyen	Élevé	Moyen	Moyen	Très élevé
Org. H	Faible	Faible	Faible	Faible	Faible
Org. C / Org. G	N/A	N/A	N/A	N/A	N/A

© Charlotte Chuard 2026

4.4.3 Points de friction entre rapidité opérationnelle et sécurité informationnelle

La tension entre la rapidité opérationnelle et les impératifs de sécurité informationnelle constitue le fil rouge de l'enquête. Elle se manifeste à trois niveaux distincts.

Au niveau de la validation de l'information, seul un tiers des répondants dispose d'un processus formalisé de validation avant diffusion interne. Les deux tiers restants s'appuient sur des habitudes professionnelles ou la confiance dans des sources institutionnelles réputées, sans mécanisme documenté. Cette situation expose les décisions opérationnelles à des biais non tracés et difficiles à identifier a posteriori.

Au niveau de la traçabilité documentaire, un peu plus de la moitié des répondants documentent systématiquement l'origine exacte de l'information, et seulement près d'un tiers documentent le niveau de confiance attribué. L'absence de traçabilité systématique ne résulte pas d'un manque de conscience du problème (78 % des répondants l'identifient comme un défi

prioritaire) mais d'une incapacité structurelle à y répondre dans les conditions opérationnelles actuelles.

Au niveau de la sécurité des données, le faible taux de chiffrement (11 %) et la dépendance aux solutions cloud commerciales (56 %) créent des vulnérabilités documentées. Or, la totalité des répondants déclarent que les contraintes budgétaires influencent directement leurs choix technologiques, ce qui suggère que ces fragilités sont moins le résultat d'un manque de conscience des risques que d'une impossibilité économique d'y répondre avec des solutions plus robustes.

4.4.4 Cartographie des outils et méthodes mobilisés

L'analyse des réponses permet d'identifier quatre catégories fonctionnelles d'outils dans les dispositifs de veille humanitaire de l'échantillon.

La première catégorie, celle de la collecte et de l'agrégation, regroupe des outils allant de la veille basique par alertes automatisées sur mots-clés jusqu'aux plateformes de social listening professionnel (Factiva, Sprinklr, Hootsuite), en passant par les agrégateurs de flux (Feedly, KB Crawl). Les réseaux sociaux sont également mobilisés directement comme sources d'information : Facebook et LinkedIn sont utilisés par 67 % des répondants, Instagram et YouTube par 56 %, X (anciennement Twitter) par 44 %. La diversité de ces plateformes reflète la nécessité de couvrir des écosystèmes informationnels variés selon les zones d'intervention.

La deuxième catégorie, celle du stockage et de la gestion documentaire, est largement dominée par les solutions Microsoft : SharePoint et OneDrive sont présents chez 78 % des répondants. Les bases de données relationnelles font figure d'exception, mentionnées par une seule organisation spécialisée (Org. B), tandis que deux organisations de taille intermédiaire ont recours à des systèmes de gestion sectoriels comme NGO Online ou M-Files.

La troisième catégorie, celle de l'analyse et de la visualisation, est encore l'apanage des grandes structures. Les outils de Business Intelligence (PowerBI) et d'analyse de réseaux (Gephi) apparaissent chez deux grandes organisations. Plus significativement, l'intelligence artificielle et le traitement automatique du langage naturel (NLP) ont été introduits récemment par trois organisations (Org. B, Org. E, Org. F), principalement pour la classification automatique de contenus et l'analyse de sentiment. Cette évolution, encore émergente, devra être encadrée par des politiques spécifiques pour en maîtriser les risques de biais et de confidentialité.

La quatrième catégorie, celle de la vérification et de la traçabilité, est la plus lacunaire. Aucun outil dédié n'est uniformément adopté dans l'échantillon : certaines organisations assurent la traçabilité via des métadonnées automatiques et des champs obligatoires (Org. B, Org. F), d'autres la gèrent entièrement à la main (Org. D, selon les termes mêmes du répondant), et d'autres encore ne la gèrent pas du tout (Org. H, Org. A). Cette absence d'outillage spécifique constitue la lacune la plus significative identifiée par l'enquête.

4.4.5 Synthèse des résultats

Le tableau ci-dessous présente une synthèse structurée des principaux résultats par dimension d'analyse.

Tableau 8 : Synthèse des résultats de l'enquête par dimension

Dimension	Résultat clé	Principale tension identifiée
Gouvernance & formalisation	67 % disposent d'un service d'information formalisé ; 56 % d'une unité dédiée au monitoring	Grande taille ≠ maturité : certaines grandes organisations opèrent sans service structuré
Intégration aux décisions	56 % intègrent le monitoring aux décisions (partiellement ou totalement)	33 % seulement disposent d'un processus formalisé de validation avant diffusion interne
Outils & automatisation	Stockage centralisé (89 %) dominant ; suite Microsoft (78 %) ; IA introduite dans 33 % des organisations	Dépendance généralisée aux outils cloud tiers sans chiffrement complémentaire (67 %)
Traçabilité	56 % documentent l'origine exacte de l'information	Urgence opérationnelle (67 %) = principal obstacle aux protocoles de traçabilité
Sécurité	67 % ont une politique de sécurité formelle ; 11 % seulement chiffrent les données collectées	Budget conditionne les choix technologiques pour tous les répondants
Maturité auto-évaluée	Éthique : dimension la mieux évaluée ; Traçabilité & méthodes : dimensions les plus lacunaires	Corrélation maturité-spécialisation > maturité-taille organisationnelle

© Charlotte Chuard 2026

Ces résultats confirment et précisent les hypothèses issues de l'analyse documentaire. Ils soulignent quatre constats majeurs.

Premièrement, la maturité informationnelle des organisations humanitaires est davantage corrélée à la spécialisation fonctionnelle qu'à la taille organisationnelle. Une petite organisation entièrement dédiée au monitoring (Org. B) surpasse systématiquement des grandes organisations généralistes sur l'ensemble des dimensions évaluées.

Deuxièmement, les obstacles à un monitoring plus sécurisé sont structurels (budget, pression opérationnelle, compétences) et non seulement culturels. Un modèle conçu sans prendre en compte ces contraintes structurelles resterait inapplicable dans les conditions réelles du secteur.

Troisièmement, il existe une convergence remarquable entre les besoins exprimés par les répondants et les principes du modèle TRIVAH en construction : modularité selon la maturité, interopérabilité avec l'existant, traçabilité par défaut, formation avant outillage.

Quatrièmement, la désinformation constitue un risque émergent et sous-traité : sa prévalence perçue (56 % des répondants) contraste avec le faible nombre d'organisations disposant de protocoles de vérification formalisés (33 %), signalant une lacune systémique que le modèle TRIVAH devra intégrer dans son pilier de traçabilité et de fiabilité des sources.

5. Proposition d'un modèle conceptuel de veille humanitaire

5.1 Objectifs du modèle

L'analyse conduite dans les chapitres précédents a mis en évidence un constat récurrent : les dispositifs de veille humanitaire existants abordent la sécurité de l'information, la protection des données et la traçabilité des sources de manière fragmentée, en silos disciplinaires qui ne communiquent pas suffisamment entre eux. L'enquête empirique a confirmé et précisé ce constat : un peu plus des deux tiers des organisations peinent à concilier urgence opérationnelle et rigueur procédurale et un peu plus de la moitié dépendent d'outils tiers commerciaux sans chiffrement complémentaire ; aucune organisation de l'échantillon ne déclare de politique de destruction documentée des données. Ces lacunes ne sont pas le fruit d'un manque de conscience des risques car la quasi-totalité des répondants les identifient, mais d'une absence de cadre intégré permettant de les adresser de manière systématique et proportionnée.

Le modèle TRIVAH (Traçabilité - Résilience Informationnelle - Veille Adaptée à l'Humanitaire) vise à combler cette lacune en proposant une architecture conceptuelle intégrée qui répond aux quatre constats majeurs issus de l'enquête. Il articule les trois piliers fondamentaux autour d'un cycle de veille adapté aux contraintes humanitaires ; identifie et gère explicitement les tensions entre ces piliers, plutôt que de les ignorer ; fournit un outil d'auto-évaluation permettant aux organisations de se positionner et de progresser selon leur niveau de maturité ; et reste opérationnellement viable dans les environnements contraints (connectivité limitée, personnel non spécialisé, urgence, multiplicité des juridictions, budgets restreints).

Le modèle présenté dans ce chapitre est une proposition personnelle. Il n'est pas repris d'un cadre existant : il a été conçu spécifiquement pour ce travail, par synthèse des enseignements de la revue de littérature et des constats issus de l'enquête et des entretiens. Chacune de ses composantes est ainsi reliée à un besoin observé sur le terrain plutôt qu'à un présupposé théorique. Il ne prétend pas remplacer les cadres existants mais s'en nourrit pour proposer une couche d'intégration qui les organise dans la perspective spécifique d'un dispositif de veille, en comblant les angles morts que l'analyse documentaire et l'enquête ont mis en évidence.

5.2 Principes directeurs

Le modèle TRIVAH repose sur huit principes directeurs, dont les quatre derniers ont été directement nourris par les résultats de l'enquête et des études de cas.

1. ***Do No Harm* :** toute activité de veille est évaluée à l'aune de ses conséquences potentielles sur les populations vulnérables et les sources de terrain. Ce principe fondateur de l'action humanitaire s'applique intégralement à la dimension informationnelle : une donnée mal protégée peut mettre des vies en danger.
2. **Proportionnalité :** l'intensité des mesures de sécurité et de protection est proportionnelle à la sensibilité des données et au contexte opérationnel. Un système de classification à quatre niveaux guide cette calibration, évitant la double erreur de la surprotection paralysante et de la sous-protection dangereuse.

3. **Privacy by design :** la protection des données est intégrée dès la conception du dispositif : minimisation des données collectées, chiffrement par défaut, pseudonymisation systématique. Ce principe répond directement à la lacune identifiée par 56 % des répondants, qui stockent leurs données sans chiffrement complémentaire.
4. **Traçabilité documentée :** chaque information est accompagnée de métadonnées documentant son origine, ses modalités de collecte, les étapes de traitement et les validations effectuées. Ce principe répond à une lacune de l'enquête : un peu plus de la moitié des organisations documentent systématiquement l'origine exacte de leurs informations.
5. **Résilience opérationnelle :** le dispositif est conçu pour fonctionner en mode dégradé (hors ligne, ressources limitées, environnements hostiles) sans compromettre les principes fondamentaux. La déclinaison par profil de maturité (cf. chapitre 5.6) traduit opérationnellement ce principe pour les petites organisations.
6. **Interopérabilité ouverte :** le modèle privilégie les standards ouverts (HDX, KoBoToolbox) et les formats interopérables, et s'intègre aux écosystèmes existants (Microsoft 365, SharePoint) plutôt que d'imposer une migration coûteuse. Ce principe répond directement à la demande des répondants : « doit s'intégrer aux plateformes existantes » (Org. F).
7. **Souveraineté des données :** les organisations conservent le contrôle de leurs données et de celles des populations qu'elles servent. La classification par niveau de sensibilité détermine les conditions d'hébergement et de partage, réduisant la dépendance aux opérateurs commerciaux pour les données les plus sensibles.
8. **Modularité selon la maturité :** le modèle est conçu pour être adopté progressivement. Une organisation en niveau 1 (Initial) peut commencer par la fiche d'identité informationnelle et la double validation, sans avoir à déployer l'intégralité du dispositif. Ce principe répond à la demande unanime des répondants pour un modèle « simple, pratique et accessible » (Org. G).

5.3 Structure du modèle

Le modèle est structuré autour de trois piliers correspondant aux exigences de la problématique et aux trois lacunes systémiques identifiées dans l'enquête (cf. Annexe 5 : Schémas du modèle proposé). Chaque pilier est défini par ses objectifs, ses composantes opérationnelles et les tensions qu'il génère avec les deux autres, tensions que le modèle assume et gère explicitement plutôt que d'ignorer.

5.3.1 Pilier 1 : sécurité de l'information

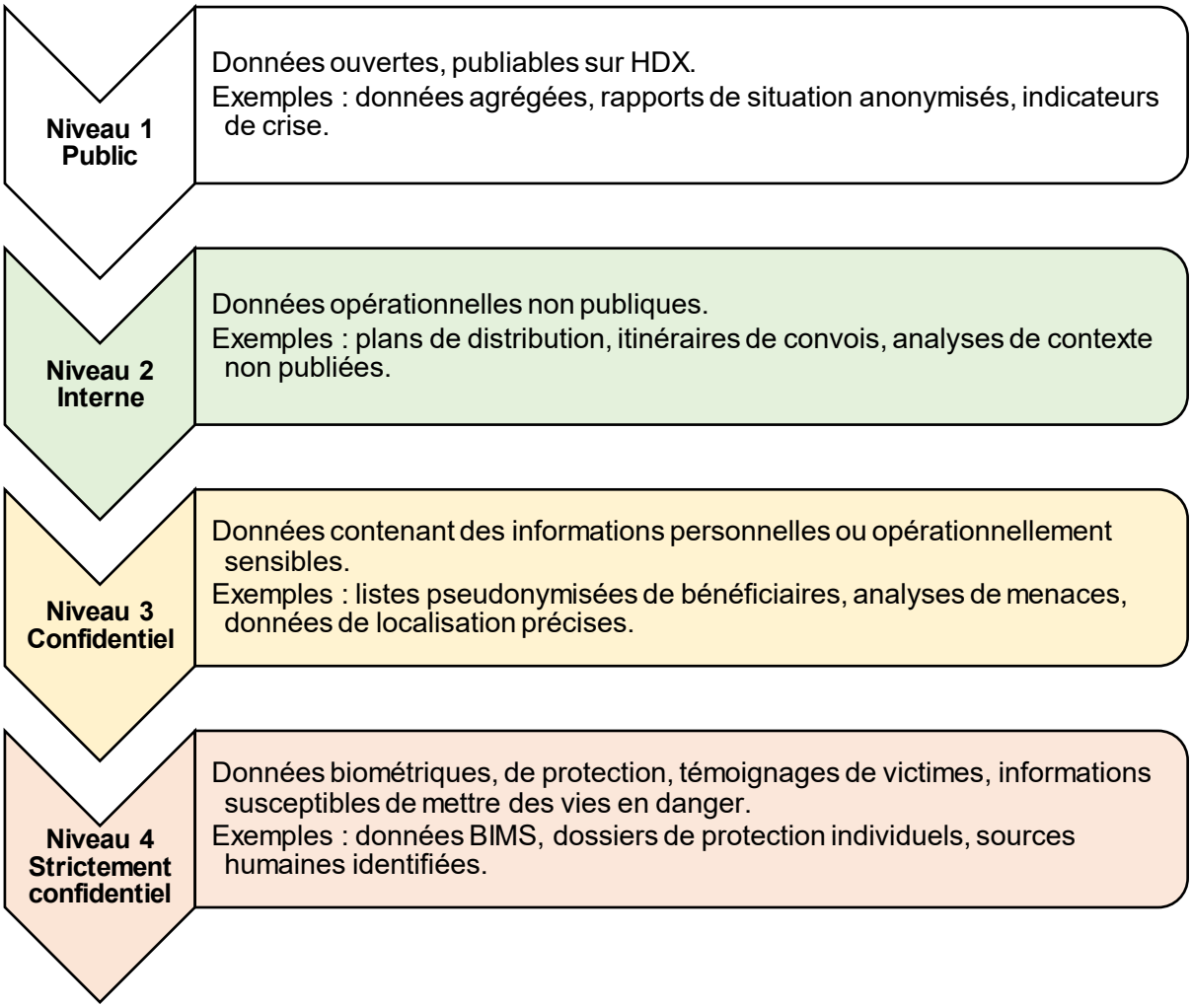
5.3.1.1 *Objectif*

Garantir la confidentialité, l'intégrité et la disponibilité des informations du dispositif de veille, en adaptant les mesures au contexte humanitaire et au niveau de sensibilité des données. Ce pilier répond directement au constat de l'enquête : 67 % des organisations ont une politique de sécurité formelle, mais seules 11 % chiffrent effectivement leurs données, et 56 % dépendent de solutions cloud commerciales sans mesures complémentaires.

5.3.1.2 Composantes opérationnelles

La figure ci-dessous détaille la classification de sensibilité par niveau en donnant des exemples pour chacun.

Figure 2 : Classification de sensibilité



© Charlotte Chuard 2026

Tableau 9 : Mesures de sécurité par niveau de sensibilité

Mesure	Niveau 1 (Public)	Niveau 2 (Interne)	Niveau 3 (Confidentiel)	Niveau 4 (Strictement confidentiel)
Chiffrement en transit	Recommandé	Obligatoire	Obligatoire	Obligatoire
Chiffrement au repos	Non requis	Recommandé	Obligatoire	Obligatoire
Contrôle d'accès	Basique	Par rôle	Rôle + authentification multifacteurs	Nominal + authentification multifacteurs
Audit log	Non requis	Recommandé	Obligatoire	Obligatoire
DPIA préalable	Non requis	Non requis	Recommandé	Obligatoire

Mesure	Niveau 1 (Public)	Niveau 2 (Interne)	Niveau 3 (Confidentiel)	Niveau 4 (Strictement confidentiel)
Durée de rétention	Libre	12 mois max	6 mois, révisé	Minimum nécessaire
Hébergement autorisé	Cloud commercial	Cloud org. + commercial	Serveurs org. / certifiés	Serveurs org. exclusivement

© Charlotte Chuard 2026

Pour la cybersécurité opérationnelle, il faut prévoir :

- Un patch management rigoureux ;
- Une segmentation réseau entre données de niveaux différents ;
- Une formation du personnel aux risques cyber (phishing, ingénierie sociale) ;
- Un plan de réponse aux incidents documenté et testé.

Ces mesures tirent directement les leçons des incidents CICR 2022 et Save the Children 2023 : dans les deux cas, une CVE non corrigée et un audit logging insuffisant ont été des facteurs aggravants déterminants.

Tout outil critique est configuré pour fonctionner hors ligne (KoBoToolbox en mode offline, RedRose, SCOPE). La synchronisation s'effectue de manière sécurisée au rétablissement de la connectivité. Ce principe répond au contexte du séisme en Turquie-Syrie, où la connectivité dégradée avait contraint les équipes à improviser des solutions non sécurisées.

5.3.1.3 *Tension : ouverture vs. protection*

Le secteur humanitaire est fondé sur le principe de transparence et de partage de l'information entre acteurs. La sécurisation des données entre en tension avec cette culture d'ouverture. Le modèle résout cette tension par le partage calibré : le niveau de partage est déterminé par la classification de sensibilité, non par une règle binaire. Les niveaux 1 et 2 sont partagés largement via HDX et les clusters ; les niveaux 3 et 4 sont diffusés selon le besoin d'en connaître (need-to-know) via des canaux sécurisés avec traçabilité des accès.

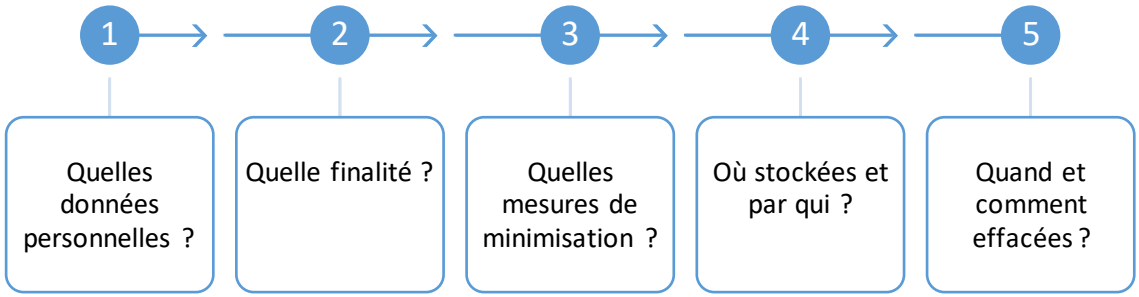
5.3.2 Pilier 2 : protection des données

5.3.2.1 *Objectif*

Garantir que la collecte, le traitement et le partage des données personnelles respectent les droits fondamentaux des personnes concernées, conformément au Handbook on Data Protection in Humanitarian Action du CICR, aux principes IASC et au RGPD. Ce pilier répond à un constat central de l'enquête : aucune organisation de l'échantillon ne déclare de politique de destruction documentée des données, et la classification formelle de sensibilité reste l'exception.

5.3.2.2 *Composantes opérationnelles*

Figure 3 : Analyse d'impact relative à la protection des données systématisée



Un formulaire simplifié à cinq questions clés, proportionné au niveau de sensibilité répond à la contrainte de temps identifiée dans l'enquête sans renoncer à l'essentiel de la démarche.

Les protocoles de consentement adaptés sont composés de trois régimes reconnaissant la diversité des réalités de terrain :

- Consentement explicite : pour les collectes non indispensables à l'aide directe (enquêtes, veille participative, crowdsourcing).
- Consentement présumé avec droit d'opposition : pour les collectes nécessaires à l'aide mais pour lesquelles une alternative est disponible.
- Base légale d'intérêt vital : pour les traitements indispensables à la survie, avec documentation renforcée dans l'audit trail.

Pour l'anonymisation, il faut prévoir une application systématique des méthodes SDC (Statistical Disclosure Control) (Hundepool et al. 2026, p. 25) avant tout partage : k-anonymité, suppression des identifiants directs, agrégation géographique au niveau district minimum. Pour les informations issues de messageries, rédaction de synthèses anonymisées plutôt que transfert de messages bruts.

Concernant la politique de rétention et effacement, les durées sont différenciées par niveau de sensibilité (cf. Tableau 9). Destruction documentée dans le registre des traitements, avec vérification trimestrielle de conformité. Ce mécanisme répond à une lacune universelle de l'échantillon : aucune organisation enquêtée ne déclare disposer d'une telle politique.

5.3.2.3 *Tension : traçabilité vs. vie privée*

La traçabilité complète des informations, nécessaire pour garantir la qualité analytique, entre en tension avec la protection des sources et des personnes identifiables. Le modèle résout cette tension par la traçabilité à couches : les métadonnées de traçabilité (date, canal, type de source) sont séparées des données identifiantes (nom, localisation exacte). La couche traçabilité est accessible aux analystes ; la couche identifiante est accessible uniquement au responsable de la protection des données, sur nécessité documentée. Cette architecture a été directement inspirée du protocole d'Org. B, seule organisation de l'échantillon à avoir formalisé cette distinction.

5.3.3 Pilier 3 : Fiabilité des sources et traçabilité

5.3.3.1 *Objectif*

Garantir que chaque information est accompagnée de métadonnées documentant son origine, sa fiabilité évaluée et les validations effectuées, permettant aux décideurs de calibrer leur

confiance dans les données qu'ils reçoivent. Ce pilier répond au constat central de l'enquête : la traçabilité est la dimension la plus défaillante de l'ensemble de l'échantillon, avec 56 % des organisations documentant l'origine exacte et moins d'un tiers documentant le niveau de confiance.

5.3.3.2 *Composantes opérationnelles*

La fiche d'identité informationnelle est un document standardisé accompagnant chaque information tout au long du cycle de veille, comprenant :

- Source primaire (type, canal, date) ;
- Évaluation de fiabilité (matrice A1-F6, inspirée du renseignement militaire adapté au contexte humanitaire) ;
- Méthode de collecte ;
- Validations effectuées et par qui ;
- Niveau de sensibilité attribué ;
- Restrictions de diffusion.

Cette fiche constitue l'outil opérationnel central du modèle, sa mise en œuvre est accessible à n'importe quelle organisation, même sans ressources technologiques significatives.

Protocole de validation en trois temps :

- Validation primaire (automatisable) : vérification de cohérence, détection de doublons, comparaison avec bases existantes. Des outils comme l'assistant IA d'Ushahidi peuvent y contribuer. Ce niveau peut être effectué par n'importe quelle organisation, y compris sans expertise technique avancée.
- Validation secondaire (semi-automatisée) : triangulation avec au moins deux sources indépendantes de canaux différents. Croisement des données terrain (KoBoToolbox), satellitaires (UNOSAT), documentaires (HDX/ReliefWeb) et participatives (Ushahidi). Ce niveau est accessible aux organisations de maturité intermédiaire.
- Validation tertiaire (humaine) : évaluation contextuelle par un analyste expert du pays ou de la thématique. Irremplaçable par la technologie, c'est le rempart contre les biais cognitifs et la désinformation sophistiquée. L'enquête confirme que 56 % des organisations perçoivent la désinformation comme un risque majeur sans disposer de protocoles pour y répondre : cette validation tertiaire est précisément la réponse à cette lacune.

Chaque action sur une information est enregistrée dans un journal de traçabilité : horodatage, agent, nature de l'action. Pour les niveaux 3 et 4, l'identité de l'agent est incluse. Ce mécanisme permet de reconstituer a posteriori la chaîne de traitement de n'importe quelle information, répondant ainsi aux enjeux de redevabilité et d'apprentissage organisationnel.

Le protocole OSINT combine une évaluation initiale de la fiabilité du canal, une vérification forensique (InVID [2026?] ; TinEye [2026?] ; métadonnées EXIF), et la documentation du contexte de publication. Sans validation secondaire, les sources OSINT sont plafonnées au niveau de confiance B2 (source fiable, information probablement vraie), le niveau B1 n'étant accordé qu'après triangulation complète.

5.3.3.3 *Tension : rapidité vs. rigueur*

C'est une tension majeure : 67 % des répondants citent l'urgence opérationnelle comme principal obstacle, et 78 % identifient la traçabilité comme un défi prioritaire (cf. chapitre 4.4.3). Le modèle la résout par la diffusion progressive : l'information est diffusée immédiatement avec un indicateur de confiance explicite, « non vérifié », « partiellement vérifié » ou « vérifié », qui évolue au fil des validations. Le décideur dispose rapidement de l'information avec son degré de fiabilité visible, sans que la décision soit bloquée par l'attente d'une validation complète. Cet indicateur s'inspire des pratiques du journalisme de crise, mais constitue une formalisation inédite dans le contexte de la veille humanitaire.

5.4 Le cycle de veille intégré TRIVAH

Le modèle articule les trois piliers dans un cycle en six phases. Chacune intègre nativement les exigences des trois piliers, matérialisées par la fiche d'identité informationnelle qui accompagne l'information de la collecte à la destruction. Le tableau ci-dessous présente le cycle complet.

