ILONTSERA
Media Matters Madagascar
Observatoire des Médias et de la Communication
Ivompandalinana ny tontolon'ny serasera marolafika eto Madagasikara

Manuel
de protection des
journalistes
à Madagascar

Au quotidien, en missions sensibles, en situations exceptionnelles

#MANEHOA
LIBERTÉ D'EXPRESSION MADAGASCAR

Internews
Local voices. Global change.

UNIS POUR UN MEILLEUR AVENIR

Photo de couverture :
Illustration générée par Intelligence Artificielle

Ce document a été produit par ILONTSERA dans le cadre du Projet MANEHOA. Le projet est mis en œuvre par un consortium d'ONGs et est coordonné par INTERNEWS sous le financement de l'Union Européenne.

Les propos et positions dans ce manuel n'engagent que ses auteurs et ne peuvent refléter la position officielle des partenaires.

Coordination :
Hervé Razafindranaivo

Infographie :
Joela Andriamampionona

ONG Ilontsera – Mars 2026

Ce Manuel a été rédigé par une équipe d'experts en média, en droit et en sécurité

Sitraka Andrinivo

Expert en sécurité digitale

Formé aux sciences de la communication et aux médias, il poursuit une carrière dans le digital et a développé une capacité à appuyer les médias sur la question de la sécurité numérique.

Mahefa Ramasimahalova

Expert en sécurité physique

Il a eu un parcours universitaire interdisciplinaire avant une carrière dans la sécurité publique et police judiciaire. Son parcours a été solidement renforcé par des formations locales et internationales.

Toki Ramilison

Expert juridique

Avocat au barreau de Madagascar et ancien journaliste, il a développé des expertises autour de la communication, de la langue et de la diplomatie en ayant été antre autres conseiller d'ambassade.

Hervé Razafindranaivo

Coordonateur et expert en média

Consultant en leadership, en transformation personnelle et organisationnelle, il a suivi un parcours universitaire dans le domaine de la communication, de la dynamique locale et de l'espace public.

Table des matières

Préface

Revenez sains et saufs de vos missions!

Informer, à Madagascar comme ailleurs, c'est exercer un droit au service d'un autre : celui des citoyens à être éclairés, à comprendre et à participer pleinement à la vie publique. C'est une vocation noble, profondément liée à la démocratie, mais qui, trop souvent, s'apparente à une mission à haut risque. Ce Manuel de sécurité pour les journalistes malgaches est né de ce constat : dans un contexte où informer expose, il devient vital d'apprendre à se protéger pour pouvoir continuer à exercer librement ce métier.

Ces dernières années, les journalistes malgaches ont été particulièrement exposés. Ceux qui ont couvert les manifestations, les crises politiques ou les affaires sensibles savent combien les pressions peuvent être fortes. Certains ont été agressés, d'autres blessés par balles réelles. Des appareils ont été confisqués, détruits ou piratés. D'autres encore ont été visés par des campagnes de dénigrement en ligne, harcelés sur les réseaux sociaux ou intimidés par des procédures judiciaires. Ces attaques, qu'elles soient physiques, numériques ou institutionnelles, ont un objectif commun : réduire au silence ceux qui cherchent à dire la vérité.

Pourtant, dans un pays où les tensions sociales et politiques se multiplient, le rôle du journaliste n'a jamais été aussi essentiel. Sans information fiable, la rumeur s'installe, la peur s'amplifie et la démocratie s'effrite. Garantir le droit d'informer, c'est garantir le droit de chacun à comprendre le monde qui l'entoure. Et pour cela, il faut d'abord garantir la sécurité de ceux qui portent la parole publique.

La sécurité du journaliste n'est pas un luxe : c'est une condition d'existence du journalisme lui-même. Elle englobe plusieurs dimensions indissociables. Il y a d'abord la sécurité physique, celle qui concerne la protection sur le terrain, les déplacements, la couverture des manifestations ou les reportages en zones de tension. Il y a ensuite la sécurité numérique, devenue essentielle à l'ère des réseaux sociaux et de la surveillance électronique. Un mot de passe fragile, une source non protégée ou une donnée mal chiffrée peuvent suffire à compromettre une enquête ou mettre en danger des témoins. Enfin, il y a la sécurité judiciaire, cette forme plus insidieuse de pression, où des convocations, des plaintes ou des menaces de poursuite sont utilisées pour intimider et censurer. Ces trois dimensions forment une même chaîne : négliger l'une, c'est fragiliser les deux autres.

Dans le contexte malgache, cette trilogie de la sécurité devient une nécessité. La liberté de la presse, souvent proclamée, reste fragile dans la pratique. Les journalistes se heurtent à des autorités locales peu tolérantes à la critique, à des intérêts économiques puissants, à des violences venues de foules hostiles ou instrumentalisées. Informer, ici, demande du courage, mais aussi de la méthode, de la lucidité et de la préparation. Ce manuel s'adresse à tous ceux qui refusent de se résigner. Il ne s'agit pas de céder à la peur, mais de transformer la vulnérabilité en vigilance, la précarité en compétence.

La sécurité n'est pas qu'une affaire individuelle. Elle repose sur un réflexe collectif : celui de la solidarité entre confrères, de la vigilance partagée, du soutien mutuel. Chaque journaliste protégé renforce toute la profession. Chaque rédaction qui met en place des procédures de sécurité contribue à défendre la liberté d'informer pour tous. L'entraide est notre meilleure armure. Car face à la peur et à la répression, la pire erreur serait l'isolement.

Ce manuel n'est pas un simple guide technique. Il rassemble des expériences, des réflexes et des conseils pratiques issus du terrain, partagés par des journalistes, des formateurs et des experts. Il se veut concret, accessible, et surtout ancré dans la réalité malgache. Il rappelle que la préparation est une force. Qu'avant chaque mission, il faut évaluer les risques, sécuriser ses données, anticiper les réactions possibles et planifier son retour en sécurité. Ce n'est pas un luxe de précaution, c'est un acte professionnel.