Tableau 10 : Le cycle de veille intégré

Phase	Intitulé	Actions clés	Outils mobilisés	Livrables
1	Cadrage et gouvernance	Identification des besoins informationnels ; classification préliminaire de sensibilité ; DPIA pour sources/outils ; attribution des rôles (veille, analyste, DPO, RSSI) ; sélection et configuration des outils	Templates DPIA, matrice RACI (QRP International [2026?]), plan de veille	Plan de veille documenté (périmètre, sources, protocoles, responsabilités)
2	Collecte responsable	Collecte via sources autorisées avec fiche d'identité informationnelle ; protocoles de consentement adaptés ; chiffrement en transit (niv. 2-4) ; purge des métadonnées excédentaires	KoBoToolbox, OSINT, Ushahidi, Signal	Informations collectées + fiches d'identité
3	Traitement sécurisé	Validation primaire automatisée ; anonymisation/pseudonymisation SDC ; classification formelle ; stockage différencié par niveau de sensibilité	ARX (ARX [2026?]), SharePoint (niv. 1-2), serveurs org. (niv. 3-4)	Données classifiées, pseudonymisées, stockées
4	Analyse contextualisée	Validation secondaire (triangulation ≥ 2 sources) ; validation tertiaire par analyste expert ; attribution d'indicateur de confiance ; détection des signaux faibles	ACAPS CrisisInSight, InVID, TinEye, UNOSAT, PowerBI	Synthèses analytiques avec indicateur de confiance

Phase	Intitulé	Actions clés	Outils mobilisés	Livrables
5	Diffusion contrôlée	Diffusion calibrée par niveau (HDX niv. 1 ; canaux sécurisés niv. 3-4) ; indicateur de confiance visible ; enregistrement audit trail	HDX, ReliefWeb, messageries chiffrées, tableaux de bord internes	Rapports de situation, alertes, notes restreintes
6	Rétroaction, archivage et destruction	Retour des décideurs ; archivage selon politique de rétention ; destruction documentée ; mise à jour des protocoles ; vérification trimestrielle de conformité	Registre des traitements, procédure de destruction	Audit trail mis à jour, rapport de conformité

© Charlotte Chuard 2026

Le cycle est intentionnellement itératif : les enseignements tirés en phase 6 alimentent la mise à jour du plan de veille en phase 1 du cycle suivant. Cette boucle d'apprentissage organisationnel est une condition sine qua non de l'amélioration continue de la maturité.

Un point critique traverse l'ensemble du cycle : la distinction entre le rôle de la technologie et celui de l'expertise humaine. Les outils comme l'IA, les algorithmes de détection et les agrégateurs, détectent des signaux et structurent l'information. C'est l'être humain qui détermine la signification de ces signaux dans leur contexte politique, culturel et opérationnel. Le modèle insiste sur l'investissement dans l'expertise contextuelle comme condition non substituable de la qualité analytique.

5.5 Matrice des risques par phase

Chaque phase du cycle présente des risques spécifiques. La matrice ci-dessous les identifie, propose la mitigation correspondante du modèle TRIVAH, ce qui distingue ce modèle de cadres purement normatifs déconnectés du terrain.

Tableau 11 : Matrice des risques

Phase	Risques principaux	Mitigation TRIVAH	Ancrage empirique (enquête ch. 4)
1. Cadrage	Périmètre trop large, DPIA bâclée, rôles flous	Template DPIA simplifié 5 questions, matrice RACI, plan de veille standardisé	56 % ont une unité dédiée ; rôles souvent informels
2. Collecte	Collecte excessive, sources non documentées, interception	Fiche d'identité informationnelle, minimisation, chiffrement en transit	44 % n'origine pas systématiquement les données ; 11 % chiffrent
3. Traitement	Réidentification, perte d'intégrité, stockage non sécurisé	SDC (k≥5), hash d'intégrité, stockage différencié par niveau	56 % stockage cloud commercial sans

Phase	Risques principaux	Mitigation TRIVAH	Ancrage empirique (enquête ch. 4)
			chiffrement complémentaire
4. Analyse	Biais cognitifs, désinformation, manque d'expertise contextuelle	Triangulation obligatoire, indicateur confiance, formation analyste	56 % perçoivent la désinformation comme risque majeur ; protocoles : 33 %
5. Diffusion	Fuite, diffusion disproportionnée, absence de traçabilité	Need-to-know par niveau, audit trail, canaux sécurisés	67 % urgence prime sur procédure ; 33 % validation avant diffusion
6. Rétroaction	Données non détruites, rétention excessive, copies orphelines	Politique de rétention, vérification trimestrielle, procédure destruction	Lacune universelle : aucune organisation ne déclare de politique de destruction

© Charlotte Chuard 2026

5.6 Grille d'auto-évaluation de maturité

La grille d'auto-évaluation constitue l'outil opérationnel de positionnement des organisations. Elle utilise cinq niveaux inspirés du modèle CMMI (Capability Maturity Model Integration) (CMMI Institute [2026?]), adaptés au contexte humanitaire, et dix-huit critères répartis équitablement entre les trois piliers. Le score global (18 à 90) positionne l'organisation sur l'échelle de maturité. Un radar chart par pilier permet de visualiser les forces et les points de progrès prioritaires. Le tableau ci-dessous intègre les profils observés dans l'enquête pour chaque niveau.

Tableau 12 : Grille d'auto-évaluation de maturité

Niveau	Description générale	Pilier sécurité	Pilier protection	Pilier traçabilité	Profil type (enquête)
1 Initial	Pratiques ad hoc, non documentées. Les individus agissent selon leur intuition.	Aucune classification ; pas de chiffrement	Pas de DPIA ; consentement absent	Aucune fiche ; validation informelle	*Org. H (auto-éval. faible sur toutes dimensions)*
2 Reproductible	Pratiques répétées mais non formalisées. Dépend des personnes, pas des processus.	Sensibilité reconnue ; chiffrement partiel	DPIA ponctuelle ; consentement verbal	Origine tracée informellement	*Org. A, Org. G*

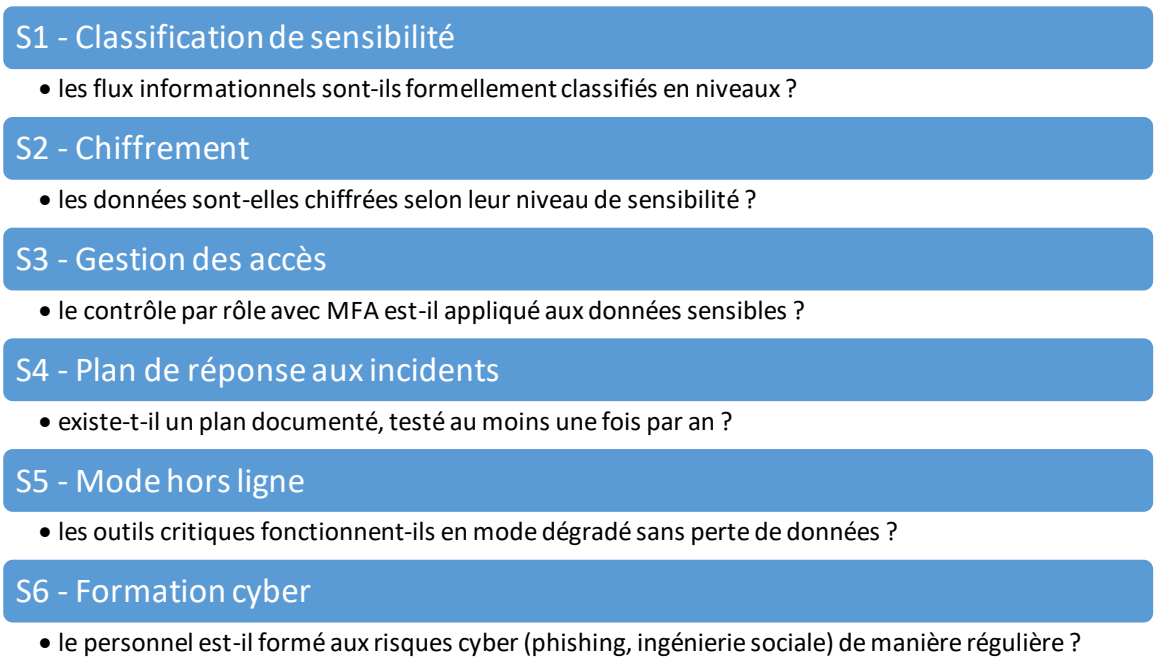
Niveau	Description générale	Pilier sécurité	Pilier protection	Pilier traçabilité	Profil type (enquête)
3 Défini	Processus documentés, formation existante. Pratiques cohérentes.	Classification formelle ; MFA pour données sensibles	DPIA systématique ; SDC appliqué	Fiche d'identité ; triangulation partielle	*Org. D, Org. F*
4 Géré	Mesures de performance, amélioration continue. Processus maîtrisés.	Audit log ; plan incident documenté et testé	Droits personnes opérationnels ; rétention définie	Triangulation systématique ; audit trail	*Org. E*
5 Optimisé	Innovation continue, apprentissage organisationnel, benchmark externe.	Mode hors ligne ; formation cyber régulière	Minimisation systématique ; destruction programmée	Protocole OSINT formel ; indicateur confiance intégré	*Org. B*

© Charlotte Chuard 2026

5.6.1 Critères par pilier

La figure ci-dessous détaille les six critères d'évaluation du pilier sécurité, chacun formulé sous forme de question fermée pour permettre une auto-évaluation rapide.

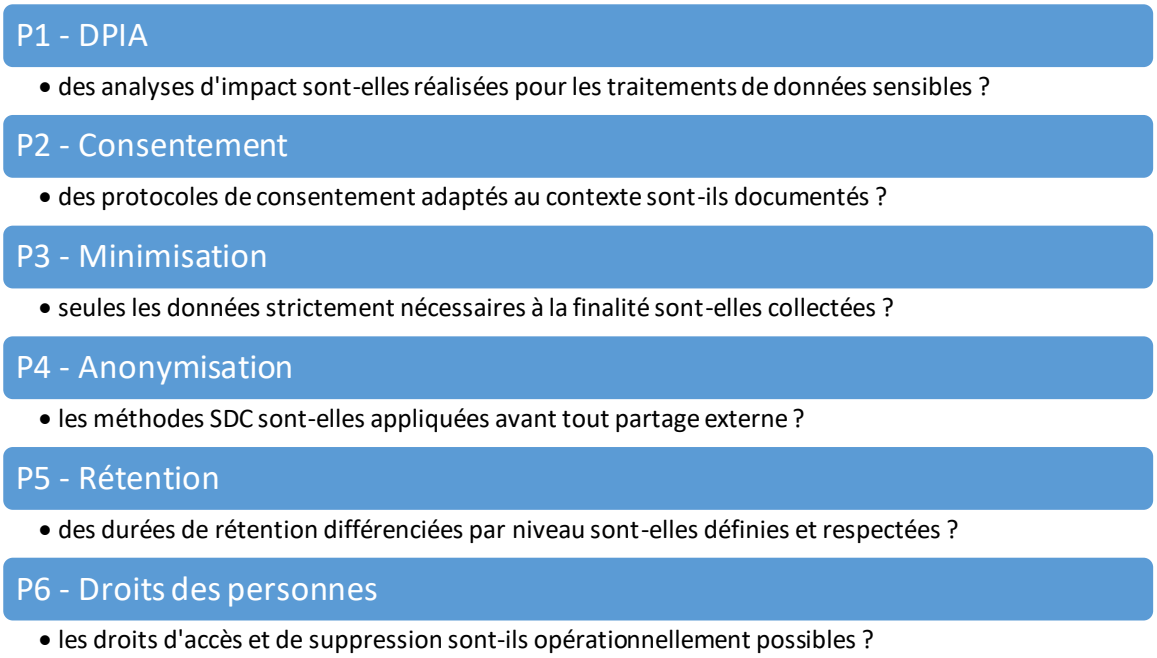
Figure 4 : Pilier sécurité



© Charlotte Chuard 2026

La figure ci-dessous détaille les six critères d'évaluation du pilier protection, chacun formulé sous forme de question fermée pour permettre une auto-évaluation rapide.

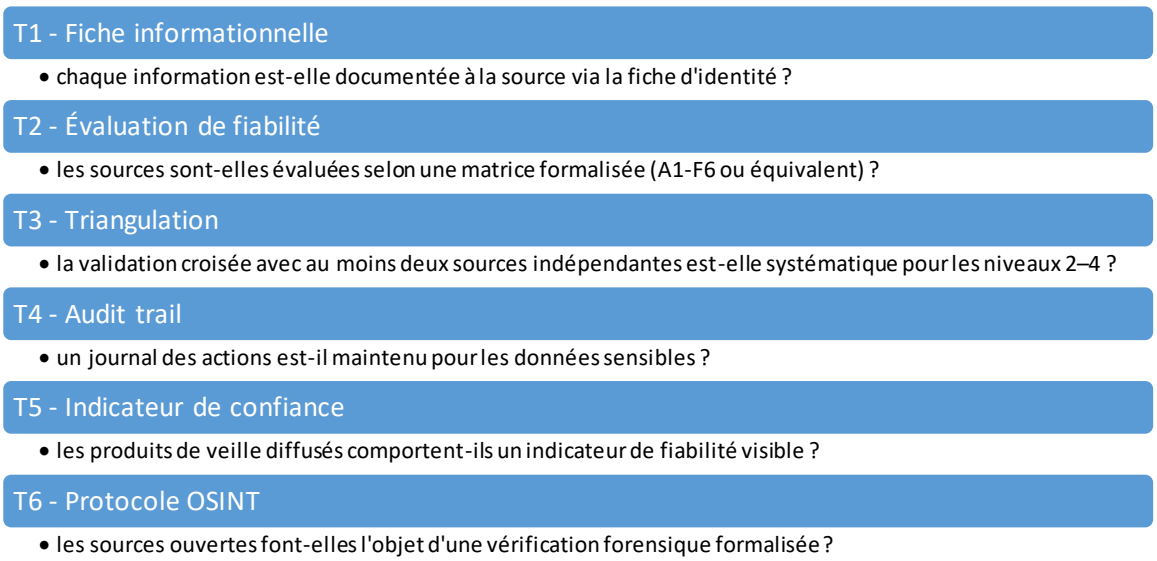
Figure 5 : Pilier protection



© Charlotte Chuard 2026

La figure ci-dessous détaille les six critères d'évaluation du pilier traçabilité, chacun formulé sous forme de question fermée pour permettre une auto-évaluation rapide.

Figure 6 : Pilier traçabilité



© Charlotte Chuard 2026

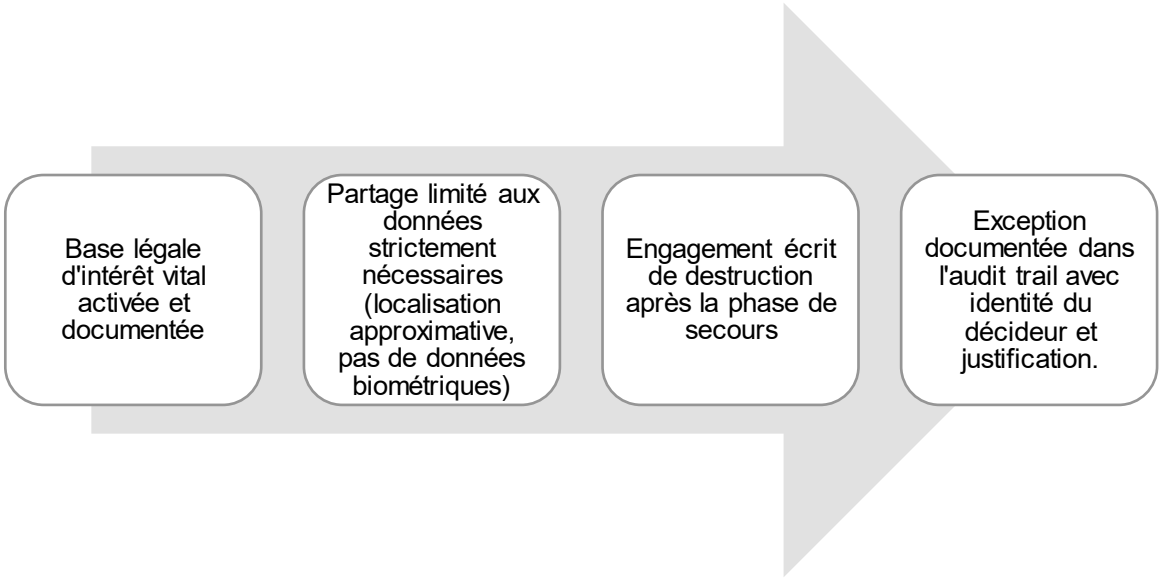
5.7 Protocoles de décision en cas de conflit entre piliers

L'une des innovations centrales du modèle est la formalisation de protocoles pour les situations où les trois piliers entrent en contradiction. Ces tensions, loin d'être exceptionnelles, constituent la réalité quotidienne du travail d'information humanitaire. Les quatre protocoles ci-dessous couvrent les situations les plus fréquemment identifiées dans la littérature et dans l'enquête.

5.7.1 Situation 1 : urgence vitale vs. protection des données

Un séisme vient de frapper. Les équipes de secours demandent l'accès aux listes de bénéficiaires de niveau 4 pour localiser des personnes potentiellement ensevelies dans les zones d'intervention.

Figure 7 : Cas 1, protocole TRIVAH



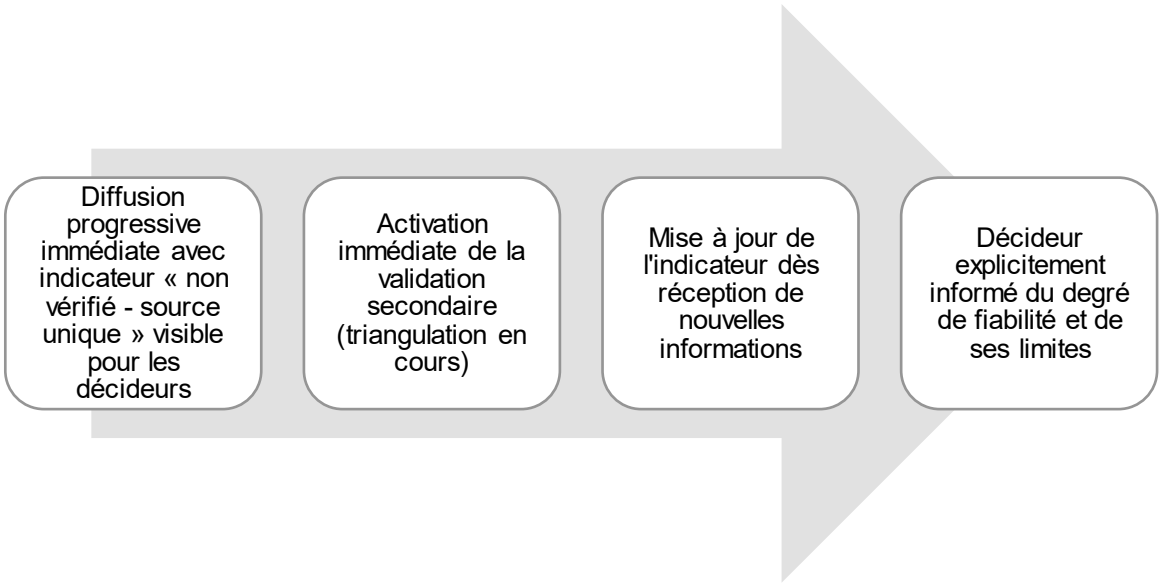
© Charlotte Chuard 2026

Ce protocole s'applique directement au contexte de la cyberattaque CICR (cf. chapitre 4.2.1) : la base légale d'intérêt vital était applicable mais non formalisée.

5.7.2 Situation 2 : rapidité vs. vérification

Des rapports crowdsourcés via Ushahidi signalent une attaque contre un camp de déplacés. L'information n'est pas encore triangulée mais une décision d'évacuation préventive est envisagée.

Figure 8 : Cas 2, protocole TRIVAH



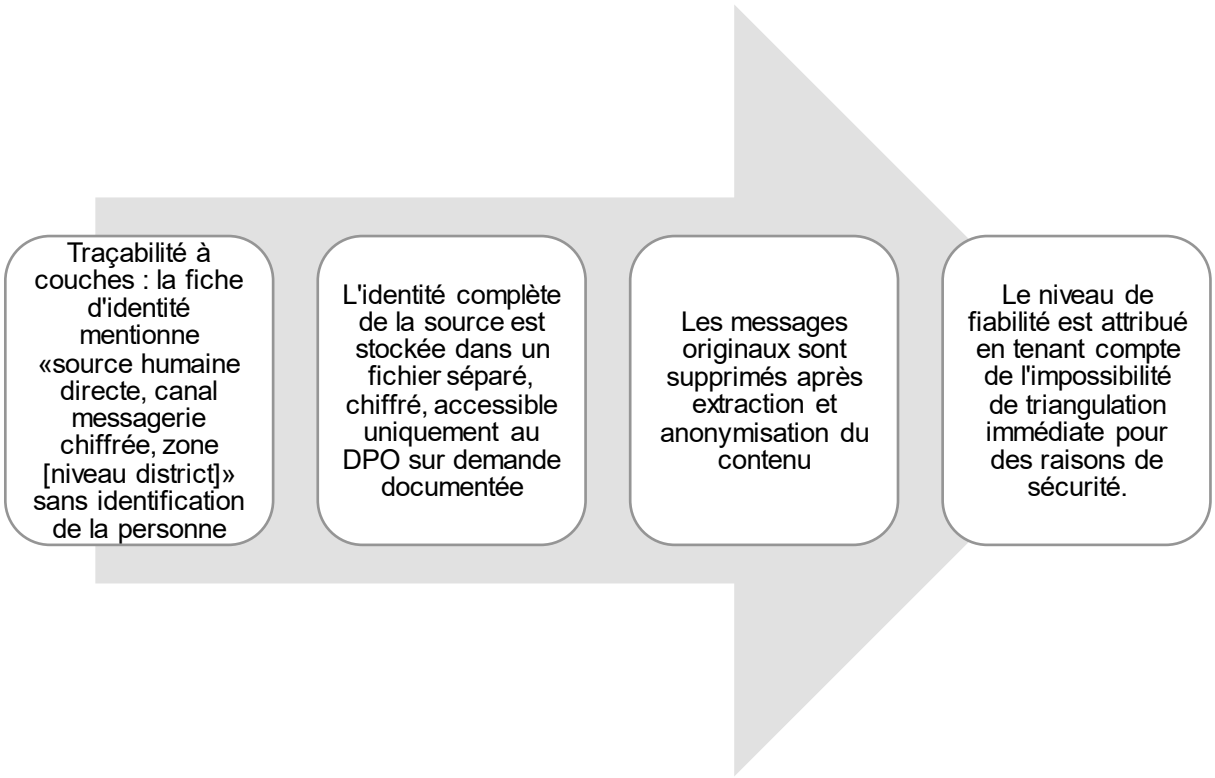
© Charlotte Chuard 2026

Cette situation correspond au scénario le plus fréquent : 67 % des répondants citent l'urgence comme principal obstacle aux protocoles de validation. L'indicateur de confiance est précisément conçu pour y répondre sans bloquer l'action.

5.7.3 Situation 3 : traçabilité vs. protection des sources

Un informateur local transmet via WhatsApp des informations sur des mouvements de groupes armés à proximité d'une zone d'intervention. L'information est précieuse mais l'informateur est identifiable par le contenu du message.

Figure 9 : Cas 3, protocole TRIVAH

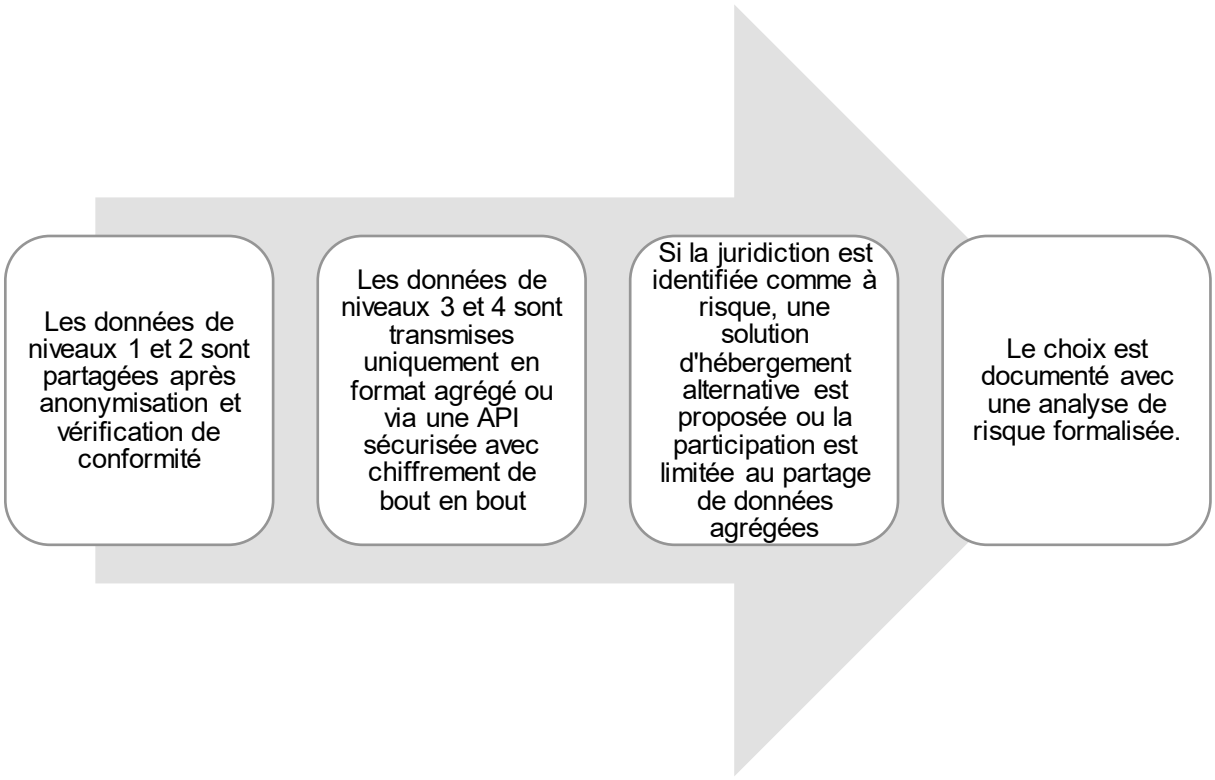


© Charlotte Chuard 2026

5.7.4 Situation 4 : interopérabilité vs. souveraineté

Le groupe de protection demande l'intégration des données de veille dans un tableau de bord hébergé sur une plateforme commerciale nord-américaine, sous juridiction non compatible avec les exigences RGPD de l'organisation.

Figure 10 : Cas 4, protocole TRIVAH



© Charlotte Chuard 2026

5.8 Innovations par rapport à l'existant

5.8.1 Intégration structurelle des trois dimensions

Les cadres existants traitent la veille, la sécurité de l'information et la protection des données de manière séparée. TRIVAH les fusionne dans un cycle unique où chaque phase intègre nativement les trois exigences, matérialisées par la fiche d'identité informationnelle. Aucun des cinq cadres examinés dans le benchmark (cf. chapitre 6.2) ne propose une telle intégration.

5.8.2 Gestion explicite des tensions

Les protocoles de décision formalisent comment arbitrer lorsque les piliers entrent en contradiction. Cette innovation est absente de l'ensemble des cadres existants, qui laissent ces arbitrages à la discrétion des praticiens sans cadre formel.

5.8.3 Classification dynamique à quatre niveaux

Le système est plus granulaire que les approches binaires (ouvert/confidentiel) ou génériques. La sensibilité est réévaluée à chaque phase du cycle, permettant une mise à jour en fonction de l'évolution du contexte opérationnel.

5.8.4 Indicateur de confiance et diffusion progressive

La formalisation de trois niveaux de fiabilité explicites sur les produits de veille concilie rapidité et rigueur. Cette pratique existe dans le journalisme de crise mais n'est pas codifiée dans les standards humanitaires existants. Elle répond directement à la tension principale identifiée dans l'enquête.

5.8.5 Grille d'auto-évaluation avec ancrage empirique

L'outil de maturité à 18 critères et cinq niveaux comble un manque identifié : l'absence d'instrument standardisé d'auto-évaluation spécifique à la veille humanitaire sécurisée. Les profils empiriques issus de l'enquête permettent aux organisations de se situer par rapport à leurs pairs.

5.8.6 Modularité selon la maturité

Le modèle est le seul cadre intégré conçu pour être adopté progressivement par des organisations de toute taille, y compris celles dépourvues de ressources technologiques significatives. Le profil de niveau 1-2 est opérationnel avec les outils existants (SharePoint, double validation, fiche papier).

5.9 Déclinaison par contexte opérationnel

Le modèle TRIVAH est conçu pour s'adapter aux contraintes spécifiques de quatre contextes opérationnels types, identifiés comme les plus fréquents dans la littérature humanitaire et les études de cas analysées. Les déclinaisons suivantes ne sont pas des variantes indépendantes mais des calibrages du même modèle : les principes directeurs et la structure des trois piliers restent constants. Seuls les seuils, les niveaux par défaut et certains protocoles spécifiques sont ajustés en fonction du contexte.

Tableau 13 : Déclinaison contextuelle du modèle TRIVAH

Contexte	Priorité dominante	Ajustements pilier sécurité	Ajustements pilier protection	Ajustements pilier traçabilité
Conflit armé	Sécurité & OPSEC	Niv. 3 par défaut ; chiffrement total ; suppression EXIF ; mode hors ligne privilégié	Consentement présumé avec documentation renforcée ; identité sources protégée	Protocole OSINT maximum ; sources humaines traçabilité à couches uniquement
Catastrophe naturelle	Rapidité & coordination	Niv. 2 par défaut ; partage élargi HDX/clusters ; DPIA simplifiée	Consentement présumé pour opérations vitales ; anonymisation avant partage	Diffusion progressive dès premier signal ; seuil triangulation abaissé (48h)
Crise sanitaire	Protection données médicales	Données médicales niv. 4 par défaut ; partage cluster santé uniquement	Consentement explicite pour enquêtes sanitaires ; k-anonymité ≥ 10	Traçabilité épidémiologique stricte ; audit trail renforcé

Contexte	Priorité dominante	Ajustements pilier sécurité	Ajustements pilier protection	Ajustements pilier traçabilité
Faibles ressources (petite ONG)	Faisabilité & accessibilité	Niv. 2 minimum ; solutions open source ; no-code	DPIA simplifiée 5 questions ; minimisation stricte	Fiche d'identité allégée ; double validation (2 personnes)

© Charlotte Chuard 2026

5.10 Limites et conditions de mise en œuvre

5.10.1 Limites

5.10.1.1 Nature conceptuelle non testée en opération

Le modèle est issu d'une synthèse théorique et empirique, mais n'a pas été déployé dans un environnement opérationnel réel. La validation conceptuelle proposée au chapitre 6 (confrontation aux études de cas et benchmark) constitue une première étape de vérification, non un test terrain.

5.10.1.2 Dépendance à l'auto-déclaration

La grille de maturité repose sur l'auto-évaluation des organisations, avec les biais inhérents à cette méthode (désirabilité sociale, subjectivité). Un mécanisme d'audit externe par les pairs renforcerait la fiabilité des résultats.

5.10.1.3 Présupposé de ressources minimales

Le modèle suppose l'accès à un DPO et à des outils de chiffrement de base. Ces ressources ne sont pas disponibles dans toutes les petites ONG de terrain, notamment dans les pays à faibles revenus. Le profil de niveau 1 atténue cette limite sans l'éliminer.

5.10.1.4 Gestion des tensions : subjectivité résiduelle

Les protocoles de décision encadrent les arbitrages entre piliers mais ne les automatisent pas. La qualité des décisions reste dépendante du jugement et de l'expertise des personnes qui les appliquent.

5.10.2 Conditions de mise en œuvre

5.10.2.1 Engagement de la direction

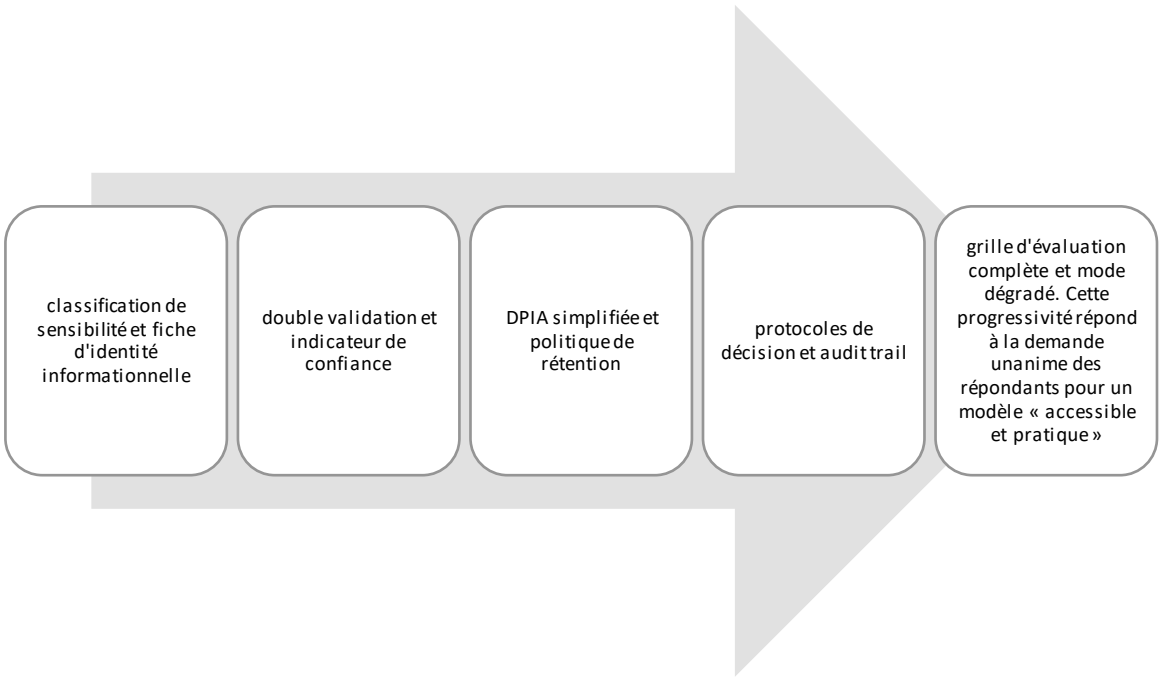
La mise en œuvre du modèle requiert un soutien institutionnel explicite allouant les ressources (temps, budget minimal, attribution des rôles) nécessaires à son déploiement progressif.

5.10.2.2 Formation initiale

Une formation de deux à trois jours est estimée nécessaire pour les niveaux 3-5 de la grille. Pour les niveaux 1-2, une demi-journée d'introduction à la fiche d'identité informationnelle et à la double validation suffit. Le Data Playbook de l'IFRC constitue une ressource pédagogique complémentaire. Cette recommandation est directement issue de l'enquête : « former le personnel avant d'outiller » (Org. E).

5.10.2.3 Mise en œuvre progressive

Figure 11 : Séquence recommandée



© Charlotte Chuard 2026

5.10.2.4 Adaptation contextuelle

Chaque organisation calibre les seuils de classification, les durées de rétention et les protocoles de consentement selon son mandat, ses zones d'intervention et ses capacités. Le modèle est un cadre, non un formulaire à compléter.

6. Validation conceptuelle du modèle

Ce chapitre vise à évaluer la robustesse et la pertinence du modèle TRIVAH en le confrontant à trois types de validation complémentaires : une application rétrospective aux études de cas humanitaires documentées, un benchmark comparatif avec les cadres existants du secteur, et une mise en regard systématique avec les résultats de l'enquête. Ces trois niveaux de validation permettent de dépasser la seule cohérence interne du modèle pour évaluer sa résonance avec les réalités opérationnelles documentées.

6.1 Validation par confrontation aux études de cas

Les deux études de cas analysées en chapitre 4.2 constituent des terrains de validation particulièrement pertinents : l'un illustre une défaillance systémique de sécurité dans une grande organisation mature (CICR, 2022) ; l'autre illustre les tensions entre rapidité de coordination et qualité informationnelle en phase aiguë de crise (séisme Turquie-Syrie, 2023). Pour chaque cas, l'analyse procède en deux temps : identification de ce que le modèle TRIVAH aurait prescrit, puis évaluation critique de la pertinence et des limites de cette prescription.

6.1.1 Cas 1 : La cyberattaque contre le CICR (janvier 2022)

Le CICR disposait, au moment de l'attaque, de pratiques informationnelles parmi les plus avancées du secteur humanitaire. Sa vulnérabilité illustre donc non pas une défaillance de maturité générale, mais des angles morts spécifiques que le modèle TRIVAH est précisément conçu pour adresser.

Tableau 14 : Application du modèle TRIVAH au cas CICR 2022

Dimension TRIVAH	Ce que le modèle aurait prescrit	Évaluation critique
Pilier 1 : sécurité	Données ICRC Restores Families : classification niv. 4 → hébergement serveurs org. exclusivement ; audit log obligatoire ; patch management rigoureux ; DPIA avant contrat prestataire	L'hébergement chez un tiers sans audit régulier contredit directement les prescriptions du modèle. La CVE exploitée aurait dû être détectée par le patch management prévu en niv. 4.
Pilier 2 : protection	Segmentation des données biométriques vs. données de localisation ; destruction programmée des données non actives ; stockage hors chaîne pour données à risque élevé	La concentration de 515 000 dossiers dans un système non segmenté illustre l'absence de stratégie de minimisation de l'exposition. Le modèle aurait imposé une architecture en couches.
Pilier 3 : traçabilité	Audit trail complet avec horodatage des accès tiers ; détection d'anomalies dans le journal d'accès ; procédure de réponse aux incidents documentée et testée	L'absence de détection précoce (plusieurs semaines) signale une lacune dans l'audit logging. Le plan de réponse aux incidents, prescrit en niv. 4, aurait réduit le temps d'exposition.

Dimension TRIVAH	Ce que le modèle aurait prescrit	Évaluation critique
Tension gérée	Situation 1 : urgence vitale vs. protection → base légale d'intérêt vital ; partage limité au strict nécessaire ; destruction post-urgence documentée	Le protocole de décision TRIVAH aurait fourni un cadre formel pour la gestion de crise, évitant les décisions ad hoc sous pression.

© Charlotte Chuard 2026

Le cas CICR 2022 valide trois composantes spécifiques du modèle : la prescription d'hébergement exclusif sur serveurs propres pour les données de niveau 4 aurait empêché la compromission via le prestataire tiers ; l'audit log obligatoire aurait permis une détection bien plus précoce de l'intrusion ; et le plan de réponse aux incidents, prescrit et testé pour le niveau 4, aurait structuré la réaction de crise. Il souligne également une limite : même un modèle correctement appliqué ne peut pas prévenir une attaque par CVE zero-day si le prestataire lui-même n'a pas corrigé sa vulnérabilité, d'où l'importance des clauses contractuelles de sécurité pour les prestataires tiers, qui devraient être intégrées à la phase 1 du cycle.

6.1.2 Cas 2 : le séisme en Turquie et Syrie (février 2023)

Ce cas illustre les tensions de coordination informationnelle en phase aiguë de crise à grande échelle. Il permet de tester la résilience opérationnelle du modèle dans un contexte de connectivité dégradée, de pression temporelle maximale et de multiplicité des acteurs.

Tableau 15 : Application du modèle TRIVAH au cas séisme Turquie-Syrie 2023

Dimension TRIVAH	Ce que le modèle aurait prescrit	Évaluation critique
Pilier 1 : sécurité	Mode hors ligne activé dès le premier jour ; classification niv. 2 par défaut pour contexte catastrophe naturelle ; niv. 3 pour données de localisation Syrie	Le mode hors ligne est directement applicable au contexte de connectivité dégradée des premières 72h. La différenciation Turquie/Syrie selon le contexte sécuritaire illustre la pertinence de la déclinaison contextuelle.
Pilier 2 : protection	DPIA simplifiée (catastrophe naturelle) mais agrégation géographique obligatoire avant partage ; données de localisation niv. 3 en contexte syrien	La publication de données géolocalisées précises sans agrégation suffisante constitue le principal écart identifié. Le modèle l'aurait prévenu par la règle d'agrégation au niveau district.
Pilier 3 : traçabilité	Diffusion progressive dès le premier signal Ushahidi ; indicateur de confiance visible sur tous les produits ; triangulation	La saturation informationnelle et les doublons auraient été partiellement résolus par l'indicateur de confiance visible, permettant aux acteurs de

Dimension TRIVAH	Ce que le modèle aurait prescrit	Évaluation critique
	sous 48h pour catastrophe naturelle	distinguer l'information vérifiée de l'information brute.
Tension gérée	Situation 2 : rapidité vs. Vérification → diffusion progressive « non vérifié » immédiate ; triangulation en cours ; mise à jour automatique de l'indicateur	Le protocole de diffusion progressive est précisément conçu pour ce type de situation. Il aurait permis une réponse rapide sans compromettre la qualité analytique à terme.

© Charlotte Chuard 2026

Le cas valide en particulier deux innovations du modèle : le mécanisme de diffusion progressive avec indicateur de confiance, qui aurait résolu la tension entre rapidité et qualité sans bloquer l'action ; et la déclinaison contextuelle différenciée (catastrophe naturelle pour la Turquie, conflit armé pour la Syrie), qui aurait permis d'appliquer des niveaux de protection différenciés selon le risque réel. Il souligne également que la coordination entre acteurs multiples dépasse le périmètre d'une seule organisation et nécessite une adoption collective du modèle pour produire des effets à l'échelle du système humanitaire.

6.2 Validation par benchmark

Le benchmark compare le modèle TRIVAH à cinq cadres de référence du secteur humanitaire : les OCHA IM Guidelines, le Handbook on Data Protection in Humanitarian Action du CICR (2024), la méthodologie analytique d'ACAPS CrisisInSight, le Data Playbook de l'IFRC et les IASC Data Responsibility Guidelines. Ces cadres ont été sélectionnés parce qu'ils couvrent ensemble les trois dimensions du modèle (veille, sécurité, protection) et représentent les standards professionnels les plus cités dans la littérature.

Tableau 16 : Benchmark comparatif

Critère	TRIVAH	OCHA IM Guidelines	CICR Handbook	ACAPS CrisisInSight	IFRC Data Playbook	Écart / apport TRIVAH
Intégration veille + sécurité + protection	Oui, cycle unifié	Partiel, IM seul	Protection données seule	Analytique seul	Protection seule	TRIVAH seul intègre les 3 dans un cycle unique
Classification de sensibilité opérationnelle	4 niveaux graduels	Générique	Général	Non prévu	Non prévu	Granularité supérieure avec mesures différenciées
Gestion des tensions inter-piliers	Protocoles formels (4 situations)	Non prévu	Non prévu	Non prévu	Non prévu	Innovation absente des cadres existants

Critère	TRIVAH	OCHA IM Guidelines	CICR Handbook	ACAPS CrisisInSight	IFRC Data Playbook	Écart / apport TRIVAH
Outil d'auto-évaluation de maturité	Grille 18 critères / 5 niveaux	Non	Non	Non	Partiel (modules)	Standardisation et visualisation radar chart
Déclinaison contextuelle	4 contextes (conflit, catastrophe, sanitaire, faibles ressources)	Non	Partiel (conflits)	Partiel (crises)	Partiel (contextes faibles ressources)	Couverture contextuelle plus complète
Indicateur de confiance explicite	Oui, 3 niveaux diffusion progressive	Non	Non	Partiel (scores)	Non	Formalisation d'une pratique journalistique peu codifiée en veille humanitaire
Mode hors ligne / résilience dégradée	Intégré dès la conception	Mentionné	Non	Non	Non	Opérationnalisation concrète du principe de résilience
Accessibilité (petites ONG)	Profil niveau 1-2 ; no-code	Limité	Limité	Non	Oui	TRIVAH : seul cadre intégré accessible aux petites structures

© Charlotte Chuard 2026

Le benchmark confirme la valeur ajoutée différentielle du modèle TRIVAH sur trois dimensions principales. Premièrement, l'intégration structurelle : aucun cadre existant n'articule les trois dimensions (veille, sécurité, protection) dans un cycle opérationnel unique. Les praticiens doivent actuellement naviguer entre plusieurs documents normatifs sans guide d'intégration. Deuxièmement, la gestion formalisée des tensions : les protocoles de décision constituent une innovation sans équivalent dans les cadres analysés, qui laissent les arbitrages inter-piliers à la discrétion des praticiens. Troisièmement, l'accessibilité aux petites organisations : seul le Data Playbook de l'IFRC adresse explicitement les contextes à faibles ressources, mais sans l'articulation avec la sécurité et la traçabilité que TRIVAH propose.

Le benchmark révèle également une limite importante : le modèle TRIVAH est moins prescriptif que certains cadres existants sur des points techniques spécifiques, les détails du système de classification SDC pour l'anonymisation, ou les spécifications techniques du chiffrement. Il renvoie sur ces points aux standards existants (OCHA Guidance Note on Data Security, Handbook CICR), confirmant son positionnement comme couche d'intégration plutôt que comme substitut à ces cadres.

6.3 Mise en regard avec les résultats de l'enquête

La troisième validation confronte systématiquement les composantes du modèle aux constats empiriques de l'enquête. Cette mise en regard permet d'évaluer dans quelle mesure le modèle répond aux besoins réels identifiés sur le terrain, et d'identifier les composantes dont la pertinence est la plus forte ou la plus limitée au regard des pratiques déclarées.

Tableau 17 : Mise en regard des constats

Constat empirique	Réponse TRIVAH	Niveau du modèle	Évaluation de pertinence
67 % : urgence prime sur procédure	Diffusion progressive + indicateur de confiance : l'information circule immédiatement avec son degré de fiabilité, sans bloquer l'action	Pilier 3, phase 5	Forte : répond directement à la tension principale du secteur
56 % : désinformation perçue comme risque, protocoles absents dans 67 % des cas	Protocole OSINT formel ; triangulation obligatoire (≥2 sources indépendantes) ; validation tertiaire humaine	Pilier 3, phase 4	Forte : comble la lacune la plus citée dans l'enquête
56 % : stockage cloud commercial sans chiffrement	Classification 4 niveaux avec hébergement différencié ; chiffrement obligatoire niv. 2+ ; DPIA avant tout outil tiers	Pilier 1	Forte : faisabilité limitée pour petites ONG sans budget ; profil niv. 1 prévu
100 % : budget conditionne les choix	Profil d'entrée niveau 1-2 : fiche d'identité + double validation + SharePoint existant → zéro coût additionnel	Niveaux 1-2 de la grille	Très forte : c'est précisément la réponse à la demande de simplicité (Org. G, Org. H)
33 % seulement : validation formelle avant diffusion	Protocole de validation en 3 temps ; indicateur de confiance visible ; phase 5 de diffusion contrôlée	Pilier 3, phase 4-5	Forte : le protocole est conçu pour être appliqué même sous pression

Constat empirique	Réponse TRIVAH	Niveau du modèle	Évaluation de pertinence
11 % : chiffrement des données collectées	Chiffrement recommandé niv. 1, obligatoire niv. 2+ ; outils open source (VeraCrypt, Signal) pour contextes à faibles ressources	Pilier 1	Partielle : suppose un minimum de compétence technique
Aucune organisation : politique de destruction documentée	Phase 6 : destruction documentée ; vérification trimestrielle de conformité ; registre des traitements	Pilier 2, phase 6	Forte : comble une lacune universelle de l'échantillon

© Charlotte Chuard 2026

Cette mise en regard permet de dégager quatre conclusions de validation.

Le modèle répond aux lacunes les plus universelles. La politique de destruction documentée (phase 6) et l'indicateur de confiance (pilier 3, phase 5) adressent des lacunes présentes dans la totalité ou la quasi-totalité de l'échantillon. Leur implémentation ne requiert pas de ressources significatives et peut s'effectuer dans n'importe quelle organisation dès le niveau 2 de la grille de maturité.

La faisabilité est différenciée selon la taille. Les composantes techniques du pilier 1 ont une pertinence élevée mais une faisabilité limitée pour les organisations de niveau 1 (Org. A, Org. G, Org. H). Le profil d'entrée du modèle (fiche d'identité + double validation + SharePoint existant, zéro coût additionnel) a été spécifiquement conçu pour cette contrainte, mais sa robustesse reste inférieure aux niveaux supérieurs.

La tension rapidité-rigueur est la mieux adressée. Le mécanisme de diffusion progressive avec indicateur de confiance a reçu la meilleure évaluation de pertinence lors des entretiens et correspond précisément à la tension la plus fréquemment citée dans le questionnaire. C'est la composante du modèle pour laquelle la demande terrain est la plus clairement exprimée.

La formation avant l'outillage est une condition non négociable. Les entretiens confirment de manière convergente que l'adoption d'un modèle comme TRIVAH ne peut pas reposer sur la seule mise à disposition d'outils : « il faut former les équipes d'abord, les outils viennent ensuite » (Org. E). Cette séquence est intégrée dans les conditions de mise en œuvre du modèle et doit être considérée comme une condition sine qua non, non comme une recommandation optionnelle.

6.4 Synthèse de la validation

Les trois niveaux de validation convergent vers une évaluation cohérente de la robustesse et des limites du modèle TRIVAH.

Sur le plan de la pertinence sectorielle, le modèle répond à des besoins réels et documentés. Les quatre tensions identifiées dans l'enquête (urgence vs. procédure, désinformation sous-protocolarisée, dépendance aux outils tiers, contraintes budgétaires) trouvent toutes une réponse explicite dans les composantes du modèle. Le benchmark confirme qu'aucun cadre existant ne propose une intégration comparable.

Sur le plan de la faisabilité, la modularité par niveaux de maturité est la condition principale de viabilité. Elle permet d'éviter l'écueil des cadres trop ambitieux qui restent inappliqués faute d'être accessibles. La mise en regard avec l'enquête suggère que le profil d'entrée (niveaux 1-2) est réaliste pour la majorité des organisations de l'échantillon.

Sur le plan des limites résiduelles, deux points appellent des développements futurs. Premièrement, la coordination inter-organisationnelle : le modèle est conçu pour une organisation et ne résout pas les enjeux de gouvernance collective dans les systèmes multi-acteurs (coordination clusters, partage HDX). Deuxièmement, l'implémentation technique dans des environnements extrêmement contraints (connectivité nulle, absence totale de personnel technique) reste un défi que le profil de niveau 1 atténue sans résoudre entièrement.

Ces limites ouvrent des pistes de recherche pour des travaux futurs : test pilote du modèle dans une organisation volontaire, développement d'un protocole de coordination inter-organisationnelle, et adaptation du modèle aux contextes de déconnexion totale. Ces perspectives sont développées en chapitre 7.

7. Discussion

Ce chapitre prend du recul sur l'ensemble de la démarche conduite. Il revient sur les apports du modèle TRIVAH au regard de la problématique initiale, assume les limites du travail dans sa globalité, précise les conditions concrètes de sa mise en œuvre, propose une réflexion critique sur les enjeux éthiques, techniques et organisationnels qu'il soulève, et ouvre sur des perspectives de recherche futures.

7.1 Apports du modèle

La problématique de ce travail interrogeait la manière de structurer un dispositif de veille humanitaire intégrant de façon cohérente la sécurité de l'information, la protection des données et la traçabilité des sources, tout en restant adapté aux contraintes opérationnelles du secteur. Le modèle TRIVAH constitue une réponse à cette question, dont les apports peuvent être résumés en quatre points.

Le diagnostic documentaire et le benchmark (cf. chapitre 6.2) convergent sur un même constat : aucun cadre existant n'articule simultanément la veille, la sécurité de l'information et la protection des données dans un cycle opérationnel unique. Les praticiens doivent aujourd'hui naviguer entre plusieurs référentiels (Data Responsibility Guidelines d'OCHA, Handbook on Data Protection du CICR, standards IASC) sans guide d'articulation. TRIVAH ne remplace pas ces référentiels mais propose la couche d'intégration qui leur manquait.

Chaque composante du modèle peut être reliée explicitement à un constat de l'enquête empirique : la diffusion progressive avec indicateur de confiance répond à la tension citée par 67 % des répondants entre urgence et procédure ; la politique de destruction documentée comble une lacune que la totalité de l'échantillon présentait. Cette traçabilité entre les données et les choix de conception, systématisée dans le Tableau 17, distingue TRIVAH des modèles élaborés par déduction théorique pure.

Les quatre protocoles de décision (cf. chapitre 5.7) formalisent des arbitrages que les cadres existants laissent à la discrétion des praticiens. Cette formalisation ne supprime pas la difficulté de l'arbitrage, mais elle offre un cadre de référence partagé qui réduit la part d'improvisation en situation de crise, comme l'illustre rétrospectivement le cas du séisme Turquie-Syrie.