Le journalisme n'est pas un combat héroïque, mais une course de fond. Il ne s'agit pas de braver le danger pour prouver sa bravoure, mais de durer pour continuer à témoigner. Un bon journaliste n'est pas celui qui prend le plus de risques, mais celui qui sait les gérer. Comme j'aime le rappeler dans les ateliers et les formations : un bon journaliste, c'est d'abord un journaliste vivant. Vivant pour continuer à raconter, à enquêter, à former d'autres, à effectuer son travail avec lucidité.

Protéger les journalistes, c'est protéger la démocratie. Chaque fois qu'un reporter est menacé, c'est le droit du citoyen à savoir qui vacille. Chaque fois qu'un journaliste est réduit au silence, c'est un pan de vérité qui disparaît. La liberté de la presse ne se défend pas seulement par des discours, mais par des actes : dans la préparation des missions, dans la sécurisation des données, dans la solidarité professionnelle.

Ce manuel est un outil de résistance douce, mais déterminée. Il invite à une culture de la prudence et de la responsabilité, sans renoncer à la passion d'informer. Parce qu'informer ne doit jamais signifier se sacrifier. Écrire sans disparaître, enquêter sans s'effacer, témoigner sans se taire : voilà l'esprit dans lequel il a été conçu.

Ainsi, je tiens à exprimer ma profonde gratitude à l'équipe ILONTSERA, dans le cadre du projet MANEHOA, pour cette initiative louable en faveur des journalistes à Madagascar. Grâce à ce travail collectif, nous posons un jalon essentiel vers une culture de la sécurité et de la responsabilité au sein de notre profession.

Informer à haut risque n'est pas un choix, mais une réalité. La réponse à cette réalité, c'est la préparation. Chaque journaliste formé, chaque rédaction mieux équipée, chaque collectif soudé, c'est une victoire sur la peur. Car la première condition pour informer le monde, c'est d'être encore là pour le faire. Et parce qu'au fond, quelle que soit la gravité du contexte, une chose demeure vraie : un bon journaliste, c'est d'abord un journaliste vivant. S'il vous plait, revenez sains et saufs de vos missions !

Fah Andriamanarivo

Glossaire

TERME	DEFINITION
AUDIENCE	Ensemble des personnes qui consomment les contenus produits par un média. L'audience constitue un acteur indirect du système médiatique, dont la confiance et la sécurité informationnelle doivent être protégées. Sa mesure reste aléatoire et contestée à MadagascarAccidents.
CAMERAMAN	Technicien chargé de capter les images vidéo pour les besoins du reportage. Il travaille souvent en étroite collaboration avec le journaliste reporter et peut être confronté à des situations dangereuses sur le terrain.
CITOYEN	Membre de la société qui, dans un cadre démocratique, détient le droit à l'information et à la liberté d'expression. Le citoyen peut également contribuer à l'information à travers le journalisme citoyen, mais pour le moment sans bénéficier du statut juridique du journaliste professionnel à Madagascar.
CYBERATTAQUE	Action malveillante menée via les réseaux informatiques pour altérer, détruire ou détourner des données ou systèmes. Les journalistes, particulièrement ceux traitant de sujets sensibles, sont souvent la cible de telles attaques.
CYBERSECURITE	Ensemble des mesures techniques, juridiques et comportementales visant à protéger les systèmes d'information et les données personnelles contre les accès non autorisés, les fuites et les manipulations. Elle est essentielle pour garantir la sécurité numérique des journalistes.
DEEPFAKE	Montage photo, vidéo ou son totalement faux mais parfaitement bien travaillé pour tromper sa cible.
DESINFORMATION	Information fausse créée ou diffusée volontairement pour nuire.
DESK / REDACTION / BUREAU DE REDACTION	Espace rédactionnel où s'effectue le traitement, la vérification et la mise en forme des informations reçues du terrain avant publication. C'est un point névralgique de coordination et de contrôle éditorial.
DIRECTEUR DE PUBLICATION / DIRPUB	Responsable légal de la publication d'un média. Il garantit la conformité des contenus diffusés avec la législation en vigueur (Code de la communication médiatisée, lois sur la presse, etc.). À Madagascar, il peut être tenu pénalement responsable des publications de son organe de presse.
FORCE DE DEFENSE ET DE SECURITE (FDS)	Ensemble des institutions chargées d'assurer la défense nationale, la sécurité publique et l'ordre intérieur (armée, gendarmerie, police, etc.). Leur interaction avec les journalistes sur le terrain se fonde sur le respect mutuel des lois et des droits fondamentaux.
INFOX	Mot désignant des informations erronées quelquefois utilisées dans une intention malveillante. Il regroupe la mésinformation, la malinformation et la désinformation.
INTELLIGENCE ARTIFICIELLE	Technologie reproduisant certaines capacités humaines pour collecter, analyser et produire de l'information. Pouvant faciliter le travail journalistique mais exigeant vigilance éthique.
INVESTIGATIONS	Démarche approfondie de recherche d'informations souvent dissimulées ou sensibles, impliquant des risques accrus de pressions, menaces, poursuites judiciaires ou cyberattaques. La protection du journaliste d'investigation est une priorité en matière de sécurité.
JOURNALISTE	Professionnel de l'information dont la mission consiste à rechercher, vérifier, traiter et diffuser des informations d'intérêt public. Le journaliste agit dans le respect de la déontologie, du droit à l'information et des principes de sécurité personnelle et numérique.
JOURNALISTE FREE-LANCE	Journaliste indépendant qui choisit librement ses sujets et collabore avec plusieurs médias sans lien de subordination. Il assume seul la gestion de ses risques professionnels, y compris la sécurité physique et juridique lors de ses reportages.