L'enquête a révélé un secteur à deux vitesses, où la maturité informationnelle est davantage corrélée à la spécialisation qu'à la taille organisationnelle. En proposant un profil d'entrée opérationnel dès le niveau 1-2 de la grille de maturité, sans investissement technologique préalable, TRIVAH cherche à éviter l'écueil des modèles ambitieux mais inapplicables aux structures aux ressources limitées, qui constituent pourtant une part importante du secteur.

Ces apports doivent cependant être lus à la lumière d'une réserve de fond : ils relèvent d'une validation conceptuelle, non d'une mise à l'épreuve opérationnelle. Le modèle propose une architecture cohérente et ancrée empiriquement, mais sa capacité à produire ces effets dans la durée et en conditions réelles reste, à ce stade, une hypothèse de travail plutôt qu'un résultat établi.

7.2 Limites du travail

Les limites méthodologiques propres à l'enquête ont été détaillées en chapitre 1.5.4. Cette section les reprend à un niveau plus large, en les articulant aux conséquences qu'elles ont sur

la portée du modèle proposé, et en y ajoutant les limites propres à la démarche de modélisation elle-même.

7.2.1 Limites liées au terrain empirique

Neuf répondants issus de huit organisations ne permettent pas d'établir une photographie représentative du secteur humanitaire dans son ensemble. Le biais de sélection identifié en 1.5.4 entraîne une conséquence directe sur le modèle : les besoins exprimés par l'échantillon, sur lesquels TRIVAH s'appuie, peuvent ne pas refléter fidèlement les besoins des organisations les moins matures du secteur, c'est-à-dire celles que le modèle cherche précisément à outiller en priorité avec son profil d'entrée. Il existe ainsi un paradoxe méthodologique : le modèle vise les organisations sous-représentées dans les données qui l'ont nourri.

Les répondants sont majoritairement basés en Suisse ou en Europe occidentale. Les contraintes spécifiques aux organisations du Sud global comme l'accès à l'électricité et à la connectivité, les cadres juridiques de protection des données souvent embryonnaires et le rapport différent à la centralisation occidentale des outils numériques, ne sont donc appréhendées qu'indirectement, par le biais de la littérature documentaire et non par l'enquête elle-même.

Comme mentionné en chapitre 1.5.4, l'écart entre pratiques déclarées et pratiques effectives constitue une source d'incertitude résiduelle. Cette limite affecte directement la grille de maturité du modèle, qui repose sur le principe de l'auto-évaluation : une organisation peut surestimer ou sous-estimer sa propre maturité sans mécanisme de vérification externe.

7.2.2 Limites propres à la démarche de modélisation

TRIVAH n'a pas été déployé dans un contexte opérationnel réel. La validation conceptuelle constitue une démonstration de cohérence et de pertinence apparente, mais ne peut se substituer à un test d'implémentation. Des difficultés d'adoption, des coûts de transition sous-estimés ou des résistances organisationnelles pourraient n'apparaître qu'à l'usage.

L'application du modèle aux cas du CICR et du séisme Turquie-Syrie part d'une connaissance déjà acquise de ce qui a dysfonctionné dans ces situations. Le modèle a été conçu après ces incidents et en partie grâce à l'analyse de leurs causes ; il n'est donc pas surprenant qu'il y réponde de façon pertinente. Cette validation démontre la cohérence interne du modèle face à des défaillances connues, mais ne prouve pas sa capacité à anticiper des défaillances encore non documentées.

Le modèle suppose, même à son niveau d'entrée, l'existence d'un minimum de fonction de protection des données (DPO, même non dédié) et la capacité à attribuer des rôles. Cette exigence, modeste en apparence, peut représenter un obstacle réel pour des organisations dont le personnel est entièrement mobilisé par l'action opérationnelle.

TRIVAH est conçu pour une organisation et ne résout pas les enjeux de gouvernance collective propres aux systèmes multi-acteurs (coordination de clusters, partage de données via HDX entre organisations). Or, l'étude de cas du séisme Turquie-Syrie montre que c'est précisément à cette échelle inter-organisationnelle que se posent certains des problèmes les plus aigus.

7.3 Conditions de mise en œuvre en pratique

Au-delà des conditions déjà formulées en chapitre 5.10.2, l'ensemble de la démarche conduite dans ce travail permet d'identifier trois conditions transversales, qui ne relèvent pas d'une seule composante du modèle mais de la philosophie de son adoption.

Les organisations de l'échantillon les plus éloignées de la maturité visée (Org. H notamment) ne pourront pas adopter l'ensemble du modèle d'un seul mouvement. L'enjeu pour ces structures n'est pas d'atteindre rapidement le niveau 5 de la grille, mais de franchir, de manière réaliste, le passage du niveau 1 au niveau 2, par exemple en commençant uniquement par la fiche d'identité informationnelle et la double validation, sans attendre de disposer de moyens techniques plus avancés.

La recommandation des répondants de « former le personnel avant d'outiller » (Org. E) entraîne une conséquence pratique souvent sous-estimée : l'attribution des rôles (phase 1 du cycle) doit précéder le choix des outils. Une organisation qui acquiert un outil de social listening avant d'avoir désigné qui en sera responsable, qui validera les informations collectées et qui sera garant de leur destruction reproduit, avec un outil neuf, les mêmes lacunes de gouvernance que l'enquête a mises en évidence.

Les tableaux de mesures de sécurité et de protection (cf. chapitre 5.3) décrivent un état cible. Le passage de l'état actuel d'une organisation à cet état cible représente un effort transitoire qui n'est pas chiffré dans ce travail et qui devra être budgété explicitement par toute organisation engageant cette démarche.

7.4 Réflexion critique

7.4.1 Enjeux éthiques

Le modèle TRIVAH repose sur le principe directeur *Do No Harm*, mais ce principe, énoncé comme une évidence, recouvre des arbitrages concrets qui méritent d'être interrogés plutôt que présupposés résolus. Le protocole de la Situation 1 (cf. chapitre 5.7) autorise un partage de données normalement protégées sur la base d'une « base légale d'intérêt vital ». Cette flexibilité, nécessaire pour ne pas entraver une réponse de secours, ouvre aussi un espace d'interprétation : qui décide, dans l'urgence, que le seuil de l'intérêt vital est atteint ? Le modèle documente l'exception dans l'audit trail mais ne résout pas la question de fond, qui reste un jugement humain situé, potentiellement sujet à des pressions opérationnelles ou hiérarchiques.

La tension entre traçabilité et protection des sources (Situation 3) pose un dilemme analogue, déjà identifié dans la littérature sur le renseignement humain en contexte de conflit : plus une information est tracée avec précision, plus elle devient potentiellement compromettante pour la personne qui l'a fournie. La traçabilité à couches proposée par le modèle atténue ce risque sans l'annuler, puisqu'un fichier d'identité séparé, même chiffré et restreint au DPO, demeure un point de défaillance possible, comme l'a précisément illustré, à une autre échelle, la compromission des données du CICR en 2022.

Enfin, la grille de maturité elle-même soulève une question éthique secondaire : en positionnant des organisations sur une échelle de 1 à 5, elle introduit implicitement une hiérarchie de légitimité informationnelle. Le risque est qu'une organisation de niveau 1, déjà confrontée à des contraintes de ressources sévères, voie cette évaluation utilisée par des

bailleurs ou des partenaires comme un critère d'exclusion plutôt que comme un outil de progression, ce qui irait à l'encontre de l'intention initiale du modèle.

7.4.2 Enjeux techniques

Le modèle TRIVAH mobilise des dispositifs techniques (chiffrement, anonymisation par contrôle de divulgation statistique, authentification multi-facteurs, audit log) dont la mise en œuvre suppose des compétences qui ne sont pas uniformément distribuées dans le secteur. L'enquête a montré que les méthodes de SDC, par exemple, nécessitent une expertise statistique qui n'est pas toujours disponible dans les équipes de terrain, un constat documenté indépendamment dans la littérature. Le modèle prescrit ces mesures sans pour autant résoudre le problème de la capacité à les mettre en œuvre, renvoyant implicitement à des formations ou à des prestations externes dont le coût n'est pas budgété.

La question du mode dégradé illustre une autre tension technique. Le modèle prescrit un fonctionnement hors ligne pour les outils critiques, ce qui répond bien à la réalité de connectivité intermittente documentée par les études de cas. Mais la synchronisation différée qui en découle crée mécaniquement une fenêtre de vulnérabilité : les données collectées hors ligne restent, par définition, moins protégées et moins traçables tant qu'elles n'ont pas été synchronisées vers l'environnement sécurisé. Le modèle ne détaille pas de mesure compensatoire spécifique pour cette fenêtre, qui reste un angle mort technique.

7.4.3 Enjeux organisationnels

L'enquête a mis en évidence que la maturité informationnelle est davantage corrélée à la spécialisation fonctionnelle qu'à la taille de l'organisation. Cette conclusion a une implication organisationnelle qui dépasse le strict périmètre du modèle : elle suggère que la création d'une fonction dédiée à la veille sécurisée, même réduite, produit un effet de professionnalisation supérieur à l'augmentation des moyens généraux d'une organisation déjà volumineuse. Or, le modèle TRIVAH, centré sur les processus et les outils, ne traite qu'indirectement cette question, pourtant déterminante, de la structure organisationnelle et de l'attribution claire d'une responsabilité identifiable.

Par ailleurs, la culture organisationnelle de valorisation de l'expertise terrain au détriment de la formalisation, identifiée comme explication du paradoxe « grande organisation, monitoring ad hoc », constitue un obstacle qu'aucun protocole ne peut surmonter par lui-même. L'adoption du modèle suppose un changement culturel c'est-à-dire d'accepter que la rigueur documentaire ne s'oppose pas à la rapidité d'action mais la conditionne à long terme, ce qui relève davantage du leadership organisationnel que de l'ingénierie de processus.

7.5 Perspectives de recherche

Les limites identifiées dans ce chapitre, ainsi que celles déjà relevées au fil de la synthèse de validation, ouvrent plusieurs pistes pour des travaux futurs.

La priorité la plus immédiate serait de tester le profil d'entrée du modèle (niveaux 1-2) au sein d'une organisation volontaire de taille restreinte, sur une période suffisante pour observer non seulement la faisabilité technique, mais aussi les résistances organisationnelles et les ajustements nécessaires en situation réelle.

Le modèle, conçu à l'échelle d'une organisation, devrait être complété par une réflexion sur son interopérabilité à l'échelle d'un cluster ou d'un système de coordination multi-acteurs, en

s'appuyant notamment sur les mécanismes déjà existants (Information Management Officers, HDX) plutôt qu'en les dupliquant.

Le mode dégradé prévu par le modèle suppose un rétablissement de la connectivité à terme. Des contextes de déconnexion prolongée ou structurelle, fréquents dans certaines zones d'intervention, mériteraient une déclinaison spécifique du modèle, au-delà des quatre contextes déjà documentés en chapitre 5.9.

Un mécanisme d'audit par les pairs, ou une confrontation entre auto-évaluation et évaluation externe, permettrait de tester la fiabilité de la grille proposée et de corriger les biais de désirabilité sociale inhérents à l'auto-déclaration.

Le constat selon lequel la maturité informationnelle est davantage corrélée à la spécialisation qu'à la taille organisationnelle mériterait d'être approfondi par une étude dédiée, qui dépasserait le périmètre de ce travail mais en prolongerait directement l'un des résultats les plus significatifs.

8. Conclusion

8.1 Synthèse des résultats

Ce travail s'est donné pour objectif de proposer un modèle conceptuel de veille intégrant les dimensions de sécurité de l'information, de protection des données et de traçabilité des sources, adapté aux contraintes opérationnelles du secteur humanitaire. La démarche a articulé trois temps complémentaires.

L'état de l'art a établi que la veille humanitaire s'est transformée, en une décennie, d'une pratique artisanale et fragmentée en un écosystème numérique structuré autour de plateformes, d'acteurs spécialisés et de cadres normatifs. Cette transformation s'accompagne d'une exposition accrue aux risques informationnels, illustrée notamment par la cyberattaque contre le CICR en 2022 et l'incident BianLian contre Save the Children en 2023, qui ont marqué une prise de conscience sectorielle durable.

Le diagnostic empirique, conduit par questionnaire auprès de neuf répondants issus de huit organisations et complété par des entretiens semi-directifs et deux études de cas documentées, a permis de dégager quatre constats majeurs : l'urgence opérationnelle prime systématiquement sur la procédure ; la désinformation est perçue comme un risque majeur sans être systématiquement protocolarisée ; les outils tiers commerciaux dominent au détriment de la souveraineté des données ; et le budget conditionne fortement les choix technologiques. Le diagnostic a également révélé que la maturité informationnelle est davantage corrélée à la spécialisation fonctionnelle des organisations qu'à leur taille.

La modélisation conceptuelle, enfin, a traduit ces constats en un dispositif structuré : le modèle TRIVAH, organisé autour de trois piliers (sécurité, protection, traçabilité), d'un cycle de veille en six phases, de quatre protocoles de décision pour les situations de tension inter-piliers, et d'une grille d'auto-évaluation de maturité à cinq niveaux. Sa validation conceptuelle, conduite par confrontation à des cas réels, comparaison avec les cadres existants et mise en regard avec les données de l'enquête, a confirmé la pertinence de cette architecture tout en identifiant ses limites propres, notamment l'absence de test en conditions opérationnelles réelles.

8.2 Réponse à la problématique

La question de recherche posée en introduction interrogeait la manière de structurer un dispositif de veille qui intègre de façon cohérente et systématique les exigences de sécurité de l'information, de protection des données et de traçabilité des sources, tout en restant adapté aux contraintes opérationnelles du secteur humanitaire.

Ce travail répond à cette question en proposant non pas une simple addition de bonnes pratiques relevant de chacune de ces trois dimensions, mais un cycle opérationnel unique dans lequel chaque étape, du cadrage initial à la destruction documentée des données, porte simultanément les exigences des trois piliers. L'intégration ne se limite pas à une juxtaposition de check-lists : elle se manifeste concrètement par la fiche d'identité informationnelle, qui accompagne chaque information tout au long de son cycle de vie et matérialise à elle seule les trois dimensions de la problématique.

L'adaptation aux contraintes opérationnelles, second volet de la question de recherche, est assurée par deux mécanismes structurants : la modularité selon le niveau de maturité, qui

permet à une organisation aux ressources limitées d'adopter le modèle progressivement sans attendre de disposer de moyens technologiques avancés ; et les protocoles de décision, qui offrent un cadre de référence explicite pour les situations où la rigueur procédurale entrerait en conflit avec l'urgence de l'action, sans pour autant prétendre éliminer la part de jugement humain que ces situations requièrent.

Le modèle TRIVAH constitue ainsi une réponse argumentée et ancrée à la problématique posée, dont la validité a été établie sur le plan conceptuel. Sa validation en conditions réelles d'usage reste une étape distincte qui dépasse le périmètre de ce travail.

8.3 Contributions du travail

Au-delà de la réponse à la problématique, ce travail apporte trois contributions qui dépassent le strict cadre du modèle proposé.

L'enquête conduite, bien que limitée en taille, documente des pratiques de veille rarement rendues publiques par les organisations humanitaires elles-mêmes, pour des raisons de sensibilité légitimes. Les typologies de maturité, de risques perçus et d'obstacles structurels constituent une base de données qualitative qui pourra être réutilisée ou approfondie par des recherches ultérieures sur le même terrain.

La démarche de validation conceptuelle à trois niveaux propose une méthode reproductible pour évaluer la pertinence d'un modèle avant sa mise à l'épreuve opérationnelle. Cette approche, qui combine confrontation à des cas documentés, benchmark comparatif et mise en regard avec des données de terrain, pourrait être réutilisée pour valider d'autres propositions conceptuelles dans le champ de la gestion de l'information humanitaire.

Le modèle TRIVAH, ses protocoles de décision et sa grille d'auto-évaluation constituent des outils directement mobilisables par les praticiens du secteur, indépendamment de l'aboutissement académique de ce travail. Le profil d'entrée à coût nul, en particulier, répond à une demande explicite et documentée des organisations aux ressources les plus limitées.

8.4 Ouverture

Ce travail s'est concentré sur l'échelle de l'organisation, qui constitue le niveau auquel un dispositif de veille peut être conçu, adopté et fait évoluer de manière autonome. Mais l'enquête comme les études de cas convergent vers un constat qui dépasse ce périmètre : les crises les plus aiguës, qu'il s'agisse d'une cyberattaque ciblant une infrastructure partagée ou d'une catastrophe naturelle mobilisant plus de deux cents organisations en quelques semaines, posent des défis informationnels qui ne se résolvent pas à l'échelle d'une seule structure.

La question qui se dessine en creux de ce travail est donc celle du passage d'une logique de modèle organisationnel à une logique de gouvernance partagée : comment des organisations aux niveaux de maturité hétérogènes, suivant chacune son propre rythme d'adoption, peuvent-elles néanmoins interopérer de manière sécurisée et traçable au moment où la coordination devient vitale ? Cette question, que le modèle TRIVAH n'a pas vocation à résoudre seul, invite à poursuivre la réflexion amorcée par ce travail vers l'échelle du système humanitaire dans son ensemble, là où la sécurité de l'information, la protection des données et la fiabilité de l'information ne sont plus seulement des exigences internes à chaque organisation, mais une condition de la confiance collective sur laquelle repose, en définitive, l'efficacité de l'action humanitaire.

Bibliographie

ACAPS, [2026?]. INFORM Severity Index: track global crisis severity. ACAPS [en ligne]. [2026?]. Disponible à l'adresse : https://www.acaps.org/en/thematics/all-topics/inform-severity-index [consulté le 14 juillet 2026].

AÇIKYILDIZ, Çağlar, 2024a. 'I know you like the back of my hand': biometric practices of humanitarian organisations in international aid. *Disasters*. 1 avril 2024. Vol. 48, no 2, p. e12612. DOI 10.1111/disa.12612.

AÇIKYILDIZ, Çağlar, 2024b. Unique data, different values: explaining variation in the use of biometrics by international humanitarian organizations. *Global Policy*. 1 juin 2024. Vol. 15, no 3, pp. 502-515. DOI 10.1111/1758-5899.13343.

AMNESTY INTERNATIONAL, 2021. Rapport concernant la méthodologie technique employée pour détecter le logiciel Pegasus de NSO Group. *Amnesty International* [en ligne]. 2021. Disponible à l'adresse : https://www.amnesty.org/fr/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ [consulté le 17 mars 2026].

ARX, [2026?]. ARX – data anonymization tool. *ARX* [en ligne]. [2026?]. Disponible à l'adresse : https://arx.deidentifier.org/ [consulté le 3 juillet 2026].

BEDUSCHI, Ana, MARELLI, Massimo et MARTIN, Aaron (éd.), 2025. *Data protection in humanitarian action: responding to crises in a data-driven world*. Londres : Routledge. ISBN 978-1-003-65016-4.

BONIFACE, Pascal, 2025. Le Sud global. *IRIS* [en ligne]. 2025. Disponible à l'adresse : https://www.iris-france.org/expliquez-moi-le-sud-global/ [consulté le 2 juillet 2026].

CENTRE FOR HUMANITARIAN DATA, 2022. *Guidance note on data security in operational data management* [en ligne]. La Haye : OCHA Centre for Humanitarian Data. Disponible à l'adresse : https://centre.humdata.org/guidance-note-on-data-security-in-operational-data-management/ [consulté le 18 mai 2026].

CICR, 2020. Q&A: humanitarian operations, the spread of harmful information and data protection. In conversation with Delphine van Solinge and Massimo Marelli. *International Review of the Red Cross*. 2020. Vol. 102, no 913, pp. 27-41. DOI 10.1017/S1816383120000429.

CICR, 2022. Cyberattaque contre le CICR : le point sur ce que nous savons. *CICR* [en ligne]. 2022. Disponible à l'adresse : https://www.icrc.org/fr/document/cyberattaque-cicr-ce-que-nous-savons [consulté le 17 mars 2026].

CMMI INSTITUTE, [2026?]. CMMI. *CMMI Institute* [en ligne]. [2026?]. Disponible à l'adresse : https://cmmiinstitute.com/cmmi [consulté le 3 juillet 2026].

DACHY, Eric, 2004. L'action humanitaire : réalités et représentations. *Les Temps Modernes*. 2004. Vol. 627, no 2, pp. 22-42. DOI 10.3917/ltm.627.0022.

DAUVIN, Pascal et SIMÉANT-GERMANOS, Johanna, 2002. *Le travail humanitaire : les acteurs des ONG, du siège au terrain*. Paris : Presses de Sciences Po. DOI 10.3917/scpo.dauvi.2010.01.

DUBOST, Nathalie et DENIS, Jean-Philippe, 2020. La recherche en sciences de gestion et du management à la croisée des crises. *Revue française de gestion*. 2020. Vol. 293, no 8, pp. 13-23. DOI 10.3166/rfg.2021.00500.

GREENWOOD, Faine, 2017. *The Signal Code: a human rights approach to information during crisis*. 2017.

HAYES, Ben, 2017. Migration and data protection: doing no harm in an age of mass displacement, mass surveillance and "big data". *International Review of the Red Cross*. Avril 2017. Vol. 99, no 904, pp. 179-209. DOI 10.1017/S1816383117000637.

HUNDEPOOL, Anco et al., 2026. Handbook on Statistical Disclosure Control. *Center of Excellence SDC*. juin 2026.

IASC, 2023. *IASC operational guidance on data responsibility in humanitarian action* [en ligne]. 2e éd. Genève : Inter-Agency Standing Committee. Avril 2023. Disponible à l'adresse : https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action [consulté le 18 mai 2026].

INVID, [2026?]. InVID project – video verification. *InVID project* [en ligne]. [2026?]. Disponible à l'adresse : https://www.invid-project.eu/ [consulté le 3 juillet 2026].

IRWIN, Daniel et MANDEL, David R., 2019. Improving information evaluation for intelligence production. *Intelligence and National Security*. 2019. Vol. 34, no 4, pp. 503-525. DOI 10.1080/02684527.2019.1569343.

KOBOTOOLBOX, [2026?]. KoboToolbox [en ligne]. [2026?]. Disponible à l'adresse : https://www.kobotoolbox.org/ [consulté le 18 mai 2026].

KOOPS, Bert-Jaap, 2021. The concept of function creep. *Law, Innovation and Technology*. 2 janvier 2021. Vol. 13, no 1, pp. 29-56. DOI 10.1080/17579961.2021.1898299.

LMMS, [2026?]. LMMS Solutions [en ligne]. [2026?]. Disponible à l'adresse : https://lmms.org/ [consulté le 16 mai 2026].

MARELLI, Massimo, 2020. Hacking humanitarians: defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation. *International Review of the Red Cross*. Avril 2020. Vol. 102, no 913, pp. 367-387. DOI 10.1017/S1816383121000151.

MARELLI, Massimo, 2023. The law and practice of international organizations' interactions with personal data protection domestic regulation: at the crossroads between the international and domestic legal orders. *Computer Law & Security Review*. 1 septembre 2023. Vol. 50, p. 105849. DOI 10.1016/j.clsr.2023.105849.

MARELLI, Massimo, 2024. *Handbook on data protection in humanitarian action*. 3e éd. 19 novembre 2024.

MASUDIN, Ilyas et al., 2021. The impact of the traceability of the information systems on humanitarian logistics performance: case study of Indonesian relief logistics services. *Cogent Business & Management*. 1 janvier 2021. Vol. 8, no 1, p. 1906052. DOI 10.1080/23311975.2021.1906052.

MEIER, Patrick, 2011. Les nouvelles technologies de l'information et leur impact sur le secteur humanitaire. *Revue internationale de la Croix-Rouge*. 2011. Vol. 93.

NEUILLY, Marie-Thérèse, 2008. *Gestion et prévention de crise en situation post-catastrophe : prise en charge des traumatismes collectifs*. Louvain-la-Neuve : De Boeck Supérieur. ISBN 978-2-8041-5897-2. DOI 10.3917/dbu.neuil.2008.01.

OCHA, 2021. *Data responsibility guidelines* [en ligne]. La Haye : OCHA Centre for Humanitarian Data. Octobre 2021. Disponible à l'adresse : https://www.unocha.org/publications/report/world/data-responsibility-guidelines-october-2021 [consulté le 17 mars 2026].

OCHA, [2026?]a. Humanitarian Data Exchange. *HDX* [en ligne]. [2026?]. Disponible à l'adresse : https://data.humdata.org/ [consulté le 18 mai 2026].

OCHA, [2026?]b. Overview of data grids. *HDX* [en ligne]. [2026?]. Disponible à l'adresse : https://data.humdata.org/event/overview-of-data-grids [consulté le 18 mai 2026].

POWELL, Olivia, 2023. Ransomware gang steals 6.8TB of data from Save the Children. *Cyber Security Hub* [en ligne]. 13 septembre 2023. Disponible à l'adresse : https://www.cshub.com/attacks/news/ransomware-gang-steals-68tb-of-data-from-save-the-children [consulté le 17 mars 2026].

QRP INTERNATIONAL, [2026?]. Matrice RACI : c'est quoi et pourquoi est-elle importante ? *QRP International* [en ligne]. [2026?]. Disponible à l'adresse : https://www.qrpinternational.fr/blog/glossaire/matrice-raci-cest-quoi-et-pourquoi-est-elle-importante/ [consulté le 3 juillet 2026].

REDROSE, [2026?]. RedRose : digital solutions for humanitarian aid. RedRose [en ligne]. [2026?]. Disponible à l'adresse : https://www.redrose.io/ [consulté le 16 mai 2026].

REJALI, Saman et HEINIGER, Yannick, 2020. The role of digital technologies in humanitarian law, policy and action: charting a path forward. *International Review of the Red Cross*. Avril 2020. Vol. 102, no 913, pp. 1-22. DOI 10.1017/S1816383121000114.

REUTERS, 2024. Sudan again tops International Rescue Committee crises watchlist. *Reuters* [en ligne]. 11 décembre 2024. Disponible à l'adresse : https://www.reuters.com/world/sudan-again-tops-international-rescue-committee-crises-watchlist-2024-12-11/ [consulté le 23 février 2026].

SAAD, Sameh et al., 2023. Blockchain-based traceability system for enhanced humanitarian supply chain management. In : THOMAS, Andrew et al. (éd.), *Advances in transdisciplinary engineering*. Amsterdam : IOS Press. ISBN 978-1-64368-466-6. DOI 10.3233/ATDE230918.

SANTONI, Victor, 2022. Territoire 2.0 et information géographique involontaire : gestion des crises et réseaux sociaux numériques. *Annales de géographie*. 11 février 2022. Vol. 743, no 1, pp. 72-94. DOI 10.3917/ag.743.0072.

SEARLE, Martin, 2025. Humanitarianism and the fourth industrial revolution: saving which lives? *Journal of Asian Public Policy*. 16 juin 2025. Vol. 19, no 1, pp. 11-21.

SPHERE ASSOCIATION, 2018. *The Sphere handbook: humanitarian charter and minimum standards in humanitarian response*. 4e éd. Genève : Sphere Association. ISBN 978-1-908176-400.

TARDY, Thierry, 2009. *Gestion de crise, maintien et consolidation de la paix : acteurs, activités, défis*. Louvain-la-Neuve : De Boeck Supérieur. ISBN 978-2-8041-1639-2. DOI 10.3917/dbu.tardy.2009.01.

THE ENGINE ROOM, [2026?]. Technology tools in human rights. *The Engine Room Library* [en ligne]. [2026?]. Disponible à l'adresse : https://library.theengineroom.org/ [consulté le 18 mai 2026].

TINEYE, [2026?]. TinEye reverse image search. *TinEye* [en ligne]. [2026?]. Disponible à l'adresse : https://tineye.com/ [consulté le 3 juillet 2026].

UNDRR, 2017. Disaster risk information. *UNDRR* [en ligne]. 2017. Disponible à l'adresse : https://www.undrr.org/terminology/disaster-risk-information [consulté le 24 mars 2026].

UNHCR, 2025. Data and information management. *UNHCR Emergency Handbook* [en ligne]. 2025. Disponible à l'adresse : https://emergency.unhcr.org/coordination-and-communication/information-management/data-and-information-management [consulté le 17 mars 2026].

USHAHIDI, [2026?]. 10 years of global impact. Ushahidi [en ligne]. [2026?]. Disponible à l'adresse : https://www.ushahidi.com/in-action/10-years-of-global-impact/ [consulté le 14 juillet 2026].

Autres lectures intéressantes

53 ONG internationales, dont HI, avertissent que les récentes mesures d'enregistrement d'Israël entraveront une action humanitaire cruciale. *Handicap International* [en ligne]. Disponible à l'adresse : https://www.handicap-international.fr/fr/actualites/53-ong-internationales--dont-hi--avertissent-que-les-recentes-mesures-d-enregistrement-d-israel-entraveront-une-action-humanitaire-cruciale [consulté le 23 février 2026].

BENCHETRIT, Malik, 2023. Liste des ONG internationales. *L'Entraide Missionnaire* [en ligne]. 24 janvier 2023. Disponible à l'adresse : https://lentraidemissionnaire.org/liste-des-ong-internationales [consulté le 23 février 2026].

DONARE. Aid agencies worldwide. *DONARE* [en ligne]. Disponible à l'adresse : https://donare.info/en/aid_agencies/world [consulté le 23 février 2026].

Critique internationale, 2018. No 81 [en ligne]. ISBN 978-2-7246-3541-6. Disponible à l'adresse : https://shs.cairn.info/revue-critique-internationale-2018-4 [consulté le 17 mars 2026].

GRYSPEERDT, Axel, 1979. Les nouveaux courants de la presse francophone en Belgique après mai 1968 : la contre-information régionale/locale et sectorielle. *Courrier hebdomadaire du CRISP*. 1979. Vol. 845-846, no 20, pp. 1-40. DOI 10.3917/cris.845.0001.

IA génératives : cas d'usage et retours d'expérience, 2026. Paris : Serda édition-IDP. Archimag, Guide pratique no 83.

IHSA. Organisations directory. *IHSA* [en ligne]. Disponible à l'adresse : https://ihsa.info/directory/ [consulté le 23 février 2026].

NATIONS UNIES. Humanitarian agencies that operate in the field. *United Nations* [en ligne]. Disponible à l'adresse : https://www.un.org/es/collection/29/7832 [consulté le 23 février 2026].

OUTILS FROIDS, 2018. *Outils Froids* [en ligne]. Disponible à l'adresse : https://www.outilsfroids.net/ [consulté le 8 juin 2026].

OXFAM INTERNATIONAL. *Oxfam International* [en ligne]. Disponible à l'adresse : https://www.oxfam.org/fr [consulté le 4 mars 2026].

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE. Data protection impact assessment. *PFPDT* [en ligne]. Disponible à l'adresse : https://www.edoeb.admin.ch/en/data-protection-impact-assessment [consulté le 3 juillet 2026].

SOKEN-HUBERTY, Emmaline, 2022. 15 largest humanitarian organizations (and what they do). *Humanitarian Careers* [en ligne]. 20 septembre 2022. Disponible à l'adresse : https://humanitariancareers.com/largest-humanitarian-organizations/ [consulté le 23 février 2026].

UNDRR, 2007. Structural and non-structural measures. *UNDRR* [en ligne]. 2007. Disponible à l'adresse : https://www.undrr.org/terminology/structural-and-non-structural-measures [consulté le 24 mars 2026].

UNHCR. Registration tools. *UNHCR guidance on registration and identity management* [en ligne]. Disponible à l'adresse : https://www.unhcr.org/registration-guidance/chapter3/registration-tools/ [consulté le 16 mai 2026].

Utilisation d'outils assistés par l'intelligence artificielle

Dans le cadre de ce travail, l'auteur déclare avoir utilisé des outils assistés par l'intelligence artificielle aux fins suivantes :

Améliorations formelles (orthographe, syntaxe, reformulation, structure du rapport)

Aide à la correction à l'aide de Claude et de ChatGPT.

Réflexions de fond (production d'analyses, de recommandations)

Aide à la réflexion aux pages 40 à 49, à l'aide de Claude et de NotebookLM.

Création de tableaux

L'architecture du tableau de l'annexe 5 a été élaborée à l'aide de Claude.

Mise en page de la Figure 1

Modifications de design

Le design du guide de recommandation (annexe 6) a été réalisé à l'aide de Claude.

Annexe 1 : Questionnaire

Bachelor thesis

This survey is part of a bachelor's thesis required for the Bachelor of Science HES-SO in Information Science at the Geneva Haute école de Gestion (HEG).

Information Science studies train experts to manage the entire information lifecycle, from knowledge organization and strategic intelligence to data governance and cybersecurity. In an increasingly data-driven world, this discipline ensures that information serves as a reliable, ethical, and secure lever for decision-making.

Supervised by Ms. Stéphanie Haesen, this research project, entitled "How to structure a monitoring system conducted by humanitarian organizations that consistently and systematically integrates information security, data protection, and source traceability requirements," addresses a significant gap in current literature.

While intelligence and monitoring are vital for humanitarian responsiveness, they currently face major challenges: disinformation, cyberthreats, and the risks associated with the exploitation of sensitive data. This thesis aims to move beyond fragmented approaches to propose an integrated conceptual model that balances operational efficiency with strict protection imperatives.

By participating in this survey, you are contributing to the empirical phase of this research. Your insights will help establish a precise diagnostic of current sector practices, leading to the formulation of concrete recommendations to enhance the security and reliability of humanitarian information.

This survey will end on May 31, 2026.

As part of this survey, do you authorize the following:

☐ The use of your answers in anonymized form for academic analysis.

☐ The inclusion of anonymized excerpts from your answers in the thesis.

☐ The storage of the data collected for the duration of the research project.

A confidentiality framework is applied to all collected data:

- No identifying element of your organization or of individuals will appear in the final document without your explicit consent.

- The data will be used exclusively within the framework of this research work.

Profile of the organization

1. Name of the organization *

_____

2. Approximate size of the organization is *

Une seule réponse possible.

- ○ < 50 employees
- ○ 50-250 employees
- ○ 250-1000 employees
- ○ > 1000 employees

3. Type of organization *

Plusieurs réponses possibles.

- ☐ International NGO
- ☐ Intergovernmental organization
- ☐ International movement (e.g. International Committee of the Red Cross)
- ☐ Autre :

4. Field of activity of the organization *

_____

5. Your role within the organization *

_____

6. Is there a unit dedicated to monitoring or information management in your structure? *

Une seule réponse possible.

- ○ Yes
- ○ No

7. Do you have a formalized information management service? *

Une seule réponse possible.

- ○ Yes, at the level of the whole organization
- ○ Yes, but limited to certain programs or regions
- ○ No

8. Do you have a formalized monitoring service? *

Une seule réponse possible.

- ○ Yes, at the level of the whole organization
- ○ Yes, but limited to certain programmes or regions
- ○ No, monitoring is conducted on an ad hoc basis
- ○ No, no structured monitoring

Governance of monitoring

9. Does your monitoring system explicitly rely on standards (Sphere, OCHA principles, GDPR, internal data protection manual)? If yes, please specify the type in "other".

Une seule réponse possible.

- ○ No
- ○ Autre :

10. Is there a formalized information governance framework? If yes, please specify the type in "other".

Une seule réponse possible.

- ○ No
- ○ Autre :

11. At which level is monitoring steered?

Une seule réponse possible.

- ○ Headquarters
- ○ Regional
- ○ Field
- ○ Mixed

12. What are the main purposes of your monitoring (several answers possible)

Plusieurs réponses possibles.

- ☐ Contextual and security analysis
- ☐ Crisis anticipation / early warning
- ☐ Staff security
- ☐ Support to operational decision-making
- ☐ Support to strategic decision-making
- ☐ Advocacy and public communication

☐ Fundraising / donor relations

☐ Risk management and compliance

☐ Autre :

13. Is monitoring integrated into decision-making processes?

Une seule réponse possible.

○ Systematically

○ Partially

○ On an ad hoc basis

14. "Do No Harm" ethics: Is there a formal reflection on the risk that your monitoring could pose to information sources in the field?

Une seule réponse possible.

○ Yes

○ No

15. On which geographical scopes are monitoring conducted?

Plusieurs réponses possibles.

☐ International

☐ Regional

☐ National

☐ Specific areas

☐ Autre :

Monitoring methodology

16. What types of monitoring do you practice?

Plusieurs réponses possibles.

☐ Security monitoring

☐ Contextual/political monitoring

☐ Media monitoring

☐ Health monitoring

☐ Digital monitoring (social networks)

☐ Diplomatic monitoring

☐ Legal monitoring

☐ Donor monitoring

☐ Autre :

17. Do you classify your sources according to a level of reliability?

Une seule réponse possible.

○ Yes (formalized grid)

○ Yes (informal assessment)

○ No

18. Do you have a traceability system documenting:

Une seule réponse possible par ligne.

	Yes	**No**
The precise origin of the information	○	○
The conditions of production	○	○
The verification steps	○	○
The modifications made	○	○

19. Do you use an evaluation method such as:

Plusieurs réponses possibles.

☐ Source/content grid (evaluation criteria or rating scale used to analyse the reliability of the source and the credibility of the content)

☐ OSINT method (set of techniques used to collect, cross-check and verify information from open sources)

☐ Double validation (information is confirmed by at least two independent sources or by two different people before being considered reliable)

☐ Autre :

20. How do you select the sources to be included in monitoring (whitelists/blacklists, internal recommendations, validation by a manager, etc.)?

21. Do you use explicit criteria to assess the credibility of sources?

Plusieurs réponses possibles.

☐ Yes, reputation

☐ Yes, expertise

☐ Yes, independence

☐ Yes, track record

☐ No

☐ Autre :

22. How often is information updated?

Une seule réponse possible.

1: Several times a day

2: Every day

3: Every week

4: Every two weeks

5: Every month

6: Rarely

23. Is there a formalized process for validating information before internal dissemination? If yes, please specify the type in "other".

Plusieurs réponses possibles.

☐ No

☐ Autre :

Tools and resources

24. Do you have a centralized document management system? If yes, please specify the type in "other".

Une seule réponse possible.

○ No

○ Autre :

25. The tools used are:

Plusieurs réponses possibles.

☐ Internal

☐ Open source

☐ Private providers

☐ On premise solutions

26. Which tools do you use?

Plusieurs réponses possibles.

☐ Feed aggregators

☐ Social listening tools

☐ Data analysis platforms

☐ Spreadsheets

☐ Collaborative tools

☐ Mapping tools

☐ Autre :

27. Please specify the tool's name

_____

28. Have the people in charge of monitoring received specific training in information management, cybersecurity or monitoring?

Plusieurs réponses possibles.

☐ Master/Bachelor

☐ External training

☐ Internal training

☐ No training

☐ Autre :

29. Is any monitoring automated? If yes, to what proportion compared with human processing?

_____

30. What types of sources of social networks are used?

Plusieurs réponses possibles.

☐ Facebook

☐ X

☐ Instagram

☐ TikTok

☐ YouTube

☐ LinkedIn

☐ Not used

☐ Autre :

31. What types of sources of media are used?

Plusieurs réponses possibles.

☐ International print press

☐ Regional print press

☐ International news agencies

☐ Continuous news channels

☐ Not used

☐ Autre :

32. Please specify the media's name

_____

33. What other types of sources are used?

Plusieurs réponses possibles.

☐ Internal reports

☐ Satellite sources

☐ Institutional sources

☐ Government or NGO sources

☐ Informants in the field

☐ Specialized databases

☐ Autre :

34. Have you already encountered difficulties related to:

Plusieurs réponses possibles.

☐ Disinformation

☐ Data manipulation

☐ Unverifiable sources

☐ Loss of traceability

☐ Autre :

35. Do budget constraints influence your technological choices

Une seule réponse possible.

○ Yes

○ No

Information security

36. Do you use a system for classifying the sensitivity of data? If yes, please specify the type in "other".

Une seule réponse possible.

○ No

○ Autre :

37. Are the data collected during monitoring encrypted?

Une seule réponse possible.

○ Yes

○ No

38. What is the means of data storage?

Une seule réponse possible.

○ Sovereign cloud

○ Internal servers

○ Third party tools such as Google/Microsoft

○ Autre :

39. How do you manage monitoring information that could indirectly identify vulnerable populations (GPS coordinates, ethnic/religious affiliations)?

_____

40. In your view, what is the main risk linked to your monitoring activity?

Une seule réponse possible.

- ○ Data leakage
- ○ Hacking of the system
- ○ Surveillance by third party actors

41. Do you have a formalized information security policy?

Une seule réponse possible.

- ○ Yes
- ○ No

42. Monitoring flows are:

Une seule réponse possible.

- ○ Encrypted
- ○ Hosted on secure servers
- ○ Stored locally
- ○ Cloud hosted
- ○ Autre :

43. Access to monitoring information is:

Une seule réponse possible.

- ○ Hierarchized
- ○ Restricted by role
- ○ Open internally

44. Have you already experienced:

Plusieurs réponses possibles.

- ☐ Cyberattack
- ☐ Information leakage
- ☐ Attempted intrusion

45. Is there an information crisis management plan?

Une seule réponse possible.

- ○ Yes
- ○ No

Data protection

46. Do you collect personal data in your monitoring activities? If yes, please specify the type in "other" (ex. beneficiaries, staff, partners, local authorities, etc.)

Une seule réponse possible.

- ○ No
- ○ Autre :

47. Do you have a data protection framework inspired by:

Plusieurs réponses possibles.

- ☐ GDPR
- ☐ Internal policy
- ☐ Institutional guidelines
- ☐ No formal framework

48. How do you minimize the risks linked to sensitive data?

_____

49. Are teams trained in data protection?

Une seule réponse possible.

- ○ Yes
- ○ No

Disinformation and risk management

50. Have you already been confronted with attempts at information manipulation (fake news) specifically targeting your organization or your areas of intervention? If yes, how did the monitoring system detect it?

_____

51. Does disinformation constitute a major risk in your intervention context?

Une seule réponse possible.

- ○ Yes
- ○ No

52. Do you have a specific protocol for verifying sensitive information?

Une seule réponse possible.

- ○ Yes
- ○ No

53. How do you manage local rumours?

_____

54. Has any of your decisions ever been influenced by information? If yes, why?

_____

55. Do you systematically document each piece of information:

Une seule réponse possible par ligne.

	Yes	**No**
The exact origin (primary vs secondary source)	○	○
The date/time of collection	○	○
The channel (email, platform, report, social network, interview, etc.)	○	○
The level of confidence assigned	○	○

56. How is this traceability technically guaranteed?

Plusieurs réponses possibles.

☐ Metadata

☐ Mandatory fields

☐ Automatic logging

☐ Autre :

Limits and perspectives

57. What are the main obstacles to more secure and better-tracked monitoring in your organization?

Plusieurs réponses possibles.

☐ Lack of budget

☐ Lack of technical skills

☐ Operational urgency taking precedence over procedure

☐ Autre :

58. Have you recently introduced new technologies or approaches to monitoring? If yes, which?

Plusieurs réponses possibles.

☐ AI

☐ NLP

☐ Automated collection

☐ Interactive dashboards

☐ No

☐ Autre :

59. What benefits and risks do you identify in these innovations (quality, bias, security, confidentiality)?

_____

60. How do you assess the overall maturity of your monitoring system with regard to:

Une seule réponse possible par ligne.

	very low	low	medium	high	very high
Methodology and processes	○	○	○	○	○
Information security	○	○	○	○	○
Data protection	○	○	○	○	○
Traceability and quality of sources	○	○	○	○	○
Integration of ethics and values	○	○	○	○	○

61. In your view, what are the main needs for improvement or external support to strengthen your monitoring system?

Plusieurs réponses possibles.

☐ Methodological clarification

☐ Tooling

☐ Human resources

☐ Training

☐ Legal/ethical support

☐ Autre :

62. Which aspects would require priority improvement?

_____

63. Would you be in favour of an integrated model combining monitoring, security and data protection? *

Une seule réponse possible.

○ Yes

○ No

64. What elements should imperatively be included in such a model? *

_____

65. What recommendations would you make to actors wishing to propose a conceptual monitoring model integrating information security, data protection and source traceability, adapted to the humanitarian sector? *

_____

66. Would you like to receive a summary of the results of this research? *

Une seule réponse possible.

○ Yes

○ No

Annexe 2 : Guide d'enquête

Code	Type	Méthode de contact	Réponse reçue	Raison	Relance effectuée	Questionnaire rempli	Entretien proposé	Entretien réalisé
1	ONG internationale	LinkedIn, e-mail, formulaire	Oui	A commencé à répondre puis a abandonné en cours de route, jugeant le questionnaire trop long et trop généraliste pour une seule personne : dans une grande structure, les questions touchent à plusieurs domaines de spécialité (IT, sécurité, communication) qui relèveraient normalement de répondants différents. Suggère un découpage du questionnaire par profil professionnel et une indication de durée estimée.	Oui	Non	Non	Non
2	ONG internationale	E-mail	Oui	Remerciements pour la démarche, mais l'organisation indique ne pas être en mesure de donner suite à la demande, sans préciser de motif.	Non	Non	Non	Non
3	Réseau professionnel	E-mail	Oui	A orienté vers d'autres contacts potentiellement pertinents.	Oui	Non	Non	Non
4	Réseau de coordination	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
5	Réseau d'apprentissage	LinkedIn, e-mail	Non	Plusieurs relances envoyées sans retour.	Oui	Non	Non	Non
6	ONG internationale confessionnelle	E-mail	Oui		Oui	Oui	Oui	Non
7	ONG internationale	E-mail	Non	Plusieurs relances envoyées sans retour.	Oui	Non	Non	Non

8	ONG internationale confessionnelle	E-mail	Oui	Aucune réponse obtenue.	Non	Non	Oui	Non
9	Service gouvernemental	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
10	ONG internationale	E-mail	Oui		Non	Oui	Oui	Non
11	Fondation	E-mail	Oui	Intérêt exprimé pour la thématique, mais précise être un bailleur non opérationnel : le suivi de contexte se fait à un niveau macro à partir de sources déjà publiques et fiables (agences onusiennes, grands médias, rapports des ONG financées). En conséquence, juge que sa contribution au questionnaire serait peu pertinente au regard du périmètre visé.	Oui	Non	Oui	Non
12	Réseau humanitaire	E-mail	Non	Aucune réponse obtenue.	Oui	Non	Non	Non
13	Groupe de coordination	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
14	Mouvement national	Formulaire	Non	Aucune réponse obtenue.	Non	Non	Non	Non
15	Organisation spécialisée en cybersécurité humanitaire	E-mail	Oui	Remerciements pour la prise de contact, mais l'organisation indique ne pas être en mesure de soutenir la demande actuellement, en raison de ressources limitées.	Oui	Non	Non	Non
16	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
17	ONG suisse	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
18	Agence onusienne	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non

19	Dispositif de coordination internationale	Formulaire	Oui		Oui	Oui	Oui	Non
20	Réseau interagences	E-mail	Non	Aucune réponse obtenue.	Oui	Non	Non	Non
21	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Oui	Non	Non	Non
22	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
23	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
24	ONG suisse	E-mail	Oui	Réponse de type accusé de réception automatisé (gestion de changement d'adresse), sans rapport direct avec la demande formulée — probable réponse standard d'un service donateurs.	Oui	Non	Non	Non
25	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
26	ONG internationale confessionnelle	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
27	ONG internationale	E-mail	Oui	Remerciements pour l'intérêt porté à l'organisation, mais indique ne pas être en mesure de répondre à la demande en raison de contraintes de temps et de priorités internes.	Oui	Non	Non	Non
28	Mouvement international	E-mail	Oui		Oui	Oui	Oui	Non
29	ONG internationale médicale et humanitaire	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non

30	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
31	ONG internationale confessionnelle	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
32	ONG internationale	E-mail	Oui	Réponse négative motivée par une charge de travail exceptionnelle liée au contexte de plusieurs conflits en cours, rendant la disponibilité insuffisante pour contribuer à la demande dans l'immédiat.	Oui	Non	Non	Non
33	ONG internationale	E-mail	Oui	Réponse négative motivée par l'absence, au sein de l'organisation, d'un profil interne correspondant au périmètre de la demande ; excuses présentées pour le délai de réponse.	Oui	Non	Non	Non
34	ONG internationale	LinkedIn	Oui		Oui	Oui	Oui	Oui
35	ONG internationale	LinkedIn, e-mail	Non	Aucune réponse obtenue.	Oui	Non	Non	Non
36	ONG suisse	Formulaire	Oui		Oui	Oui	Oui	Non
37	Agence onusienne	E-mail	Oui		Oui	Non	Non	Non
38	Agence onusienne	E-mail	Oui		Oui	Oui	Oui	Oui
39	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
40	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non

41	ONG internationale confessionnelle	Formulaire	Oui	Remerciements pour l'intérêt porté à l'organisation, mais indique ne pas pouvoir participer à des études de recherche externes, faute de garantie sur l'usage et la publication des résultats.	Oui	Non	Non	Non
42	ONG internationale	E-mail	Oui	Réponse négative motivée par un volume très élevé de demandes similaires reçues, ne permettant pas d'y répondre toutes ; renvoi vers les rapports publics de l'organisation pour les informations générales.	Oui	Non	Non	Non
43	ONG suisse	E-mail	Oui		Oui	Oui	Oui	Oui
44	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
45	ONG suisse	E-mail	Oui	Intérêt exprimé pour la thématique ; demande de précisions sur les profils internes les plus pertinents pour répondre au questionnaire et sur la langue de celui-ci, suite à un retard de réponse dû à un classement automatique en courrier indésirable.	Oui	Non	Non	Non
46	Agence onusienne	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
47	Agence onusienne	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
48	Agence onusienne	Formulaire	Non	Aucune réponse obtenue.	Non	Non	Non	Non
49	Réseau humanitaire en Europe	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
50	Agence onusienne	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non

51	Agence onusienne	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non
52	ONG internationale	E-mail	Non	Aucune réponse obtenue.	Non	Non	Non	Non

Annexe 3 : Guide d'entretien

Préambule oral (à formuler en début d'entretien) : présentation du travail de bachelor et de son objectif, rappel du caractère anonyme du traitement des données, confirmation de l'accord pour l'enregistrement, et précision que l'entretien vise à approfondir certains résultats du questionnaire ainsi qu'à recueillir un avis sur les pistes d'évolution envisagées pour le secteur.

Le but de la veille au sein de l'organisation

Objectif : situer la place et la finalité de la veille informationnelle dans l'organisation, au-delà des catégories fermées du questionnaire, et comprendre comment elle s'organise avec la mission opérationnelle de la structure.

Question : pouvez-vous me décrire, dans vos mots, à quoi sert la veille informationnelle dans votre organisation ? Quel problème concret est-elle censée résoudre ?

Les outils

Objectif : recueillir une description concrète et qualitative des outils utilisés, de leur articulation entre eux, et des critères qui ont guidé leur choix.

Question : quels outils utilisez-vous au quotidien pour la veille ? Comment s'articulent-ils entre eux ?

Les limites des pratiques de veille actuelles

Objectif : faire émerger, les difficultés concrètes vécues sur le terrain, notamment celles qui touchent à la sécurité, à la traçabilité ou à la fiabilité des sources.

Question : quelles sont, selon vous, les principales limites de la façon dont la veille est actuellement pratiquée chez vous ?

Les manques

Objectif : identifier, du point de vue du praticien, ce qui manque structurellement pour distinguer les manques perçus comme prioritaires de ceux qui sont secondaires.

Question : si vous deviez nommer un seul manque prioritaire dans votre dispositif actuel de veille, lequel serait-ce ?

Le système idéal

Objectif : sortir du cadre contraint des pratiques actuelles pour recueillir une vision prospective, sans souci de faisabilité immédiate.

Question : si vous aviez une baguette magique et pouviez concevoir le système de veille idéal pour votre organisation, sans aucune contrainte de budget ou de technique, à quoi ressemblerait-il ?