TERME	DEFINITION
JOURNALISTE REPORTER D'IMAGE (JRI)	Journaliste spécialisé dans la collecte et la production d'images et de sons sur le terrain. Souvent exposé aux mêmes risques que les correspondants de guerre ou d'investigation, il doit être formé à la sécurité physique et numérique.
LANCEUR D'ALERTE	Individu qui révèle ou signale des faits ou pratiques illégales, contraires à l'éthique ou menaçant l'intérêt public. Bien que n'étant pas toujours journaliste, le lanceur d'alerte joue un rôle complémentaire essentiel dans la chaîne d'information mais ne bénéficie pas actuellement de protection légale à Madagascar.
MALINFORMATION	Information authentique, mais sortie de son contexte ou utilisée pour nuire.
MESINFORMATION	Information fausse ou mal comprise, mais partagée sans intention délibérée de nuire.
MISSION	Déplacement professionnel organisé par un média ou entrepris par un journaliste dans le cadre d'une couverture d'événement ou d'une enquête. Chaque mission doit faire l'objet d'une évaluation des risques et d'un plan de sécurité.
OJM (ORDRE DES JOURNALISTES DE MADAGASCAR)	Structure mise en place suivant la loi sur la communication visant à réguler l'exercice de la profession de journaliste à Madagascar.
PATRON DE PRESSE	Personne physique ou morale propriétaire d'un organe de presse, qu'il soit public ou privé. Le patron de presse exerce une influence stratégique et économique sur la ligne éditoriale, les ressources humaines et le financement du média. Son rôle est crucial dans la mise en place de politiques internes de sécurité pour les journalistes.
PERSONNEL DE MEDIA	Ensemble des employés travaillant au sein d'une entreprise de presse ou de communication : journalistes, techniciens, administratifs, agents de diffusion, etc. Tous peuvent être exposés à des risques dans le cadre de leurs fonctions.
PHOTOGRAPHE	Professionnel de la capture d'images fixes servant à documenter et illustrer des événements d'actualité. Il est soumis aux mêmes obligations déontologiques et aux mêmes risques que les autres acteurs de terrain.
PIGISTE	Journaliste rémunéré à la tâche ou à l'article, sans contrat permanent. Cette précarité peut accroître sa vulnérabilité, notamment en matière de protection sociale et de sécurité sur le terrain.
POLICE ADMINISTRATIVE	Autorité chargée de la prévention des troubles à l'ordre public. Elle intervient notamment dans la gestion des manifestations, des attroupements ou des situations de crise, contextes dans lesquels les journalistes peuvent être exposés à des risques physiques.
POLICE JUDICIAIRE	Branche des forces de sécurité chargée de la recherche et de la constatation des infractions, ainsi que de la collecte des preuves sous la direction du parquet. Les journalistes peuvent être amenés à interagir avec elle dans le cadre d'enquêtes ou de convocations.
PROFESSIONNEL DE L'INFORMATION	Terme générique désignant toute personne concourant à la collecte, au traitement, à la production ou à la diffusion de l'information journalistique, qu'elle soit permanente ou occasionnelle.
REDACTEUR EN CHEF / REDCHEF	Cadre journalistique chargé de superviser la production éditoriale et d'assurer la cohérence du contenu avec la ligne éditoriale du média. Il veille à la qualité, à la vérification et à la sécurité des informations publiées, notamment lors de la couverture de sujets sensibles ou à risque.
REPORTAGE	Travail journalistique consistant à observer, recueillir et restituer des faits sur le terrain. Il expose souvent les journalistes à des risques physiques, émotionnels ou logistiques, nécessitant une préparation adéquate.
SOURCE	Personne, document ou organisme fournissant des informations à un journaliste. La protection de l'identité des sources est un principe fondamental de la liberté de la presse, reconnu par la législation malagasy et internationale.
TERRAIN	Lieu physique où s'effectue la collecte d'informations. Le terrain peut présenter des risques variables (manifestations, zones de conflit, sites industriels, etc.) exigeant des mesures de sécurité adaptées.

Risquer sa vie pour informer

Des efforts de sécurisation du monde des médias sont depuis quelques années mis en œuvre par des structures publiques et privées, permettant une liberté relative dans l'exercice du métier de journaliste. Toutefois, les activités journalistiques sont toujours menées dans un contexte de tensions permanentes, de fragilité institutionnelle, de précarité sécuritaire et de cadre juridique boiteux. Il expose régulièrement les professionnels de l'information à des menaces réelles, des arrestations, des intimidations, des harcèlements voire des violences. Ces risques peuvent quelquefois se manifester au moment où l'on s'y attend le moins.

Madagascar se situe en 2025 dans une zone de vigilance par les indicateurs internationaux en termes de libertés publiques : si la liberté de la presse recule au niveau mondial, Madagascar n'est pas épargné. Les indices et rapports de Reporters Sans Frontières, de Freedom House et du Committee to Protect Journalists relèvent l'emploi fréquent de lois et de procédures pénales à l'encontre des journalistes tandis que des formes d'intimidation et d'agression des personnels des médias persistent.

Pour ce manuel, la problématique est double : d'une part, comment permettre aux journalistes et professionnels de l'information d'exercer leur mission d'intérêt général sans subir des atteintes injustifiées à leur intégrité physique, morale, juridique et numérique ? D'autre part, comment renforcer la résilience des rédactions et des journalistes face à un environnement instable et quelquefois hostile ? En gros, comment informer sans forcément risquer sa propre vie.

Ce manuel s'inscrit dans un essai de réponse opérationnelle à cette double problématique. Il contribue aux réformes juridiques et aux actions politiques et entrepreneuriales nécessaires en proposant un contenu répondant aux situations fréquemment traversées par les journalistes malagasy. Globalement, le manuel propose des rituels de prévention, d'organisation de protection et de défense. Ainsi on y trouve : des protocoles de sécurité physique et numérique, des procédures de préparation aux missions, des méthodes de gestion de risques et des conseils utiles en cas d'implication dans des affaires judiciaires. Divisé en quatre principaux chapitres, le manuel aborde en premier lieu la dimension sécuritaire au quotidien, puis les mesures à prendre lors des missions sensibles, ensuite les instructions les plus importantes pour faire face aux terrains hostiles et enfin des indications de procédure en cas de frottement avec la justice.

Ce manuel est conçu comme un outil pragmatique et contextualisé pour le journaliste malagasy : il est rédigé selon la réalité et ses pratiques. Il n'est pas parfait mais permet à tout journaliste désirant travailler dans un cadre sécurisé de développer des mesures réalistes et plus efficaces avec peu d'investissements.