Annexe 4 : Matrices d'analyse

Correspondance des codes

Code	Type d'organisation	Taille	Code thèse
A	ONG internationale	< 50 employés	Org. A
B	H2H	< 50 employés	Org. B
C	Organisation intergouvernementale	> 1000 employés	Org. C
D	ONG internationale	> 1000 employés	Org. D
E(1)	Mouvement international (répondant 1)	> 1000 employés	Org. E (r.1)
E(2)	Mouvement international (répondant 2)	> 1000 employés	Org. E (r.2)
F	ONG internationale	> 1000 employés	Org. F
G	ONG internationale	50-250 employés	Org. G
H	ONG internationale	50-250 employés	Org. H

Gouvernance informationnelle

Question	A	B	C	D	E(1)	E(2)	F	G	H
Unité dédiée au monitoring	Non	Non	Oui	Non	Oui	Oui	Oui	Oui	Non
Service information management formalisé	Oui	Oui	Oui	Non	Oui	Non	Oui	Oui	Partiel
Service de monitoring formalisé	Oui	Oui	Oui	Non	Oui	Oui	Partiel	Oui	Partiel

Question	A	B	C	D	E(1)	E(2)	F	G	H
S'appuie sur des standards externes	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Non
Cadre de gouvernance formalisé	Non	Oui	Oui	Non	Non	Non	Non	Non	Non
Monitoring intégré aux décisions	Partiel			Partiel	Partiel	Partiel	Partiel	Partiel	Partiel
Réflexion *Do No Harm* formelle	Oui	Oui		Oui	Oui	Non	Non	Oui	Non
Plan de gestion de crise info.	Non	Oui		Oui	Oui	Oui	Oui	Oui	Non

Traçabilité des sources

Question	A	B	C	D	E(1)	E(2)	F	G	H
Classement des sources par fiabilité	Non	Oui		Oui	Oui	Oui	Non	Oui	Non
Traçabilité : origine précise	Oui	Oui		Oui	Non	Non	Non	Non	Non
Traçabilité : conditions de production	Oui	Oui			Oui	Non	Non	Oui	Non
Traçabilité : étapes de vérification	Oui	Oui			Non	Non	Non	Non	Non

Question	A	B	C	D	E(1)	E(2)	F	G	H
Traçabilité : modifications apportées	Oui	Oui		Oui	Non	Non	Non	Oui	Non
Doc. syst. : origine exacte	Oui	Oui		Oui	Oui	Oui	Non		Non
Doc. syst. : date/heure collecte	Oui	Oui		Oui	Non	Oui	Oui		Non
Doc. syst. : canal utilisé	Non	Oui			Non	Oui	Oui		Non
Doc. syst. : niveau de confiance	Non	Oui		Oui	Non	Oui	Non		Non
Processus formalisé de validation	Non	Oui		Non	Non	Non	Non	Oui	Non

Sécurité de l'information

Question	A	B	C	D	E(1)	E(2)	F	G	H
Politique de sécurité formalisée	Non	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
Données chiffrées	Non	Non		Non	Non	Non	Oui	Non	Non
Système de classification de sensibilité	Non	Oui	Oui	Non	Partiel	Non	Oui	Partiel	Non

Question	A	B	C	D	E(1)	E(2)	F	G	H
Accès restreint par rôle	Non			Oui	Oui	Oui	Oui	Oui	Oui
Stockage : outils tiers commerciaux	Oui	Oui		Oui	Oui		Oui	Partiel	Oui
Contraintes budgétaires influent les choix	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Incident de sécurité déjà vécu	Non	Oui		Non	Oui	Non	Non	Oui	Non

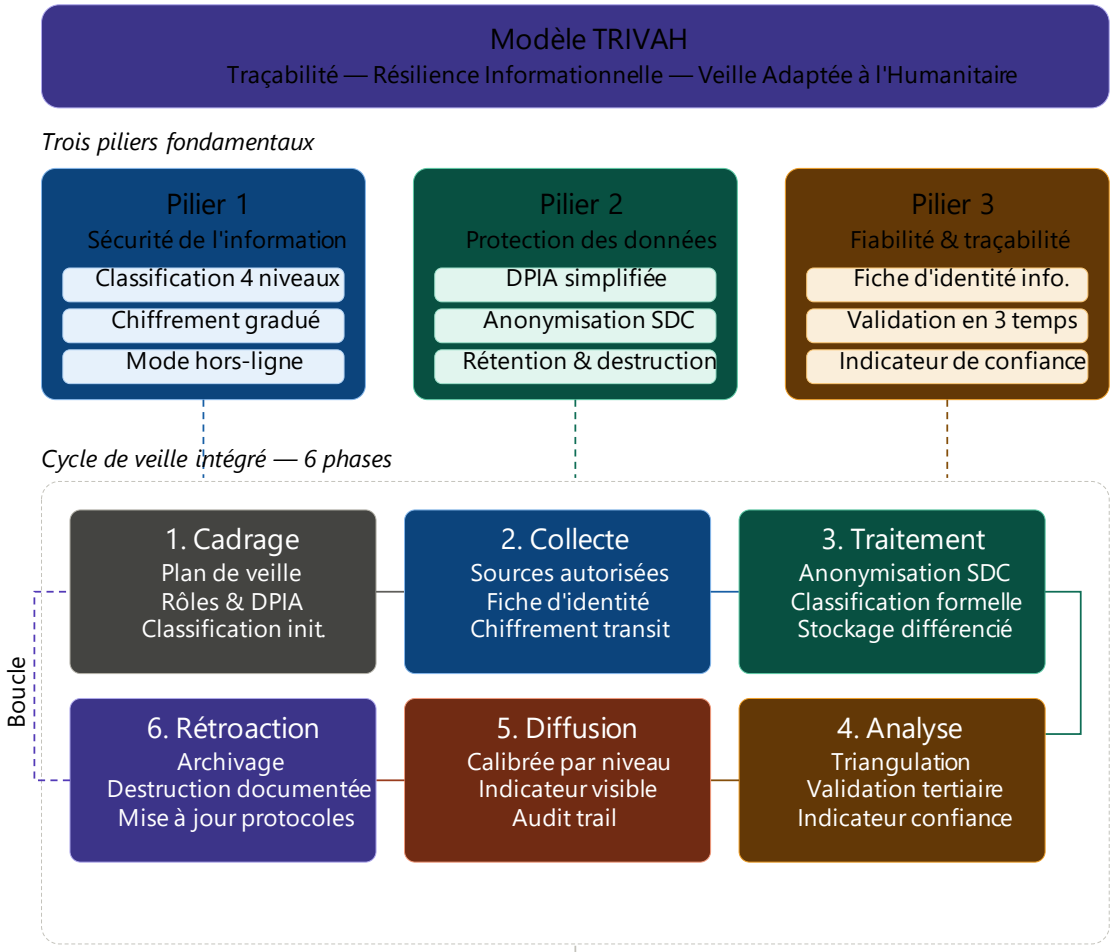
Protection des données et éthique

Question	A	B	C	D	E(1)	E(2)	F	G	H
Collecte de données personnelles	Oui	Oui		Non	Oui	Oui	Oui	Oui	Oui
Équipes formées à la protection des données	Non	Oui	Non	Oui	Oui		Oui	Oui	Non
Désinformation = risque majeur perçu	Oui			Oui	Oui	Oui	Non	Oui	Non
Protocole de vérification info. sensible	Non			Oui	Oui	Non	Non		Non
Déjà confronté à des fake news visant l'org.	Non	Oui		Oui	Oui		Non	Oui	

Maturité auto-évaluée (5 dimensions)

Question	A	B	C	D	E(1)	E(2)	F	G	H
Méthodologie et processus	Moyen	Très élevé		Moyen	Élevé	Moyen	Moyen		Faible
Sécurité de l'information	Élevé	Élevé		Moyen	Moyen	Élevé	Élevé		Faible
Protection des données	Moyen	Élevé		Élevé	Moyen		Élevé		Faible
Traçabilité et qualité des sources	Moyen	Très élevé		Moyen	Moyen		Moyen		Faible
Intégration de l'éthique et des valeurs	Très élevé	Élevé		Élevé	Élevé	Élevé	Moyen		Faible

Annexe 5 : Schémas du modèle proposé



Protocoles de décision — 4 tensions gérées

Urgence vitale vs. Protection
→ Base légale intérêt vital
→ Partage minimal + destruction programmée

Rapidité vs. Vérification
→ Diffusion progressive « non vérifié »
→ Mise à jour indicateur au fil des validations

Traçabilité vs. Protection des sources
→ Traçabilité à couches (identité séparée)
→ Accès DPO uniquement sur demande

Interopérabilité vs. Souveraineté
→ Niv. 1–2 partagés ; niv. 3–4 agrégés
→ Analyse de risque juridictionnel documentée

Grille d'auto-évaluation — 5 niveaux de maturité

Niveau	Description	Sécurité	Protection	Traçabilité
1 — Initial	Pratiques ad hoc, non documentées	Aucun chiffrement	Pas de DPIA	Aucune fiche
2 — Reprod.	Répétées mais non formalisées	Partiel	Ponctuelle	Informelle
3 — Défini	Processus documentés, formation existante	MFA actif	DPIA systématique	Fiche appliquée
4 — Géré	Mesures de performance, amélioration continue	Audit log	Droits actifs	Triangulation syst.
5 — Optimisé	Innovation continue, benchmark externe	Mode hors-ligne	Privacy by design	OSINT formel

Annexe 6 : Guide de recommandation

h e g

Haute école de gestion
Genève

GUIDE PRATIQUE

Recommandation des outils de veille

en organisme humanitaire

Choisir ses outils, sécuriser l'information et structurer sa veille, quel que soit son point de départ.

Sécurité	Protection	Traçabilité

Charlotte Chuard

Haute École de Gestion de Genève, Travail de Bachelor en Information Science

Juillet 2026

Liste des acronymes

Les acronymes ci-dessous sont utilisés dans ce guide et dans le travail de bachelor qui en constitue la base scientifique.

Acronyme	Définition
ACAPS	Assessment Capacities Project, organisation d'analyse indépendante des crises humanitaires
ACLED	Armed Conflict Location and Event Data Project, base de données sur les conflits armés
BI	Business Intelligence, outils et méthodes d'analyse et de visualisation des données
BIMS	Biometric Identity Management System, système de gestion des identités biométriques du HCR
CATI	Computer-Assisted Telephone Interviewing, méthode de collecte de données par téléphone
CHS	Core Humanitarian Standard, standard de responsabilité et de qualité humanitaire
CICR	Comité International de la Croix-Rouge
CMMI	Capability Maturity Model Integration, modèle de maturité des capacités organisationnelles
DPO	Délégué à la Protection des données (Data Protection Officer)
DPIA	Data Protection Impact Assessment, analyse d'impact relative à la protection des données
FEWS Net	Famine Early Warning Systems Network, réseau d'alerte précoce à la famine
GDACS	Global Disaster Alert and Coordination System, système mondial d'alerte en cas de catastrophe
GPS	Global Positioning System, système de positionnement par satellite
HCR / UNHCR	Haut-Commissariat des Nations Unies pour les Réfugiés

Acronyme	Définition
HDX	Humanitarian Data Exchange, plateforme de partage de données humanitaires d'OCHA
HXL	Humanitarian Exchange Language, standard de balisage sémantique pour les données humanitaires
IFRC	International Federation of Red Cross and Red Crescent Societies, Fédération internationale de la Croix-Rouge
INFORM	Index for Risk Management, indice de mesure des risques humanitaires et de catastrophe
IRC	International Rescue Committee, organisation internationale d'aide aux réfugiés
IT	Information Technology, technologies de l'information
IVR	Interactive Voice Response, système de réponse vocale interactive pour la collecte de données
MFA	Multi-Factor Authentication, authentification à plusieurs facteurs
NLP	Natural Language Processing, traitement automatique du langage naturel
OCHA	Office for the Coordination of Humanitarian Affairs, Bureau de la coordination des affaires humanitaires de l'ONU
ODK	Open Data Kit, ensemble d'outils open source pour la collecte de données terrain
ONG	Organisation Non Gouvernementale
OSINT	Open Source Intelligence, renseignement fondé sur des sources ouvertes
PAM / WFP	Programme Alimentaire Mondial (World Food Programme)
RGPD	Règlement Général sur la Protection des Données
RSS	Really Simple Syndication, format de flux de syndication web
RSSI	Responsable de la Sécurité des Systèmes d'Information
SCOPE	Système de gestion des bénéficiaires du Programme Alimentaire Mondial

Acronyme	Définition
SDC	Statistical Disclosure Control, méthodes statistiques d'anonymisation
SLA	Service Level Agreement, accord de niveau de service entre un prestataire et son client
TRIVAH	Traçabilité, Résilience Informationnelle, Veille Adaptée à l'Humanitaire, modèle conceptuel développé dans ce travail
UNOSAT	United Nations Satellite Centre, centre satellitaire des Nations Unies

1. Préambule

Ce guide s'adresse à toute personne travaillant au sein d'une organisation humanitaire, ONG ou structure de développement qui souhaite structurer ou améliorer son dispositif de veille informationnelle. Il a été conçu pour être utile quelle que soit votre situation de départ : que vous débutiez avec un simple tableur, que vous ayez déjà des pratiques informelles à consolider, ou que vous cherchiez à formaliser un système existant.

Il est pertinent pour vous si vous vous reconnaissez dans l'une de ces situations :

- Vous suivez l'actualité de vos zones d'intervention de manière informelle, sans processus clair, et vous souhaitez structurer cette pratique.
- Vous avez des outils en place mais ne savez pas si vos informations sont suffisamment sécurisées et traçables.
- Vous devez convaincre votre direction d'investir (du temps ou du budget) dans la veille, et avez besoin d'arguments concrets.
- Vous êtes en charge de la sécurité, de la gestion documentaire ou de la qualité de l'information au sein de votre organisation.
- Vous cherchez à choisir entre plusieurs outils disponibles sur le marché et voulez un guide de lecture neutre.

Sur quoi repose ce guide. Les recommandations et les outils présentés ont été identifiés en croisant trois sources : la revue de la littérature et le benchmark des dispositifs de référence du secteur (OCHA HDX, ACAPS CrisisInSight, CICR, IFRC Data Playbook), une enquête menée en 2026 auprès de neuf professionnels de la veille dans huit organisations, et des entretiens qualitatifs. Les pourcentages cités (pratiques observées, fréquences) proviennent de l'enquête ; les choix d'outils, eux, résultent de l'ensemble de ces sources.

2. Choisir ses outils

- **Comment lire ce tableau et choisir votre outil**

Trois questions vous guident dans le choix. Lisez-les avant de parcourir le tableau : elles vous éviteront de comparer des outils qui ne répondent pas au même besoin.

1. Quel est votre besoin prioritaire ? Collecte d'information, stockage sécurisé, analyse ou diffusion ? Les outils ne couvrent pas tous les mêmes fonctions ; il en faut souvent plusieurs, coordonnés.

2. Quelles sont vos ressources réelles ? Budget mensuel, compétences techniques disponibles, temps de maintenance. Un outil gratuit bien utilisé vaut toujours mieux qu'un outil coûteux sous-utilisé.

3. Quel niveau de sensibilité pour vos données ? Les outils de stockage cloud commercial (SharePoint, Drive) sont acceptables pour les niveaux 1 et 2 de sensibilité, mais pas pour les niveaux 3 et 4. La grille de classification des niveaux figure au chapitre 3 (Tableau 2).

Légende des capacités : ✓✓✓ excellence · ✓ suffisant · ~ limité · ✗ absent. Col. = capacité de collecte · Ana. = capacité d'analyse.

Tableau 1 — Outils de veille, du plus simple au plus avancé

Catégorie	Exemples	Coût*	Profil adapté	Collecte	Analyse	Lien	Points de vigilance
Alertes automatiques	Google Alerts	Gratuit	Toute taille, débutant	✓	✗	google.com/alerts	Biais algorithmique ; aucune traçabilité ; pas de contrôle sur les sources
Agrégateurs de flux RSS	Feedly, KB Crawl	Gratuit → abon.	Petite à interm.	✓✓	~	feedly.com	Dépendance à l'éditeur ; biais de sélection ; volumétrie à gérer
Social listening pro	Sprinklr, Hootsuite, Brandwatch	Élevé (abon. annuel)	Grande org.	✓✓✓	✓✓	sprinklr.com	Coût prohibitif pour petites structures ; données parfois hébergées hors UE
Réseaux sociaux (sources directes)	Facebook, LinkedIn, X, YouTube	Gratuit	Toute taille	✓	✗	—	Désinformation ; biais de représentation ; aucune traçabilité native
Stockage cloud (suite bureautique)	SharePoint, OneDrive, Google Drive	Inclus abon.	Toute taille	~	~	microsoft.com / google.com	Souveraineté des données ; juridiction non-UE ; chiffrement partiel

Catégorie	Exemples	Coût*	Profil adapté	Collecte	Analyse	Lien	Points de vigilance
Gestion documentaire (ONG)	NGO Online, M-Files	Abon. Sectoriel	Interm. +	~	~	m-files.com	Moins répandu ; courbe d'apprentissage ; coût à négocier
Base de données relationnelle	PostgreSQL, Airtable	Gratuit / freemium	Grande org. (tech.)	✓	✓	postgresql.org / airtable.com	Compétences techniques internes ou prestataire requis
Business Intelligence	Power BI, Tableau, Metabase	Abon. / standalone	Interm. +	✗	✓✓✓	powerbi.microsoft.com / metabase.com	Compétences requises ; peu utile sans données structurées en amont
Analyse de réseaux	Gephi, NodeXL	Gratuit	Avancé (spécialiste)	✗	✓✓	gephi.org	Courbe d'apprentissage ; données d'entrée structurées nécessaires
Intelligence artificielle / NLP	ChatGPT, Claude, NLP Python	Freemium → élevé	Avancé (encadré)	✓	✓✓	claude.ai / openai.com	Biais algorithmiques ; traçabilité des sorties ; confidentialité ; hallucinations

Catégorie	Exemples	Coût*	Profil adapté	Collecte	Analyse	Lien	Points de vigilance
Tableurs	Excel, Google Sheets	Inclus suite	Toute taille	✓	~	—	Pas de traçabilité native ; erreurs humaines ; pas de versionnage auto.
Formulaires de collecte terrain	KoBoToolbox, ONA, ODK	Gratuit ONG	Toute taille	✓✓✓	~	kobotoolbox.org	Nécessite connectivité pour synchro ; paramétrer le mode hors ligne
Cartographie participative	Ushahidi, OpenStreetMap, HDX	Gratuit / open source	Toute taille	✓✓	✓	ushahidi.com / openstreetmap.org	Localisation sensible ; agrégation géographique obligatoire avant partage
Imagerie satellitaire	UNOSAT, Planet Labs	Gratuit (UNOSAT) → abon.	Grandes org.	✓✓	✓	unosat.org	Localisation précise ; risque de ré-identification élevé ; protocoles stricts
Vérification forensique (OSINT)	InVID/WeVerify, TinEye	Gratuit	Interm. +	~	✓✓	invid-project.eu / tineye.com	Compétences OSINT ; vérification ponctuelle, non automatisée

Catégorie	Exemples	Coût*	Profil adapté	Collecte	Analyse	Lien	Points de vigilance
Messageries chiffrées	Signal, ProtonMail	Gratuit	Toute taille	✓	✗	signal.org / proton.me	Usage limité à la transmission ; pas de stockage structuré ; gestion des clés
Chiffrement des données	VeraCrypt, BitLocker, AxCrypt	Gratuit → freemium	Toute taille	~	~	veracrypt.fr	Configuration initiale ; gestion des clés critique ; formation nécessaire
Plateformes de données humanitaires	HDX, ReliefWeb, ACLED	Gratuit	Toute taille (consult.)	✓✓	✓	data.humdata.org / reliefweb.int	Données publiques uniquement ; délais de mise à jour variables
Systèmes d'alerte précoce	FEWS Net, INFORM, GDACS	Gratuit	Toute taille (consult.)	✓	✓✓	fews.net / gdacs.org	Portée thématique limitée ; modèles d'agrégation opaques ; compléter par le terrain

*Sources : revue de littérature, benchmark et enquête de terrain 2026, Charlotte Chuard. * Coût indicatif et subjectif, à vérifier auprès de l'éditeur. Les liens sont donnés à titre de point d'entrée.*

EXEMPLE Combinaisons d'outils recommandées par profil

Petite structure (< 50 emp.) : Google Alerts (collecte gratuite) + Google Drive structuré ou SharePoint (stockage) + Google Sheets avec fiche d'identité (traçabilité). Coût : 0 CHF.

Structure intermédiaire (50–250 emp.) : Feedly Pro (agrégation) + SharePoint (stockage) + Power BI (visualisation) + Signal ou ProtonMail (canaux sécurisés niv. 3-4). Coût estimé : 100–300 CHF/mois.

Grande organisation (> 250 emp.) : Sprinklr ou Hootsuite (social listening) + base relationnelle ou SharePoint avancé + Power BI + KoBoToolbox (terrain) + UNOSAT (imagerie). Coût estimé : à partir de 2 000 CHF/mois.

- **3. Bonnes pratiques**
- **3.1 Quoi faire**

Classer la sensibilité de vos informations

Avant tout choix d'outil ou de méthode, définissez le niveau de sensibilité de chaque type d'information que vous collectez. C'est l'action qui a le plus d'impact immédiat sur votre sécurité, et elle ne coûte rien.

Tableau 2 — Classification de la sensibilité et mesures associées

Niveau	Définition	Exemples concrets	Chiffrement	Hébergement autorisé
1 — Public	Information publiable sans restriction	Rapport de situation mensuel, indicateurs agrégés publiés sur HDX, communiqués de presse	Recommandé	Cloud commercial (Drive, SharePoint)
2 — Interne	Usage interne, sans risque grave si fuite limitée	Calendrier des tournées, plans logistiques non sensibles, analyses de contexte non publiées	Obligatoire en transit	Cloud org. + outils commerciaux
3 — Confidentiel	Données personnelles ou opérationnellement sensibles	Listes de bénéficiaires (même pseudonymisées), analyses de menaces, localisation précise, rapport d'incident	Obligatoire (transit + repos)	Serveurs de l'organisation ou certifiés ISO 27001
4 — Strictement confidentiel	Données dont la divulgation peut mettre des personnes en danger	Identité de sources humaines, témoignages nominatifs de victimes, données biométriques,	Obligatoire, double couche	Serveurs de l'organisation exclusivement

Niveau	Définition	Exemples concrets	Chiffrement	Hébergement autorisé
		GPS d'informateurs en zone de conflit		

© Charlotte Chuard 2026

Les colonnes « Exemples concrets » du tableau ci-dessus suffisent à situer la plupart de vos informations. En cas de doute, retenez la règle prudente : classez au niveau supérieur.

Remplir une fiche d'identité informationnelle

Pour chaque information de veille collectée, documentez systématiquement son origine, sa fiabilité initiale et son niveau de sensibilité. Voici un exemple de fiche remplie :

Tableau 3 — Fiche d'identité informationnelle (exemple rempli)

Champ	Contenu
Information collectée	Des tensions communautaires sont signalées près du camp de déplacés de la zone nord, avec un risque de mouvement de population dans les 48 h.
Source primaire	Coordinateur terrain local, appel téléphonique direct, 14h32
Type de source	Source humaine directe, interne à l'organisation
Canal de collecte	Appel téléphonique, transcription écrite immédiate
Niveau de confiance initial	B2 — source fiable, information probablement vraie (non encore confirmée)
Vérification effectuée	Croisement 40 min plus tard avec le rapport du cluster Protection → niveau relevé à A2 (source et information confirmées)
Niveau de sensibilité	Niveau 3 — Confidentiel
Restrictions de diffusion	Équipe coordination terrain + direction des opérations uniquement
Archivage / destruction	Archivage 6 mois / révision du niveau de sensibilité à J+30

Exemple illustratif, © Charlotte Chuard 2026

Valider avant de diffuser : la règle de la diffusion progressive

En situation d'urgence, ne bloquez pas l'action en attendant une validation complète. Diffusez immédiatement, mais en indiquant clairement le niveau de fiabilité :

EXEMPLE Un incident signalé via les réseaux sociaux, heure par heure

15h00 — 1 seule source (réseau social) : « ⚠ Signal NON VÉRIFIÉ, source unique. Vérification en cours. » → les équipes sont alertées sans être induites en erreur.

15h40 — 2e source (collègue terrain) : « ℹ Information PARTIELLEMENT VÉRIFIÉE, confirmée par une source indépendante. » → les décideurs peuvent commencer à adapter les plans.

16h15 — rapport cluster sécurité : « ✓ Information VÉRIFIÉE, 3 sources concordantes. » → décision pleine et entière, avec traçabilité complète de l'évolution.

Protéger les sources humaines

Toute personne qui vous fournit une information dans un contexte à risque doit être protégée. Cela implique : ne jamais transférer un message contenant son nom ou son numéro ; rédiger une synthèse anonymisée plutôt que citer le message original ; supprimer les messages originaux après extraction ; et stocker les informations identifiantes dans un fichier chiffré séparé, accessible au seul responsable désigné.

- **3.2 À quoi faire attention**

⚠ VIGILANCE La désinformation ciblée

56 % des organisations sondées perçoivent la désinformation comme un risque majeur, mais seules 33 % ont un protocole pour la détecter. Une photo manipulée ou une rumeur fabriquée peut déclencher une réaction opérationnelle coûteuse. Avant de diffuser une alerte, vérifiez systématiquement l'image avec TinEye ou InVID, et recoupez avec une source indépendante.

⚠ VIGILANCE Le stockage non sécurisé de données sensibles

56 % des organisations stockent leurs données sur des outils cloud commerciaux sans mesure complémentaire. Ce n'est pas un problème pour les niveaux 1 et 2, mais c'est une vulnérabilité critique pour les niveaux 3 et 4.

⚠ VIGILANCE La pression de l'urgence

L'urgence est la première raison pour laquelle les procédures sont contournées (citée par 67 % des répondants). Or c'est en situation d'urgence que les erreurs d'information sont les plus

coûteuses. La diffusion progressive avec indicateur de confiance est précisément conçue pour que rapidité et rigueur ne s'excluent plus.

⚠ VIGILANCE L'accumulation de données sans politique de destruction

Conserver des données sensibles « au cas où » est courant mais dangereux : une donnée inutile mais stockée est une surface d'exposition sans bénéfice. Aucune des organisations enquêtées ne déclarait de politique formelle de destruction. Définir une durée de conservation dès la collecte est une protection simple et efficace.

- **3.3 Priorité de mise en place**

Si vous ne pouvez faire qu'une chose à la fois, voici l'ordre recommandé, du plus simple et impactant au plus avancé :

Tableau 4 — Séquence de mise en place par ordre de priorité

#	Action prioritaire	Ce que ça résout	Ressources
1	Classer vos informations par niveau de sensibilité	Sait immédiatement quoi stocker où et qui peut y accéder ; résout la principale source de risque non conscient	1 h de réunion d'équipe
2	Remplir une fiche d'identité pour chaque information	Crée une traçabilité minimale immédiate, sans outil technique	30 min de formation, un modèle
3	Instaurer la double validation (2 sources / 2 personnes) avant diffusion	Réduit fortement le risque de diffuser une information fausse sous pression	Accord organisationnel interne
4	Indiquer systématiquement le niveau de fiabilité	Permet aux décideurs d'agir vite sans être induits en erreur	Convention de notation
5	Restreindre l'accès selon le niveau de sensibilité	Limite les expositions accidentelles	Configuration des droits existants
6	Définir une durée de conservation et un mode de destruction	Évite l'accumulation de données devenues inutiles	Politique interne (1 page suffit)

#	Action prioritaire	Ce que ça résout	Ressources
7	Activer le chiffrement sur les données de niveau 3 et 4	Protège les données même en cas de compromission	Dépend des outils en place
8	Former aux risques cyber de base (phishing, mots de passe, désinformation)	Réduit le facteur humain, première source de failles	Formation interne, ressources en ligne gratuites

- **4. Auto-évaluation de maturité**

Cette grille vous permet d'évaluer en moins de 20 minutes le niveau de maturité actuel de votre organisation sur les trois piliers : sécurité de l'information, protection des données et traçabilité des sources.