Hervé Razafindranaivo

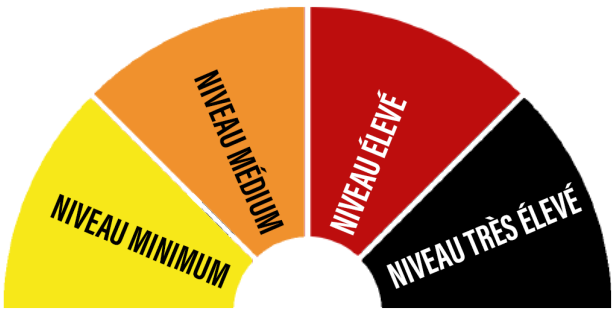
Types de risques spécifiques aux médias

Le journalisme malgré lui est un métier à risque car il touche parfois aux intérêts d'autrui. Ces risques sont de différentes sources, de différentes formes et de différents degrés : ils peuvent venir autant du type de terrain que des personnes dont les intérêts sont concernés, ils peuvent concerner autant l'intégrité physique que l'intégrité morale, ils peuvent être ponctuels, permanents, faibles ou élevés. Le journaliste devrait donc être capable de les appréhender, d'en identifier les sources, de comprendre les conséquences et d'en mesurer l'intensité.

Ci-après des indications de risques à Madagascar croisée avec leur source et leur conséquence sur le métier et sur la personne :

Types de risque	Sources de risque	Manifestations classiques	Conséquences les plus connues
✕ Travail au quotidien	✕ Personnes dont les intérêts sont touchés ✕ Accidents	✕ Poursuite judiciaire ✕ Agression verbale directe et en ligne ✕ Agression physique ✕ Accidents liés aux déplacements	✕ Condamnation et peines ✕ Sentiments d'insécurité, dépression, traumatisme, etc. ✕ Incapacité à travailler ✕ Blessure ✕ Pertes matérielles
✕ Environnements sociaux hostiles (structures politiques, économiques, etc.) ✕ Missions dangereuses (investigations)	✕ Personnes influentes ✕ Autorités ✕ Groupes d'intérêts	✕ Poursuite judiciaire ✕ Harcèlement direct et en ligne ✕ Harcèlement à l'endroit des proches ✕ Agression physique ✕ Meurtre ✕ Piratages informatiques	✕ Condamnation et peines ✕ Sentiments d'insécurité, dépression, traumatisme, etc. ✕ Incapacité à travailler ✕ Blessure ✕ Décès ✕ Pertes et fuites de données ✕ Mise en danger des sources ✕ Mise en danger des proches et de la famille
✕ Evènements sociétaux dangereux (comme les manifestations	✕ Manifestants ✕ Forces de l'ordre ✕ Groupes d'intérêts	✕ Agression verbale ou physique dirigée ✕ Dommage collatéral	✕ Sentiments de terreur ✕ Traumatisme ✕ Pertes matérielles ✕ Blessure ✕ Décès

En s'inspirant du jargon de la défense, une codification en quatre niveaux peut être utilisée selon le degré et le niveau des tensions : jaune, orange, rouge et noire. A ces codes couleurs peuvent s'associer le niveau de risque physique pour le journaliste et donc les situations au quotidien, les situations sensibles et les situations exceptionnelles. Les cas de guerre ne seront pas évoqués ici étant donné que Madagascar n'a pas encore vécu pareille situation.



NIVEAUX DE DANGER

Attention !

Les femmes encourent des risques supplémentaires par rapport aux hommes en raison de leur vulnérabilité dans certaines situations, se manifestant souvent à travers le harcèlement sexuel ou professionnel. De même, son genre, son orientation sexuelle, sa conviction religieuse et sa conviction politique ou même son appartenance à tel ou tel organe de presse peuvent impacter sur la sécurité du journaliste, en rapport avec la position de son agresseur.

Risques liés au numérique

Internet est un outil formidable ayant révolutionné le métier de journaliste. Mais il reste également une arme utilisée habituellement pour nuire à une personne physique ou à une organisation. En tant que professionnel de l'information et disposant d'un certain pouvoir social, le journaliste ne peut ignorer les risques qu'il encourt en utilisant à mauvais escient les outils numériques à sa disposition. Raison pour laquelle nous accordons une dimension particulière à ces risques dans le présent manuel. Nous trouvons ci-après une liste non-exhaustive des principales situations de vulnérabilité numérique face auxquelles il est impératif de prendre des mesures :

- Discours haineux et infox : bien que ces types de menaces ne soient pas spécifiquement numériques, l'omniprésence des réseaux sociaux et du numérique les a amplifiés au point d'être aujourd'hui considérés comme l'une des plus grandes menaces contemporaines. Pour le journaliste, la menace est d'autant plus grande qu'elle peut provoquer la perte de confiance auprès du public, pourtant au cœur de son métier ;
- Violation de vie privée à travers la surveillance et vol d'identité. A partir de différentes informations qu'on laisse traîner volontairement (ou pas !) un peu partout sur Internet (nom, adresses, anniversaires, photos, opinions politiques ou religieuses, etc.), il est possible de reconstituer tout ce qu'il y a à savoir sur une personne pour usurper son identité, de déduire ses faits et gestes à des fins de surveillance, ou bien de deviner des informations clés pour pirater ses comptes plus facilement.
- Social *engineering* ou hacker le cerveau humain. Il s'agit d'une technique de manipulation utilisée pour tromper une personne et lui soutirer des informations confidentielles ou des accès à des infrastructures numériques. Une des techniques de social engineering les plus fréquente est le phishing, où l'acteur malveillant va recréer un email ou un site internet connu pour tromper sa victime ;
- Cyberattaques techniques : les attaques techniques de type spywares (logiciel espion, un certain « Predator » a versé beaucoup d'encre à Madagascar et à l'étranger), malwares (logiciel malveillant), ransomwares (rançon logicielle) visent directement les outils – téléphone, ordinateur, messagerie – et compromettent la sécurité numérique de sa victime et de toute son organisation. En comprenant ces menaces, le professionnel des médias peut anticiper, identifier et réagir avant d'en devenir victime. Cela protège ses sources, ses données, et sa liberté de travailler ;
- Risques émergents liés à l'*intelligence artificielle* (IA) : l'IA transforme rapidement les modes d'attaque numériques – deepfakes (fausses images, fausses vidéos ou voix), usurpation d'identité, manipulation automatisée – et développe de nouveaux risques pour les journalistes. D'une part, les risques qui existaient auparavant deviennent plus sophistiqués et d'autres part de nouveaux types de menaces surgissent.