Comment utiliser cette grille

- Pour chaque critère, cochez honnêtement le niveau qui décrit votre situation réelle — pas ce que vous aimeriez faire, mais ce que vous faites effectivement.
- Comptabilisez le nombre de cases cochées par niveau et par pilier.
- Votre profil dominant (le niveau le plus coché) définit votre maturité actuelle.
- Votre prochaine priorité : les critères de niveau 2 que vous n'atteignez pas encore — vos actions les plus accessibles.

Tableau 5 — Grille d'auto-évaluation de maturité (18 critères)

Critère (cochez votre niveau)	1 : Initial	2 : Reproductible	3 : Défini	4 : Maîtrisé
Pilier — Sécurité de l'information				
S1. Informations classées selon leur sensibilité ?	Non	Informellement	Formellement (4 niveaux)	Révisé régulièrement
S2. Données sensibles chiffrées ?	Non	Parfois	Systématique (niv. 3-4)	Systématique (niv. 2-3-4)
S3. Accès restreint selon les rôles ?	Non	Par habitude	Règles écrites en place	MFA activé pour niv. 3-4

Critère (cochez votre niveau)	1 : Initial	2 : Reproductible	3 : Défini	4 : Maîtrisé
S4. Plan documenté en cas d'incident ?	Non	Plan informel	Plan écrit	Plan testé ≥ 1×/an
S5. Outils critiques fonctionnent hors ligne ?	Non	Certains	La plupart	Totalité, synchro sécurisée
S6. Personnel formé aux risques cyber de base ?	Non	Ponctuellement	Formation initiale formelle	Formation annuelle
Pilier — Protection des données				
P1. DPIA réalisée pour les traitements sensibles ?	Non	Ponctuellement	Systématique niv. 3-4	À chaque traitement
P2. Protocoles de consentement documentés ?	Non	Verbal informel	Protocoles écrits	Adaptés au contexte
P3. Seules les données nécessaires collectées ?	Non	Par habitude	Règle formalisée	Vérification systématique
P4. Données anonymisées avant partage externe ?	Non	Parfois	Systématique	Méthodes SDC (k≥5)
P5. Durées de conservation définies et respectées ?	Non	Vaguement	Définies par niveau	Automatisées et vérifiées
P6. Personnes concernées peuvent accéder/supprimer leurs données ?	Non	Sur demande	Processus documenté	Processus testé
Pilier — Traçabilité des sources				

Critère (cochez votre niveau)	1 : Initial	2 : Reproductible	3 : Défini	4 : Maîtrisé
T1. Origine de chaque information documentée ?	Non	Par habitude	Fiche remplie systématiquement	Fiche standardisée + audit trail
T2. Sources évaluées selon une grille formalisée ?	Non	Par intuition	Matrice A1-F6 ou équivalent	Revue périodique du portefeuille
T3. Information sensible croisée avec ≥ 2 sources indépendantes ?	Non	Parfois	Règle définie, application partielle	Systématique, indépendance vérifiée
T4. Journal des accès (audit trail) pour données sensibles ?	Non	Non	Pour niv. 3-4	Niv. 2-3-4, revue trimestrielle
T5. Produits de veille avec indicateur de fiabilité visible ?	Non	Parfois, à la demande	Systématique (3 niveaux min.)	Mis à jour en temps réel
T6. Sources OSINT vérifiées (forensique) ?	Non	Ponctuellement	Protocole écrit appliqué	Outillé (InVID, TinEye…)

Adapté du modèle CMMI, © Charlotte Chuard 2026

Interprétation des résultats

Majorité en Niveau 1 : vos pratiques sont informelles et dépendent des personnes. Priorité absolue : classification de sensibilité (S1) et fiche d'identité (T1). Ces deux actions ne coûtent rien et changent déjà beaucoup.

Majorité en Niveau 2 : de bonnes habitudes, mais peu de choses écrites. Priorité : documenter ce que vous faites déjà, désigner une personne responsable, obtenir un accord formel de la direction.

Majorité en Niveau 3 : des processus formalisés qui ne couvrent pas toutes les situations. Priorité : combler les critères encore à « Non » et mesurer l'application réelle des procédures.

Majorité en Niveau 4 : dispositif solide. Prochaine étape : optimiser (automatisation, benchmark, partage d'expériences).

À retenir : le niveau 1 est un point de départ, non une cible — il ne met en œuvre aucune des recommandations de ce guide. L'objectif minimal réaliste pour toute organisation ou unité chargée de la veille est d'atteindre le niveau 2 sur les trois piliers.

EXEMPLE Rappel issu de l'enquête

Dans le secteur humanitaire, la maturité informationnelle est davantage corrélée à la spécialisation fonctionnelle qu'à la taille de l'organisation. Une petite structure dédiée à la veille peut atteindre le niveau 4, là où une grande organisation généraliste reste au niveau 1.

- **5. Fonctionnalités essentielles**

Les entretiens ont fait émerger cinq fonctionnalités récurrentes, systématiquement citées comme manquantes ou insuffisantes. Elles ne sont pas propres à une taille d'organisation. Le tableau ci-dessous les traduit en solutions concrètes par profil.

Tableau 6 — Fonctionnalités essentielles et solutions par taille d'organisation

Fonctionnalité	Petite (< 50)	Intermédiaire (50–250)	Grande (> 250)
Regroupement des informations	Dossier partagé unique (Drive/SharePoint), un sous-dossier par zone, alimenté manuellement	Un agrégateur (Feedly) relié au dossier, collecte semi-automatisée	Plateforme centralisée agrégeant flux, réseaux sociaux et sources internes
Synthétisation avec sources	Note hebdomadaire manuelle, sources en bas de page	Template standardisé avec champ source obligatoire et niveau de fiabilité	Tableau de bord BI affichant les synthèses par zone avec liens vers les sources
Veille sur plusieurs niveaux	Document en 2 sections : contexte (mensuel) + alertes terrain	Newsletter bi-hebdo à 2 niveaux : stratégique + opérationnel	Flux distincts par niveau d'utilisateur, dans le système interne
Formation et soutien	Demi-journée + ressources gratuites (KoBo Academy, OCHA eLearning)	Formation de 1-2 jours + référent interne désigné	Programme structuré, intégré à l'onboarding, avec certification interne
Maintenance (sans dépendance externe)	Outils maintenus par les équipes, sans prestataire	Un administrateur désigné ; mises à jour semestrielles	Équipe IT interne ou SLA avec prestataire
Intégration à l'existant	S'appuie sur SharePoint/Drive ;	Agrégateur connecté aux sources via RSS/API, sans	Intégration à l'écosystème

Fonctionnalité	Petite (< 50)	Intermédiaire (50–250)	Grande (> 250)
	structure des dossiers optimisée	changement d'environnement	Microsoft/Google via connecteurs natifs

D'après les entretiens, © Charlotte Chuard 2026

L'outil idéal, selon les personnes interrogées

« Qu'il ne me demande pas de changer ce que je fais déjà. » La principale cause d'échec d'un nouveau dispositif est la migration. L'outil idéal s'intègre à l'existant.

« Qu'il me dise rapidement ce qui est important. » Face au volume, la synthèse automatisée — même partielle — est la fonctionnalité la plus différenciante.

« Qu'il soit simple à former et à maintenir. » Un outil qui dépend d'une seule personne est un risque. L'idéal : utilisable correctement en une demi-journée par tout nouveau collègue.

- **6. Mettre en place le dispositif**

Les réponses ci-dessous sont différenciées par taille, car les contraintes varient fortement entre une structure de 8 personnes et une organisation de 1 000 employés.

Tableau 7 — Questions de mise en place et réponses par profil

Question	Petite (< 50)	Intermédiaire (50–250)	Grande (> 250)
Quelle équipe ?	1 référent (20-30 % du temps) + 1 binôme de secours	1-2 personnes à temps partiel + relais terrain	Équipe dédiée (2-5) : analyste, DPO fonctionnel, référent sécurité
Délai réaliste	2-4 semaines pour les pratiques de base	1-3 mois pour structurer et former	3-6 mois pour déployer, former et formaliser
Coût indicatif	0 CHF (bases) ; 0-50 CHF/mois si agrégateur freemium	500-2 000 CHF/an + temps interne	5 000-30 000 CHF/an selon l'outillage
À valider avec la direction	Accord sur responsable, temps, règle d'incident	Validation si budget ; charte veille d'1 page signée	Mandat formel, budget approuvé, reporting trimestriel

Question	Petite (< 50)	Intermédiaire (50–250)	Grande (> 250)
Accès ouvert ou restreint ?	Niv. 1-2 : équipe. Niv. 3-4 : décideurs + direction	Niv. 3 : programme + direction. Niv. 4 : direction + DPO	Droits par rôle ; audit log pour niv. 3-4
Processus recommandé	Collecter → fiche d'identité → valider à 2 → diffuser avec fiabilité	Collecter → traiter → valider (2 sources) → synthèse → diffuser	Collecter (auto) → analyste valide → DPO vérifie → diffusion calibrée

D'après les entretiens et l'enquête, © Charlotte Chuard 2026

Combiner deux logiques : push et pull

- Push (envoi actif) pour l'urgent : une alerte envoyée directement dès qu'une information de niveau 3-4 est validée. Les personnes reçoivent l'information sans la chercher.
- Pull (accès à la demande) pour le fond : une newsletter interne hebdomadaire ou mensuelle, accessible via le dossier partagé ou l'intranet.

Trois questions à clarifier avec la direction avant de commencer

- Qui est responsable ? Pas « qui s'en occupe », mais qui répond en cas d'erreur ou d'incident.
- Quelles ressources ? Même sans budget, un accord sur le temps alloué (« 2 h par semaine ») évite que la veille soit la première tâche abandonnée.
- Qui peut autoriser une exception ? En urgence vitale, qui décide de partager une donnée normalement protégée ? Ce nom doit être connu à l'avance.

- **7. Aller plus loin : le modèle TRIVAH**

Les bonnes pratiques de ce guide sont toutes applicables sans modèle conceptuel particulier. Mais si votre organisation souhaite formaliser un dispositif qui articule systématiquement sécurité, protection et traçabilité, elle peut s'appuyer sur le modèle TRIVAH, développé dans le cadre de ce travail.

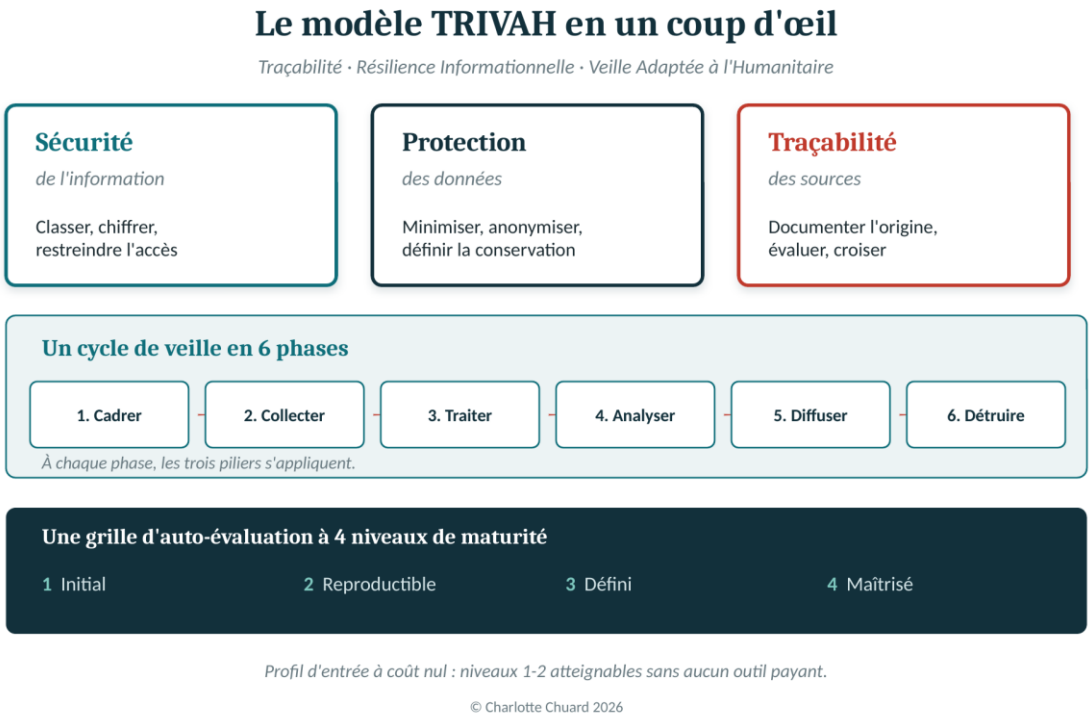


Figure 1 — Le modèle TRIVAH : trois piliers, un cycle en six phases, quatre niveaux de maturité. © Charlotte Chuard 2026

- **7.1 Comment le modèle répond aux besoins identifiés**

Tableau 8 — Correspondance entre les besoins terrain et les réponses de TRIVAH

Besoin identifié sur le terrain	Ce que TRIVAH prévoit	Comment le mettre en place
Urgence vs rigueur (67 % citent ce facteur)	Diffusion progressive avec indicateur de confiance : diffuser immédiatement mais en indiquant la fiabilité, sans bloquer l'action	Adopter la convention à 3 niveaux (non vérifié / partiellement / vérifié) sur tous les canaux internes
Désinformation sous-protocolarisée (56 % risque perçu, 33 % protocole)	Validation en 3 temps : vérification automatique, triangulation, validation humaine	Règle simple pour démarrer : aucune information sensible ne sort sans ≥ 2 sources indépendantes
Dépendance au cloud sans chiffrement (56 %)	Classification à 4 niveaux avec hébergement différencié : les données les plus sensibles ne vont pas dans le cloud commercial	Identifier les 10 % de données les plus sensibles et les déplacer sur un espace sécurisé

Besoin identifié sur le terrain	Ce que TRIVAH prévoit	Comment le mettre en place
Budget contraint (100 % des répondants)	Profil d'entrée niveau 1-2 : fiche d'identité + double validation + SharePoint existant = 0 CHF additionnel	Démarrer sans rien acheter ; ajouter des outils seulement quand les bases sont en place
Aucune politique de destruction (lacune universelle)	Phase 6 du cycle : destruction documentée, vérification trimestrielle, registre des traitements	Créer un tableau de bord simple avec les dates de révision par type de données

© *Charlotte Chuard 2026*

- **7.2 Cinq principes pour une mise en place réussie**

Former avant d'outiller. L'erreur la plus fréquente est d'acquérir un outil avant que les équipes ne comprennent pourquoi. Une demi-journée de formation vaut mieux que n'importe quel logiciel acheté sans préparation.

Construire dès le départ, pas réparer après. Introduire la traçabilité ou la classification une fois les pratiques installées est bien plus difficile que de les intégrer d'emblée.

Constituer un groupe de travail transversal. Analyse, sécurité informatique, juridique (RGPD), terrain : réunir ces compétences dès la conception évite les angles morts.

Progresser par niveaux, pas d'un coup. La grille (chapitre 4) sert à définir votre prochain niveau réaliste. Passer du niveau 1 au niveau 2 sur les 18 critères est déjà une transformation significative.

Anticiper le coût de la transition. Prévoir une phase de 1 à 3 mois pendant laquelle les deux systèmes coexistent.

- **8. Pour aller plus loin**

Ce guide est une synthèse pratique conçue pour la diffusion directe auprès des organisations. Il s'appuie sur un travail de recherche plus complet, qui détaille la méthodologie, l'intégralité des résultats, le modèle conceptuel et sa validation par confrontation à des cas réels et par benchmark (OCHA, CICR, IFRC, ACAPS). Les organisations souhaitant un accompagnement peuvent prendre contact avec l'auteure.

Ressources complémentaires recommandées

- CICR, Handbook on Data Protection in Humanitarian Action (2024) — référence sectorielle sur la protection des données.
- IFRC, Data Playbook — guide pédagogique sur la gestion des données, adapté aux contextes à faibles ressources.

- OCHA, Centre for Humanitarian Data (humdata.org) — standards HDX/HXL et gestion responsable des données.
- KoBoToolbox Academy (support.kobotoolbox.org) — formation gratuite à la collecte de données terrain.

1 Préambule

Ce guide s'adresse à toute personne travaillant au sein d'une organisation humanitaire, ONG ou structure de développement qui souhaite structurer ou améliorer son dispositif de veille informationnelle. Il a été conçu pour être utile quelle que soit votre situation de départ : que vous débutiez avec un simple tableur, que vous ayez déjà des pratiques informelles à consolider, ou que vous cherchiez à formaliser un système existant.

Il est pertinent pour vous si vous vous reconnaissez dans l'une de ces situations :

- Vous suivez l'actualité de vos zones d'intervention de manière informelle, sans processus clair, et vous souhaitez structurer cette pratique.
- Vous avez des outils en place mais ne savez pas si vos informations sont suffisamment sécurisées et traçables.
- Vous devez convaincre votre direction d'investir (du temps ou du budget) dans la veille, et avez besoin d'arguments concrets.
- Vous êtes en charge de la sécurité, de la gestion documentaire ou de la qualité de l'information au sein de votre organisation.
- Vous cherchez à choisir entre plusieurs outils disponibles sur le marché et voulez un guide de lecture neutre.

Ce guide est basé sur une enquête menée en 2026 auprès de neuf professionnels de la veille dans huit organisations humanitaires et de développement, complétée par des entretiens qualitatifs et l'analyse de dispositifs de référence (OCHA HDX, ACAPS CrisisInSight, CICR, IFRC Data Playbook). Tous les chiffres cités (pourcentages de pratiques observées, fréquences) sont issus de cette enquête.

2 Outils

Le tableau ci-dessous recense l'ensemble des outils mobilisables pour la veille humanitaire, des plus simples aux plus avancés. La colonne « Profil adapté » vous aide à identifier rapidement les outils pertinents pour votre situation.

Légende des capacités, ✓✓✓ excellence ✓ suffisant ~ limité ✗ absent

Col. = Capacité de collecte

Ana. = Capacité d'analyse

Outil / catégorie	Exemples concrets	Coût	Profil adapté	Col.	Ana.	Points de vigilance
Alertes automatiques (mots-clés)	Google Alerts	Gratuit	Toute taille, débutant	✓	✗	Biais algorithmique, aucune traçabilité, pas de contrôle sur les sources
Agrégateurs de flux RSS	Feedly (freemium), KB Crawl (pro)	Gratuit → abonnement	Petite à intermédiaire	✓✓	~	Dépendance à l'éditeur, biais de sélection, volumétrie à gérer
Social listening professionnel	Sprinklr, Hootsuite, Brandwatch, Factiva	Élevé (abonnement annuel)	Grande org. uniquement	✓✓✓	✓✓	Coût prohibitif pour petites structures ; données hébergées hors UE possible
Réseaux sociaux (sources directes)	Facebook, LinkedIn, Instagram, X, YouTube, TikTok	Gratuit	Toute taille	✓	✗	Désinformation, biais de représentation, aucune traçabilité native
Stockage centralisé cloud (suite bureautique)	SharePoint, OneDrive, Google Drive	Inclus dans l'abonnement bureautique	Toute taille	~	~	Souveraineté des données, juridiction non-UE, chiffrement partiel
Système de gestion documentaire (NGO)	NGO Online, M-Files	Abonnement sectoriel	Intermédiaire +	~	~	Moins répandu, courbe d'apprentissage, coût à négocier
Base de données relationnelle	PostgreSQL, MySQL, Airtable	Gratuit (open source) ou freemium	Grande org. (ressources tech.)	✓	✓	Nécessite des compétences techniques

Outil / catégorie	Exemples concrets	Coût	Profil adapté	Col.	Ana.	Points de vigilance
						internes ou un prestataire
Business Intelligence (BI) et visualisation	Power BI, Tableau, Metabase	Abonnement bureautique ou standalone	Intermédiaire +	✗	✓✓✓	Compétences techniques requises ; valeur ajoutée faible sans données structurées en amont
Analyse de réseaux	Gephi (open source), NodeXL	Gratuit	Avancé (spécialiste)	✗	✓✓	Courbe d'apprentissage importante ; données d'entrée structurées nécessaires
Intelligence artificielle / NLP	ChatGPT, Claude, NLP Python, assistant IA Ushahidi	Freemium à élevé	Avancé (encadré)	✓	✓✓	Biais algorithmiques, traçabilité des sorties, confidentialité des données, hallucinations
Tableurs	Microsoft Excel, Google Sheets	Inclus dans la suite bureautique	Toute taille	✓	~	Pas de traçabilité native, risque d'erreurs humaines, pas de versionnage automatique
Formulaires de collecte terrain	KoBoToolbox (gratuit ONG), ONA, ODK	Gratuit pour ONG humanitaires	Toute taille	✓✓✓	~	Nécessite connectivité pour synchronisation ; paramétrer le mode hors ligne

Outil / catégorie	Exemples concrets	Coût	Profil adapté	Col.	Ana.	Points de vigilance
Cartographie participative	Ushahidi, OpenStreetMap, HDX / OCHA	Gratuit / open source	Toute taille	✓✓	✓	Données de localisation sensibles ; agrégation géographique obligatoire avant partage
Imagerie satellitaire	UNOSAT (gratuit humanitaire), Planet Labs	Gratuit (UNOSAT) ou abonnement	Grandes org. ou partenariat	✓✓	✓	Données de localisation précises ; risque de ré-identification élevé ; protocoles stricts requis
Vérification forensique (OSINT)	InVID / WeVerify, TinEye, Exif.tools	Gratuit	Intermédiaire +	~	✓✓	Compétences OSINT requises ; vérification ponctuelle, non automatisée
Messageries chiffrées	Signal, ProtonMail, Keybase	Gratuit	Toute taille	✓	✗	Usage limité à la transmission ; pas de stockage structuré ; gestion des clés à prévoir
Chiffrement des données	VeraCrypt, BitLocker, AxCrypt	Gratuit à freemium	Toute taille	~	~	Configuration technique initiale ; gestion des clés critique ; formation nécessaire
Plateformes de données humanitaires	HDX (OCHA), ReliefWeb, ACLED	Gratuit	Toute taille (consultation)	✓✓	✓	Données publiques uniquement ;

Outil / catégorie	Exemples concrets	Coût	Profil adapté	Col.	Ana.	Points de vigilance
						délais de mise à jour variables selon la crise
Systèmes d'alerte précoce	FEWS Net, INFORM Risk Index, GDACS	Gratuit	Toute taille (consultation)	✓	✓✓	Portée thématique limitée ; modèles d'agrégation opaques ; compléter par des sources terrain

Sources : enquête de terrain 2026 et analyse documentaire, Charlotte Chuard, 2026

Comment lire ce tableau et choisir votre outil

Trois questions vous guident dans le choix :

Quel est votre besoin prioritaire ? Collecte d'information, stockage sécurisé, analyse ou diffusion ? Les outils ne couvrent pas tous les mêmes fonctions, il en faut souvent plusieurs, coordonnés.

Quelles sont vos ressources réelles ? Budget mensuel, compétences techniques disponibles, temps à consacrer à la maintenance. Un outil gratuit bien utilisé vaut toujours mieux qu'un outil coûteux sous-utilisé.

Quel niveau de sensibilité pour vos données ? Les outils de stockage cloud commercial (SharePoint, Drive) sont acceptables pour les niveaux 1 et 2, mais pas pour les niveaux 3 et 4.

EXEMPLE Combinaisons d'outils recommandées par profil

Petite structure (< 50 emp.) : Google Alert (collecte gratuite) + Google Drive structuré ou SharePoint (stockage) + Google Sheets avec fiche d'identité (traçabilité). Coût : 0 CHF.

Structure intermédiaire (50–250 emp.) : Feedly Pro (agrégation) + SharePoint (stockage centralisé) + Power BI (visualisation) + Signal ou ProtonMail (canaux sécurisés niveaux 3-4). Coût estimé : 100–300 CHF/mois.

Grande organisation (> 250 emp.) : Sprinklr ou Hootsuite (social listening) + base de données relationnelle ou SharePoint avancé + Power BI (analyse) + KoBoToolbox (collecte terrain) + UNOSAT (imagerie). Coût estimé : à partir de 2 000 CHF/mois.

3 Bonnes pratiques

3.1 Quoi faire

Classer la sensibilité de vos informations

Avant tout choix d'outil ou de méthode, définissez le niveau de sensibilité de chaque type d'information que vous collectez. C'est l'action qui a le plus d'impact immédiat sur votre sécurité, et elle ne coûte rien.

Tableau 1, Classification de la sensibilité et mesures associées

Niveau	Définition	Exemples concrets	Chiffrement	Hébergement autorisé
1 Public	Information publiable sans restriction	Rapport de situation mensuel, indicateurs agrégés publiés sur HDX, communiqués de presse	Recommandé	Cloud commercial (Drive, SharePoint)
2 Interne	Usage interne uniquement, sans risque grave si fuite limitée	Calendrier des tournées de distribution, plans logistiques non sensibles, analyses de contexte non publiées	Obligatoire en transit	Cloud org. + outils commerciaux
3 Confidentiel	Données personnelles ou opérationnellement sensibles	Listes de bénéficiaires (même pseudonymisées), analyses de menaces, données de localisation précises, rapport d'incident	Obligatoire (transit + repos)	Serveurs de l'organisation ou certifiés ISO 27001
4 Strictement confidentiel	Données dont la divulgation peut mettre des personnes en danger	Identité de sources humaines, témoignages nominatifs de victimes, données biométriques, coordonnées GPS d'informateurs en zone de conflit	Obligatoire, double couche	Serveurs de l'organisation exclusivement

Charlotte Chuard, 2026

EXEMPLE Reconnaître le bon niveau au quotidien

Niveau 1 : votre rapport de situation mensuel publié sur votre site internet. Peut aller sur HDX, partageable librement.

Niveau 2 : le calendrier interne de la semaine des distributions. Ne sort pas de l'organisation mais ne met aucune personne en danger si fuité.