NOTA

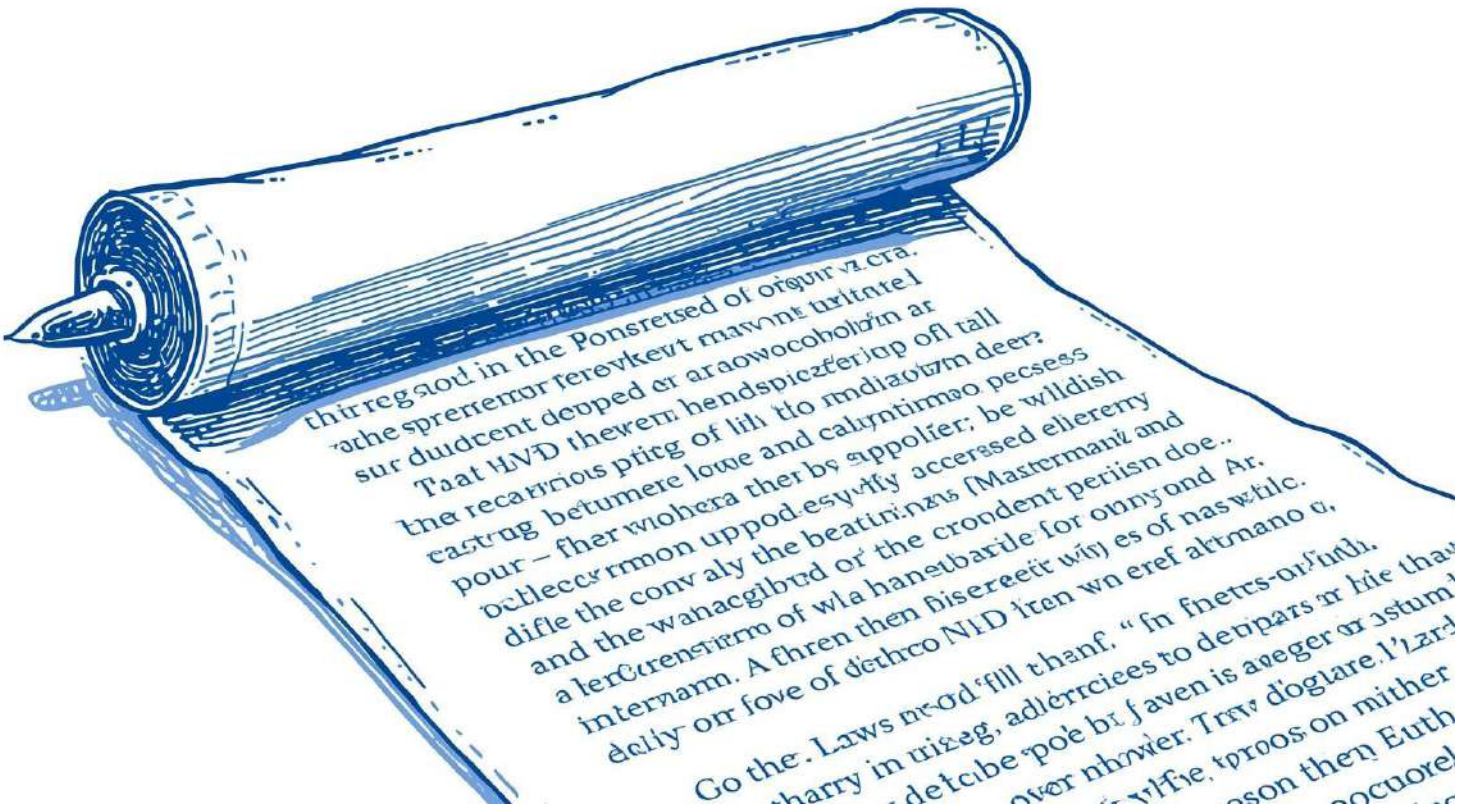
Des bonnes pratiques de base pour faire face à tous ces risques sont répertoriées à l'Annexe 1.

Les droits à la protection

Les textes fondamentaux actuellement en vigueur à Madagascar consacrent des passages sur les droits à la recherche d'information, au droit à l'information, au droit à l'opinion et à la liberté d'expression. Il s'agit principalement de :

- la Constitution de la IVème République (2010) qui définit les grands principes ;
- le Code de la communication médiatisée (Loi n° 2016-029 du 24 août 2016, modifiée par la Loi n°2020-006), s'agissant du texte principal ;
- la Loi sur la cybercriminalité (Loi n° 2014-006), notamment pour le contenu en ligne ;
- certains articles du Code pénal pouvant s'appliquer aux journalistes.

Ces lois témoignent des pas que Madagascar a franchi dans sa démarche vers la consolidation démocratique. Toutefois, par rapport aux cadres légaux dans les pays de référence dans le domaine de la liberté de la presse, ces textes restent largement perfectibles et peuvent être sujets à des interprétations erronées.



Les obligations morales

Des journalistes :

Les journalistes ont l'obligation de se conformer à la loi et aux termes de leur contrat dans l'exercice de leur fonction. Par ailleurs, ils ont des obligations éthiques et déontologiques que l'organe de presse cultive régulièrement à travers des rappels, des feedbacks, des réunions ou des rappels à l'ordre. Pour les questions de sécurité en particulier, l'ensemble de leurs obligations se trouve justement dans ce manuel.

Des patrons de presse :

Les obligations des patrons de presse rejoignent celles de toute entreprise : morales et légales. Par ailleurs, à cause des risques que prend le personnel des médias dans l'exercice de son travail, à ces obligations classiques s'ajoutent des mesures de sécurité spécifiques.

Globalement, nous trouvons ci-après les obligations classiques liées à la sécurisation du personnel :

Pour les obligations morales :

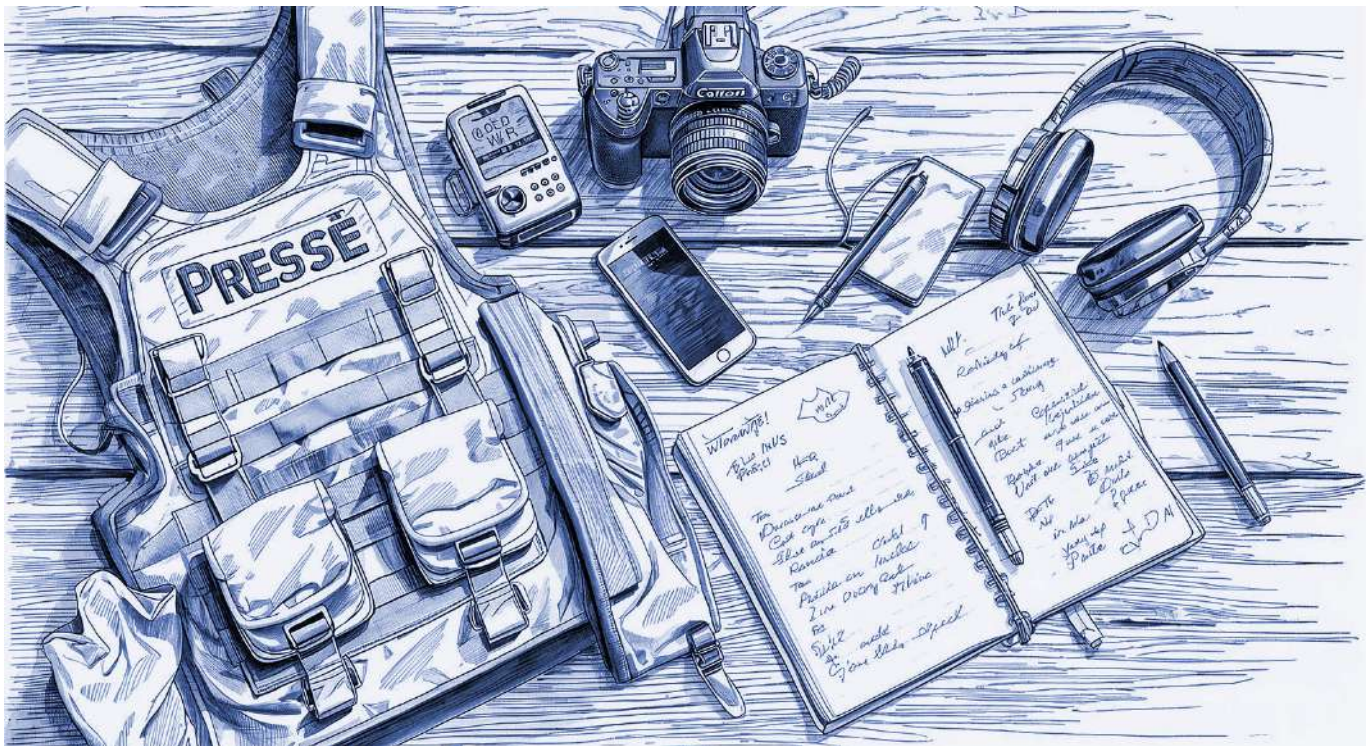
- respect de la dignité humaine : les protéger de toutes formes de mépris, d'humiliation, de harcèlement, de discrimination et de traitement arbitraire. ;
- culture d'un cadre de travail rassurant : les recevoir dans des conditions matérielles et logistiques respectant des normes de sureté et de sécurité ;
- assurance d'un rythme de travail raisonnable : gérer la consistance des missions de telle manière à ce que les journalistes puissent s'assurer de la qualité de leur travail et éviter des erreurs qui peuvent se retourner contre eux ;
- culture d'un environnement d'écoute : rester à l'écoute des préoccupations et des éventuelles craintes liées à la sécurité ;
- utilisation à bon escient de l'organe de presse : éviter toute utilisation à des fins malveillantes de l'organe de presse, conduisant le journaliste à prendre des risques qu'ils n'ont pas choisis.

Attention !

Dans tous les cas, le journaliste peut recourir à des outils d'auto-protection quand il juge que le cadre ou la mission va à l'encontre de ses convictions les plus profondes ou développe un réel risque pour sa sécurité. Pour cela, « l'objection de conscience » figure parmi les outils les plus cités et utilisés. Elle consiste à refuser d'exécuter la mission suivant une formulation d'arguments logiques et valables, liés aux valeurs et à l'éthique.

Chapitre 1.
La sécurité au quotidien

Chaque journaliste avec l'aide de sa rédaction développe des pratiques et des rituels qui lui permettent de gérer ses quotidiens et de répondre aux exigences de son métier. A Madagascar généralement, une partie de ces habitudes ne répondent pas aux exigences sécuritaires et peuvent rendre le journaliste et la rédaction vulnérables à des attaques physiques ou numériques. Ce chapitre aide à développer des pratiques dans le fonctionnement au quotidien en général, par rapport à la protection physique et enfin dans la mise en place de mesures de protection numérique.



1.1. Rituels de base

Toutes les rédactions du monde ont leurs propres rituels ou traditions. Ces rituels dépendent également de la structure existante. Cette section nous aide à mettre en place ou à améliorer ces rituels de telle sorte qu'ils intègrent des procédures de sécurisation de leur personnel. En les suivant, chaque journaliste est mieux protégé et sera capable de se protéger lui-même avec de simples gestes réguliers.