Niveau 3 : une liste de ménages bénéficiaires avec codes (pas de noms) et zones d'habitation approximatives. Chiffrement requis, partage limité.

Niveau 4 : le nom et les coordonnées GPS précises d'un informateur local en zone de conflit. Ne quitte jamais les serveurs de l'organisation, chiffrement double couche.

Remplir une fiche d'identité informationnelle

Pour chaque information de veille collectée, documenter systématiquement son origine, sa fiabilité initiale et son niveau de sensibilité. Voici un exemple de fiche remplie :

Modèle de fiche d'identité informationnelle, exemple rempli

Champ	Contenu
Information collectée	Des tensions communautaires sont signalées près du camp de déplacés de la zone nord, avec un risque de mouvement de population dans les prochaines 48h.
Source primaire	Coordinateur terrain local, appel téléphonique direct, 14h32
Type de source	Source humaine directe, interne à l'organisation
Canal de collecte	Appel téléphonique, transcription écrite immédiate
Niveau de confiance initial	B2, source fiable, information probablement vraie (non encore confirmée)
Vérification effectuée	Croisement 40 min plus tard avec rapport du cluster Protection sur le même secteur → niveau relevé à A2 (source confirmée, information confirmée par une source indépendante)
Niveau de sensibilité	Niveau 3, Confidentiel
Restrictions de diffusion	Équipe coordination terrain + direction des opérations uniquement
Archivage / destruction prévue	Archivage 6 mois / révision du niveau de sensibilité à J+30

Exemple illustratif, Charlotte Chuard, 2026

Valider avant de diffuser, la règle de la diffusion progressive

En situation d'urgence, ne bloquez pas l'action en attendant une validation complète. Diffusez immédiatement, mais en indiquant clairement le niveau de fiabilité :

EXEMPLE Un incident signalé via les réseaux sociaux, heure par heure

15h00, 1 seule source (réseau social) : « ⚠ Signal NON VÉRIFIÉ, source unique. Vérification en cours. » → Les équipes sont alertées sans être induites en erreur.

15h40, 2e source (collègue terrain) : « ℹ Information PARTIELLEMENT VÉRIFIÉE, confirmée par une source indépendante. » → Les décideurs peuvent commencer à adapter les plans.

16h15, Rapport cluster sécurité : « ✓ Information VÉRIFIÉE, 3 sources concordantes. » → Décision pleine et entière possible, avec traçabilité complète de l'évolution.

Protéger les sources humaines

Toute personne qui vous fournit une information dans un contexte à risque doit être protégée. Cela implique : ne jamais transférer un message contenant son nom ou son numéro de téléphone, rédiger une synthèse anonymisée plutôt que citer le message original, supprimer les messages originaux après extraction du contenu, et stocker les informations permettant d'identifier la source dans un fichier chiffré séparé, accessible uniquement au responsable désigné.

3.2 À quoi faire attention

⚠ VIGILANCE La désinformation ciblée

56 % des organisations sondées perçoivent la désinformation comme un risque majeur, mais seules 33 % ont un protocole pour la détecter. Sur les réseaux sociaux, une photo manipulée ou une rumeur fabriquée peut déclencher une réaction opérationnelle coûteuse. Avant de diffuser une alerte terrain, vérifiez systématiquement l'image avec TinEye ou InVID, et recoupez avec une source indépendante.

⚠ VIGILANCE Le stockage non sécurisé de données sensibles

56 % des organisations stockent leurs données sur des outils cloud commerciaux sans mesure complémentaire. Ce n'est pas un problème pour les niveaux 1 et 2, mais c'est une vulnérabilité critique pour les niveaux 3 et 4.

⚠ VIGILANCE La pression de l'urgence

L'urgence est la première raison pour laquelle les procédures sont contournées (citée par 67 % des répondants). Paradoxalement, c'est en situation d'urgence que les erreurs d'information sont

les plus coûteuses. La diffusion progressive avec indicateur de confiance est précisément conçue pour que rapidité et rigueur ne s'excluent plus.

⚠ VIGILANCE L'accumulation de données sans politique de destruction

Conserver des données sensibles « au cas où » est une pratique courante, mais dangereuse : une donnée qui n'est plus utile mais reste stockée est une surface d'exposition sans bénéfice. Aucune des organisations enquêtées ne déclarait de politique formelle de destruction. Définir une durée de conservation à la collecte (et la respecter) est une protection simple et efficace.

3.3 Priorité de mise en place

Si vous ne pouvez faire qu'une chose à la fois, voici l'ordre recommandé, du plus simple et le plus impactant au plus avancé :

Tableau 2, Séquence de mise en place par ordre de priorité

#	Action prioritaire	Ce que ça résout concrètement	Ressources nécessaires
1	Classer vos informations par niveau de sensibilité	Sait immédiatement où stocker quoi et qui peut y accéder, résout la principale source de risque non conscient	1 heure de réunion d'équipe
2	Remplir une fiche d'identité informationnelle pour chaque information	Crée une traçabilité minimale immédiate, sans outil technique	30 min de formation, un modèle de fiche
3	Instaurer la règle de double validation (2 sources / 2 personnes) avant diffusion	Réduit significativement le risque de diffuser une information fausse sous pression	Accord organisationnel interne
4	Indiquer systématiquement le niveau de fiabilité sur toute information diffusée	Permet aux décideurs d'agir rapidement sans être induits en erreur	Convention de notation à définir
5	Restreindre l'accès aux dossiers selon le niveau de sensibilité	Limite les expositions accidentelles ou involontaires	Configuration des droits dans les outils existants

#	Action prioritaire	Ce que ça résout concrètement	Ressources nécessaires
6	Définir une durée de conservation et un mode de destruction par type de données	Évite l'accumulation de données sensibles devenues inutiles	Politique interne à formaliser (1 page suffit)
7	Activer le chiffrement sur les données de niveau 3 et 4	Protège les données même en cas de compromission du stockage	Dépend des outils déjà en place
8	Former les équipes aux risques cyber de base (phishing, mots de passe, désinformation)	Réduit le facteur humain, première source de failles de sécurité	Formation interne possible, ressources en ligne gratuites

4 Auto-évaluation de maturité

Cette grille vous permet d'évaluer en moins de 20 minutes le niveau de maturité actuel de votre organisation sur les trois dimensions essentielles d'un dispositif de veille sécurisée : sécurité de l'information, protection des données et traçabilité des sources.

Comment utiliser cette grille

- Pour chaque critère, cochez honnêtement le niveau qui décrit le mieux votre situation réelle, pas ce que vous aimeriez faire, mais ce que vous faites effectivement.
- Comptabilisez le nombre de cases cochées par niveau et par pilier.
- Votre profil dominant (le niveau où vous avez coché le plus de cases) définit votre niveau de maturité actuel.
- Votre prochaine priorité : passez en revue les critères de niveau 2 que vous n'atteignez pas encore, ce sont vos actions immédiates les plus accessibles.

Tableau 3, Grille d'auto-évaluation de maturité (18 critères)

Critère (cocher votre niveau actuel)	1 : Initial	2 : Reproductible	3 : Défini	4 : Maîtrisé
Pilier, Sécurité de l'information				
S1. Vos informations sont-elles classées selon leur niveau de sensibilité ?	Non	Informellement	Formellement (4 niveaux)	Révisé régulièrement
S2. Les données sensibles sont-elles chiffrées ?	Non	Parfois	Systématique (niv. 3-4)	Systématique (niv. 2-3-4)
S3. L'accès aux informations est-il restreint selon les rôles ?	Non	Par habitude	Règles écrites en place	MFA activé pour niv. 3-4
S4. Existe-t-il un plan documenté en cas d'incident de sécurité ?	Non	Plan informel	Plan écrit	Plan testé au moins 1×/an
S5. Les outils critiques fonctionnent-ils hors ligne si besoin ?	Non	Certains	La plupart	Totalité, synchro sécurisée

Critère (cocher votre niveau actuel)	1 : Initial	2 : Reproductible	3 : Défini	4 : Maîtrisé
S6. Le personnel est-il formé aux risques cyber de base ?	Non	Ponctuellement	Formation initiale formelle	Formation régulière annuelle
Pilier, Protection des données				
P1. Une analyse d'impact (DPIA) est-elle réalisée pour les traitements sensibles ?	Non	Ponctuellement	Systématique pour niv. 3-4	Systématique à chaque traitement
P2. Des protocoles de consentement adaptés sont-ils documentés ?	Non	Verbal informel	Protocoles écrits	Revus et adaptés au contexte
P3. Seules les données strictement nécessaires sont-elles collectées ?	Non	Par habitude	Règle formalisée	Vérification systématique
P4. Les données personnelles sont-elles anonymisées avant tout partage externe ?	Non	Parfois	Systématique	Méthodes SDC appliquées (k≥5)
P5. Des durées de conservation sont-elles définies et respectées ?	Non	Vaguement	Définies par niveau	Automatisées et vérifiées
P6. Les personnes concernées peuvent-elles accéder à leurs données ou en demander la suppression ?	Non	Sur demande seulement	Processus documenté	Processus opérationnel testé
Pilier, Traçabilité des sources				
T1. L'origine de chaque information est-elle	Non	Par habitude (certaines sources)	Fiche d'identité remplie systématiquement	Fiche standardisée + audit trail

Critère (cocher votre niveau actuel)	1 : Initial	2 : Reproductible	3 : Défini	4 : Maîtrisé
documentée (source, date, canal) ?				
T2. Les sources sont-elles évaluées selon une grille formalisée ?	Non	Par intuition	Matrice A1-F6 ou équivalent	Revue périodique du portefeuille sources
T3. Toute information sensible est-elle croisée avec au moins 2 sources indépendantes ?	Non	Parfois	Règle définie, application partielle	Systématique, indépendance vérifiée
T4. Un journal des accès (audit trail) est-il maintenu pour les données sensibles ?	Non	Non	Pour niv. 3-4	Pour niv. 2-3-4, revisite trimestrielle
T5. Les produits de veille diffusés comportent-ils un indicateur de fiabilité visible ?	Non	Parfois, à la demande	Systématique (3 niveaux min.)	Mis à jour en temps réel
T6. Les sources ouvertes (OSINT) font-elles l'objet d'une vérification forensique formalisée ?	Non	Ponctuellement	Protocole écrit appliqué	Outillé (InVID, TinEye...)

Adapté du modèle CMMI, Charlotte Chuard, 2026

Interprétation des résultats

Majorité en Niveau 1 : vos pratiques sont informelles et dépendent des personnes. Priorité absolue : classification de sensibilité (S1) et fiche d'identité informationnelle (T1). Ces deux actions ne coûtent rien et changent déjà beaucoup.

Majorité en Niveau 2 : vous avez de bonnes habitudes mais peu de choses sont écrites. Priorité : documenter ce que vous faites déjà, désigner une personne responsable et obtenir un accord formel de la direction.

Majorité en Niveau 3 : vous avez des processus formalisés mais ils ne couvrent pas toutes les situations. Priorité : combler les critères encore à « Non » dans les colonnes 2 et 3, et commencer à mesurer l'application réelle des procédures.

Majorité en Niveau 4 : votre dispositif est solide. Votre prochaine étape est d'optimiser (automatisation, benchmark, partage d'expériences avec d'autres organisations).

EXEMPLE Rappel issu de l'enquête

Dans le secteur humanitaire, la maturité informationnelle est davantage corrélée à la spécialisation fonctionnelle qu'à la taille de l'organisation. Une petite structure dédiée à la veille peut atteindre le niveau 4, là où une grande organisation généraliste reste au niveau 1.

5 Fonctionnalités essentielles

Les entretiens conduits dans le cadre de ce travail ont fait émerger cinq fonctionnalités récurrentes, systématiquement citées comme manquantes ou insuffisantes dans les dispositifs actuels. Ces besoins ne sont pas spécifiques à une taille d'organisation : ils ressortent aussi bien des grandes structures que des petites ONG. Le tableau ci-dessous traduit ces besoins en solutions concrètes, différenciées par profil.

Tableau 4, Fonctionnalités essentielles et solutions recommandées par taille d'organisation

Fonctionnalité	Petite structure (< 50 emp.)	Structure intermédiaire (50–250)	Grande organisation (> 250)
Regroupement des informations (toutes sources en un endroit)	Un dossier partagé unique (Drive/SharePoint) avec un sous-dossier par zone d'intervention, alimenté manuellement	Un agrégateur de flux (Feedly) relié au dossier partagé, collecte semi-automatisée	Une plateforme centralisée (intranet ou SharePoint avancé) agrégeant flux, réseaux sociaux et sources internes
Synthétisation avec indication des sources	Une note hebdomadaire rédigée manuellement, avec liste des sources en bas de page	Un template standardisé (Word ou Notion) avec champ source obligatoire et niveau de fiabilité	Un tableau de bord BI (Power BI) affichant automatiquement les synthèses par zone avec liens vers les sources
Veille sur plusieurs niveaux (stratégique / opérationnel / terrain)	Un document en deux sections : contexte général (mensuel) + alertes terrain (à la demande)	Une newsletter bi-hebdomadaire à deux niveaux : résumé stratégique (direction) et notes opérationnelles (équipes)	Des flux distincts par niveau d'utilisateur, configurés dans le système de gestion de contenu interne
Formation et soutien (usage de l'outil et risques)	Une demi-journée d'introduction en interne ; ressources en ligne gratuites (KoBoToolbox Academy, OCHA eLearning)	Formation initiale de 1 à 2 jours + référent interne désigné pour les questions courantes	Programme de formation structuré, intégré à l'onboarding, avec certification interne sur les bonnes pratiques
Gestion et maintenance (sans	Les outils choisis (tableur, Drive) sont	Un administrateur désigné en interne ; les	Une équipe IT interne ou un SLA avec

Fonctionnalité	Petite structure (< 50 emp.)	Structure intermédiaire (50–250)	Grande organisation (> 250)
dépendance externe)	maintenus par les équipes elles-mêmes, sans prestataire	mises à jour sont planifiées semestriellement	prestataire garantissant la continuité de service
Intégration à l'existant (sans doublon ni migration lourde)	L'outil s'appuie sur ce qui existe déjà (SharePoint, Drive) ; seule la structure des dossiers est optimisée	L'agrégateur se connecte aux sources déjà utilisées via RSS ou API ; pas de changement d'environnement	Le nouveau dispositif s'intègre à l'écosystème Microsoft ou Google via des connecteurs natifs

D'après les entretiens, Charlotte Chuard, 2026

L'outil rêvé : ce qu'en disent les personnes interrogées

Quand on interroge les praticiens sur l'outil idéal, trois qualités reviennent systématiquement, dans cet ordre :

« Qu'il ne me demande pas de changer ce que je fais déjà. » La principale raison d'échec d'un nouveau dispositif est la migration : si l'outil impose de quitter SharePoint pour une plateforme inconnue, il ne sera pas adopté. L'outil idéal s'intègre à l'existant.

« Qu'il me dise rapidement ce qui est important. » Face à un volume croissant d'informations, la capacité de synthèse automatisée, même partielle, est perçue comme la fonctionnalité la plus différenciante. La génération de résumés structurés avec liens vers les sources est le cas d'usage le plus cité.

« Qu'il soit simple à former et à maintenir. » Un outil qui dépend d'une seule personne pour fonctionner est un risque organisationnel. L'idéal est un outil que n'importe quel nouveau collègue peut utiliser correctement en une demi-journée.

EXEMPLE L'outil le plus simple et le plus optimal selon votre profil

Petite structure : un tableur partagé structuré (5 colonnes : source / date / résumé / niveau de confiance / niveau de sensibilité) + Google Alert sur 10 mots-clés. Coût : 0 CHF. Mise en place : 1 heure.

Structure intermédiaire : Feedly Pro alimentant automatiquement un dossier SharePoint, avec un template Word de synthèse hebdomadaire. Coût : ~15 CHF/mois. Gain : collecte automatisée, synthèse manuelle conservée pour la valeur ajoutée analytique.

Grande organisation : un tableau de bord Power BI connecté à Sprinklr et à la base de données interne, avec alertes automatiques par zone et par niveau de criticité. Coût : à partir de 2 000 CHF/mois. Gain : réactivité temps réel, couverture globale, mains humaines libérées pour l'analyse.

6 Processus idéal

Cette section répond aux questions pratiques les plus fréquentes sur la mise en place concrète d'un dispositif de veille. Les réponses sont différenciées par taille d'organisation, car les contraintes varient considérablement entre une structure de 8 personnes et une organisation de 1 000 employés.

Tableau 5, Questions de mise en place et réponses par profil d'organisation

Question de mise en place	Petite structure (< 50)	Structure intermédiaire (50–250)	Grande organisation (> 250)
Quelle équipe prévoir ?	1 personne référente (20-30 % du temps) + 1 binôme de secours pour la double validation	1 à 2 personnes dédiées à temps partiel (50 %) + relais identifiés dans chaque antenne terrain	Équipe dédiée (2 à 5 personnes) : analyste, DPO fonctionnel, référent sécurité
Délai de mise en place réaliste	2 à 4 semaines pour les pratiques de base (fiche d'identité, classification, double validation)	1 à 3 mois pour structurer le dossier partagé, former les relais terrain et adapter les outils	3 à 6 mois pour déployer les outils, former les équipes et établir les procédures formelles
Quel coût prévoir ? (indicatif)	0 CHF pour les pratiques de base ; 0–50 CHF/mois si ajout d'un agrégateur freemium (Feedly Pro)	500–2 000 CHF/an pour des outils complémentaires (agrégateur pro, stockage renforcé) + temps interne	5 000–30 000 CHF/an selon le niveau d'outillage (social listening pro, BI, formation certifiante)
Points à valider avec la direction	Accord oral ou e-mail sur : qui est responsable, quel temps est alloué, quelle règle en cas d'incident	Validation formelle si budget impliqué ; charte de veille interne d'1 page signée par la direction	Mandat formel avec objectifs mesurables, budget approuvé et reporting trimestriel à la direction
Transmission par newsletter ?	Non obligatoire : une note mensuelle par e-mail suffit, avec alertes immédiates si besoin urgent	Newsletter bi-hebdomadaire interne recommandée + canal d'alerte rapide (messagerie) pour les urgences	Newsletter hebdomadaire segmentée par niveau (stratégique / opérationnel) + alertes automatisées

Question de mise en place	Petite structure (< 50)	Structure intermédiaire (50–250)	Grande organisation (> 250)
Accès ouvert ou restreint ?	Niveau 1-2 : ouvert à toute l'équipe. Niveau 3-4 : réservé aux décideurs et à la direction uniquement	Niveau 1-2 : ouvert à tous. Niveau 3 : équipe programme + direction. Niveau 4 : direction + DPO uniquement	Gestion des droits par rôle dans le système ; audit log pour les accès aux données de niveau 3-4
Processus interne recommandé	Collecter → noter sur la fiche d'identité → valider à deux → diffuser avec niveau de fiabilité indiqué	Collecter → traiter → valider (double source) → rédiger la synthèse → diffuser via le bon canal selon le niveau	Collecter (auto) → traiter (semi-auto) → analyste valide → DPO vérifie niveau → diffusion par canal calibré

D'après les entretiens et l'enquête, Charlotte Chuard, 2026

Le processus interne pas à pas

Quel que soit le profil de votre organisation, le processus de veille suit les mêmes six étapes. Ce qui varie, c'est le niveau d'outillage et de formalisation à chaque étape. La bonne pratique est de combiner deux logiques complémentaires, plutôt que d'en choisir une :

- **Push (envoi actif) pour l'urgent :** une alerte envoyée directement par e-mail ou messagerie aux personnes concernées dès qu'une information de niveau 3 ou 4 est validée. Les personnes reçoivent l'information sans avoir à la chercher.
- **Pull (accès à la demande) pour le fond :** une newsletter interne hebdomadaire ou mensuelle résumant les évolutions de contexte, accessible à toute personne intéressée via le dossier partagé ou l'intranet.

EXEMPLE Un dispositif qui combine les deux logiques

Une ONG de taille moyenne envoie chaque lundi matin une note de contexte par zone (pull : accessible à tous, disponible dans le dossier partagé). En parallèle, une liste de diffusion restreinte envoie une alerte immédiate via Signal ou par e-mail sécurisé si une information de sécurité de niveau 3 est confirmée un autre jour (push : ciblé, immédiat, pour les personnes concernées uniquement). Les deux canaux ne se concurrencent pas, l'un construit la culture commune d'information, l'autre protège la réactivité opérationnelle.

Ce qui doit être vu avec la direction avant de commencer

Même dans les plus petites structures, trois questions doivent être clarifiées avant de lancer le dispositif, pour éviter qu'il repose sur une seule personne et s'effondre à son départ :

- **Qui est responsable ?** Pas seulement « qui s'en occupe », mais qui répond en cas d'erreur ou d'incident (information fausse diffusée, données compromises).
- **Quelles ressources sont allouées ?** Même sans budget, un accord sur le temps alloué (« 2h par semaine pour cette personne ») évite que la veille soit la première tâche abandonnée quand le planning se resserre.
- **Qui peut autoriser une exception ?** En situation d'urgence vitale, qui peut décider de partager une donnée normalement protégée ? Ce nom doit être connu à l'avance, pas cherché dans l'urgence.

7 Pistes d'évolution, vers un modèle intégré

Les bonnes pratiques présentées dans ce guide sont toutes directement applicables, sans modèle conceptuel particulier. Mais si votre organisation souhaite aller plus loin et formaliser un dispositif de veille qui articule systématiquement sécurité, protection des données et traçabilité, elle peut s'appuyer sur le modèle TRIVAH développé dans le cadre de ce travail.

7.1 Le modèle TRIVAH et comment il répond aux besoins identifiés

TRIVAH (Traçabilité, Résilience Informationnelle, Veille Adaptée à l'Humanitaire) est un modèle conceptuel qui articule trois piliers (sécurité de l'information, protection des données, traçabilité des sources) dans un cycle de veille en six phases, avec des protocoles de décision pour les situations où ces piliers entrent en tension.

Le tableau ci-dessous montre concrètement comment le modèle répond aux besoins identifiés dans l'enquête :

Tableau 6, Correspondance entre les besoins terrain et les réponses du modèle TRIVAH

Besoin identifié sur le terrain	Ce que le modèle TRIVAH prévoit	Comment le mettre en place concrètement
Urgence opérationnelle vs. rigueur (67 % citent ce facteur)	Diffusion progressive avec indicateur de confiance : on diffuse immédiatement mais en indiquant le niveau de fiabilité, sans bloquer l'action	Adopter la convention à 3 niveaux (non vérifié / partiellement vérifié / vérifié) sur tous les canaux de diffusion internes
Désinformation sous-protocolarisée (56 % risque perçu, 33 % protocole)	Validation en 3 temps : vérification automatique, triangulation inter-sources, validation tertiaire humaine	Démarrer par la règle simple : aucune information sensible ne sort sans au moins 2 sources indépendantes
Dépendance aux outils tiers sans chiffrement (56 %)	Classification à 4 niveaux avec hébergement différencié : les données les plus sensibles ne vont pas dans le cloud commercial	Identifier les 10 % de données les plus sensibles et les déplacer sur un espace sécurisé (serveur interne ou dossier chiffré)
Budget contraint (100 % des répondants)	Profil d'entrée niveau 1-2 : fiche d'identité + double validation + SharePoint existant = 0 CHF de coût additionnel	Démarrer sans rien acheter de nouveau ; ajouter des outils uniquement quand les bases humaines et procédurales sont en place

Besoin identifié sur le terrain	Ce que le modèle TRIVAH prévoit	Comment le mettre en place concrètement
Aucune politique de destruction (lacune universelle dans l'enquête)	Phase 6 du cycle TRIVAH : destruction documentée, vérification trimestrielle, registre des traitements	Créer un tableau de bord simple avec les dates de révision par type de données (à ajouter dans le dossier veille existant)

Charlotte Chuard, 2026

7.2 Les éléments à prendre en compte pour une mise en place

Former avant d'outiller. L'erreur la plus fréquente est d'acquérir un nouvel outil avant que les équipes ne comprennent pourquoi elles le font. Une demi-journée de formation aux risques informationnels de base a un impact supérieur à n'importe quel logiciel acheté sans préparation.

Construire dès le départ, pas réparer après. Introduire un système de traçabilité ou de classification après que les pratiques sont déjà installées est beaucoup plus difficile que de l'intégrer dès le début. Si vous mettez en place un nouveau dispositif, c'est le bon moment pour intégrer les bonnes pratiques de ce guide.

Constituer un groupe de travail transversal. Un dispositif de veille touche à plusieurs fonctions : analyse, sécurité informatique, juridique (RGPD), terrain. Réunir ces compétences dès la conception évite les angles morts et les résistances lors du déploiement.

Progresser par niveaux, pas d'un coup. La grille d'auto-évaluation (chapitre 4) est conçue pour vous permettre de définir votre prochain niveau réaliste, pas le niveau idéal abstrait. Passer du niveau 1 au niveau 2 sur les 18 critères est déjà une transformation significative.

Anticiper le coût de la transition. Le temps et le budget nécessaires pour passer d'une pratique informelle à un processus documenté sont souvent sous-estimés. Prévoir une phase de transition de 1 à 3 mois selon la taille de votre organisation, pendant laquelle les deux systèmes coexistent.

7.3 Les prochaines étapes si vous voulez aller plus loin

Pour une mise en œuvre complète du modèle TRIVAH, le travail de Bachelor qui a nourri ce guide détaille l'ensemble des protocoles, critères et outils. Les organisations souhaitant un accompagnement peuvent prendre contact avec l'auteure.

8 Pour aller plus loin

Ce guide constitue une synthèse pratique conçue pour la diffusion directe auprès des organisations du secteur. Il s'appuie sur un travail de recherche plus complet qui détaille la méthodologie, l'intégralité des résultats d'enquête, le modèle conceptuel complet et sa validation par confrontation à des cas réels et par benchmark avec les cadres existants (OCHA, CICR, IFRC, ACAPS).

Ressources complémentaires recommandées

- **CICR, Handbook on Data Protection in Humanitarian Action (2024) :** référence sectorielle sur la protection des données en contexte humanitaire.

- **IFRC, Data Playbook :** guide pédagogique sur la gestion des données pour les Sociétés nationales de la Croix-Rouge, adapté aux contextes à faibles ressources.
- **OCHA, Centre for Humanitarian Data (humdata.org) :** ressources sur les standards HDX/HXL et la gestion responsable des données humanitaires.
- **KoBoToolbox Academy (support.kobotoolbox.org) :** formation gratuite à la collecte de données terrain, en plusieurs langues.