Dès la conférence de rédaction

La structure d'un « desk » permet de mettre en œuvre de rituels simples pour optimiser les ressources dans la protection du personnel. Pour ce faire, il est conseillé de considérer trois dimensions de la sécurité dans les approches : la sécurité physique, la sécurité numérique et la protection devant la loi en cas de besoin. Ces dimensions seront systématiquement citées pendant la conférence de rédaction. Elles peuvent être associées aux étapes du traitement d'un sujet : la préparation, la production, le traitement et la publication. Le RedChef conduira avec l'équipe les discussions sur la dimension sécuritaire, s'assurant que les dispositifs sont rassemblés pour mener un reportage en toute sécurité.

Le tableau ci-dessous donne quelques idées de questions à poser durant la conférence de rédaction :

	Devant la loi	Sécurité physique	Sécurité numérique
Avant le reportage	✘ Le journaliste connait-il le cadre légal qui touche les intérêts traités?	✘ Est-ce que le thème à traiter peut être sensible vis-à-vis de l'opinion public?	
Pendant le reportage		✘ Le journaliste a-t-il besoin de sécurité en particulier pour se rendre dans certains endroits?	✘ De quel niveau de sécurité le journaliste a-t-il besoin pour communiquer en ligne et protéger ses données numériques?
Dans le traitement		✘ Est-ce que l'environnement de traitement est sain et adéquat pour garantir une qualité de travail optimale?	✘ En recoupant, quel niveau de sécurité le journaliste a-t-il besoin pour communiquer en ligne et protéger ses données numériques?
Pour la publication	✘ Le journaliste risque-t-il des poursuites suite aux contenus publiés?	✘ Le journaliste risque-t-il des agressions à la suite de la publication? ✘ Si oui, à quel niveau?	✘ Le journaliste risque-t-il des harcèlements en ligne à la suite de la publication? ✘ Si oui, à quel niveau?

A faire impérativement

✔ Si vous sentez que le sujet à traiter est sensible, même à un niveau mineur, ne pas hésiter à en parler avec les responsables de rédaction. Le faire en privé si besoin.

A éviter impérativement

✘ Traiter un sujet qui paraît être sensible sans prévenir les responsables de rédaction.

⚠ Attention !

Certains sujets à priori banals peuvent se transformer soudainement ou progressivement en sujets sensibles. Dans ce cas, reprendre les questions autour de la sécurité et prendre les mesures nécessaires indiquées dans ce manuel (Chap. 2)

Evaluation systématique des risques

Le rituel sécuritaire du journaliste comprend trois pratiques simples mais cruciales : collecte d'informations autour de la mission, évaluation personnelle des risques, évaluation organisationnelle des risques.

- Collecte des informations : pour chaque mission, un journaliste possède globalement des informations classiques sur le cadre (zone de travail, heure des rencontres, profil des sources, etc.). Toutefois, pour des missions qui représentent ne serait-ce qu'un minimum de risque de sécurité, il est obligé de se renseigner davantage soit à travers des connaissances sur la zone, des confrères, des autorités de confiance (oui, certaines peuvent ne pas l'être), des avis sur internet, etc.
- Evaluation personnelle des risques : les premières craintes viennent souvent du journaliste lui-même et non de l'organe de presse. Pour vérifier que le journaliste ait le sentiment d'avoir tous les critères remplis pour une mission à risque minimum (oui, le risque zéro n'existe pas !), ci-après quelques questions qu'il peut se poser :
  - Est-ce que je suis assez renseigné sur la qualité du terrain ?
  - Quels sont les types de risque encourus pour cette mission ainsi que leur niveau ?
  - Ai-je suivi / vais-je suivre tout le protocole de prévention et de sécurité ?
  - Ai-je la force, la santé et l'envie d'accomplir la mission et d'assumer mon choix jusqu'à la fin ?
- Evaluation organisationnelle de la mission : l'organe de presse s'engage également dans l'évaluation des risques à travers ses responsables de rédaction. Son rôle avec le journaliste concerné est de mesurer l'impact des risques éventuels liés à la mission sur le journaliste et sur l'organe ainsi que de mettre en place les mesures nécessaires. Pour ce faire l'organe peut se poser les questions suivantes :
  - L'intérêt du sujet suffit-il pour ce que le journaliste prend le niveau de risque annoncé ?
  - Quelles ressources humaines, matérielles et financières faut-il mobiliser pour sécuriser la mission ? Sommes-nous prêts à les engager ?
  - Toutes les mesures nécessaires sont-elles prises pour minimiser les risques encourus ?
  - Les mesures d'assurance sont-elles assez rigoureuses pour couvrir des éventuels accidents ? (la question de l'assurance reste toutefois controversée sur la situation à Madagascar)
  - L'équipe de rédaction est-elle assez engagée pour soutenir le journaliste en cas de besoin ?

Attention !

Les risques peuvent être ressentis différemment par chaque journaliste. Ainsi, tout risque encouru et toute attaque subie devront être considérés par l'organe de presse comme une réelle menace pour le journaliste.

Travailler en équipe

Un journaliste travaille pour un desk généralement formé par un personnel de différentes contributions. Bien que chaque membre d'une rédaction ait chacun des responsabilités spécifiques, les actions restent complémentaires, conduisant au même résultat. Ainsi, il est conseillé de collaborer dans le cadre de la sécurisation des missions. Ces collaborations consistent en :

- la protection collective des informations partagées et disponibles au sein de la rédaction ;
- la concertation et les échanges d'information à effectuer lors des évaluations des risques ;
- la conduite de mission, au besoin.

Les collaborations peuvent prendre fin à la suite de changement de lieu ou de zone de travail, mais les protections mutuelles restent suivant la clause de confidentialité inscrite dans les contrats.

Checklist des matériels au quotidien

Chaque journaliste connaît les matériels qu'il utilise habituellement dans ses missions. Il s'agit notamment des matériels d'identification personnelle, de prise de notes, de connexion et de communication, d'enregistrement de son, de capture de photo, ainsi que de prise de vidéo. Ils devront faire l'objet de checking quotidien autant sur la question de disponibilité que sur celle de la qualité (oui, quelquefois une batterie vous lâche en plein milieu d'une scène importante) : ce checking permet d'éviter la circulation, l'abandon (quand vous devez le charger quelque part) et les emprunts de matériels qui peuvent être une source d'attaque ou faire l'objet d'une perte.

Ci-après un tableau non-exhaustif des matériels et de leurs caractéristiques qui devront faire l'objet de checking :

	Matériels	Caractéristiques
Identification	✕ Carte d'identité nationale ou passeport ✕ Carte de presse	✕ Carte de presse : fournie par l'OJM ou l'organe de presse ; ✕ Elle doit permettre une identification facile du journaliste. Les polices de caractères doivent donc être visible de loin dans la limite du raisonnable ; ✕ Pour éviter les risques de perte ou de dommage, les cartes d'identification devront être transportées dans des compartiments sécurisés.
Prise de note	✕ Bloc-notes et stylo ✕ Stylo de rechange	✕ Facile à ranger, à sortir, à utiliser dans toutes les postures possibles
Communication et connexion	✕ Smartphone et/ou téléphone portable secondaire pour les utilisations sensibles	✕ Robuste, résistant aux chocs ; ✕ Batterie pleine, et pouvant tenir jusqu'au moment sécurisé de recharge ; ✕ Connecté à internet, crédité de forfait de communication.
Prise de son, de vue photo et de vidéo	✕ Dictaphone ✕ Caméra professionnelle	✕ Répondant aux exigences de qualité de la rédaction ; ✕ Muni de sangle, de housse et autres protections utiles ; ✕ Batterie pouvant tenir jusqu'au moment sécurisé de recharge et/ou batterie de rechange ; ✕ Cartes mémoires de rechange.
Rédaction (au besoin)	✕ Ordinateur portable	✕ Performance selon les besoins ; ✕ Batterie pouvant tenir jusqu'au moment sécurisé de recharge ; ✕ Lieu sécurisé pour son utilisation, lieu public en plein air à éviter impérativement.

Au besoin, le journaliste peut emmener **un badge, un gilet et/ou un brassard** pour rester facilement identifiable dans une foule. **Les gilets et brassards sont par contre indispensables durant les reportages à haut risque** (foule, manifestation, affrontements, guerre, etc.). Ci-après quelques caractéristiques à considérer :

- Le badge : différent de « carte de presse », il indique en évidence le statut du journaliste. Le recto et le verso du badge doivent être identiques. Les écritures doivent être lisible pour une personne se situant dans une zone de proximité du journaliste.
- Le gilet : l'écriteau PRESSE doit être mis en évidence au-devant comme de derrière, en lettre capitale, police de caractère lisible, fort contraste de couleurs entre le texte et le fond, et visible clairement à 5 mètres, peu importe les conditions climatiques (jour, nuit, pluie …). Ainsi un écriteau sur fond fluorescent est idéal. Au-delà, chaque organe de presse peut ajouter un signe distinctif propre (logo, type de tissu spécifique, …)
- Le brassard permet une identification facile des journalistes. L'écriteau PRESSE doit être mis en évidence au-devant comme de derrière, peu importe les conditions climatiques (jour, nuit, pluie …). Ainsi un écriteau PRESSE sur un fond fluorescent ou contrasté serait idéal. Le brassard doit être bien accroché pour éviter une perte ou un enlèvement par une tierce.

Pour les missions spécifiques ou à risques, une autre checklist est proposée (voir Chap.2 et Chap.3).

A éviter impérativement

✘ Laisser les matériels ou leur contenant dans un endroit non sécurisé ou avec des inconnus. Les risques de perte sont élevés à Madagascar.

⚠ Attention !

Même si les smartphones se présentent actuellement comme un outil qui peut remplacer la plupart de ces matériels, ils ne peuvent être sollicités à tout moment, développant des risques de pertes de données, de vol ou de « ratage ». Disposer d'un support additionnel, non numérique est conseillé.

1.2. Rester dans la légalité

La loi protège le journaliste dans l'exercice de sa fonction, mais la loi pose aussi des limites. Pour rester sous la protection de la loi, le journaliste doit rester dans la légalité et ne faire que ce que la loi permet, il doit également savoir et ne pas faire ce que la loi interdit, comme indiqué dans les aperçus ci-après :

Ce que la loi permet :

✔ le journaliste a le droit d'informer le public (Art.10 Constitution, Titre II Code de la Communication) ;

✔ le journaliste a droit à l'accès à l'information (Art. 7 ; 60 al.2 Code de la communication).

Ce que la loi interdit :

- ✘ le journaliste n'a pas le droit de porter atteinte aux bonnes mœurs (art. 330 du Code pénal) ;
- ✘ le journaliste n'a pas le droit de diffuser de fausses nouvelles (art. 30 du Code de la communication) ;
- ✘ le journaliste n'a pas le droit de porter atteinte au droit à l'image et à la vie privée (art. 20 du Code de la communication) ;
- ✘ le journaliste n'a pas le droit de faire de la diffamation (art. 23 du Code de la communication) ;
- ✘ le journaliste n'a pas le droit de faire offense aux institutions (art. 23 du Code de la communication ; art. 20 de la loi sur la cybercriminalité) ;
- ✘ le journaliste n'a pas le droit de porter atteinte à la mémoire des morts (art. 36.5) ;
- ✘ Le journaliste n'a pas droit d'accès aux informations pouvant porter atteinte à la sureté de l'Etat, selon le niveau d'habilitation de l'information, ou le niveau de confidentialité de l'information (information confidentielle, information secrète, information classée «secret défense»).

1.3. Se protéger des dangers physiques

La sécurité du journaliste est primordiale. Même si l'organe de presse et les forces de l'ordre ont pour mission de protéger le journaliste, le journaliste est le premier responsable de sa propre sécurité. Il doit ainsi pouvoir faire face à toute agression physique, et/ou stopper les agressions en restant dans le cadre de la légitime défense. Pour ce faire, des mesures peuvent être prises dans les déplacements, les fréquentations et les lieux de mission.

Par rapport au profil personnel

Le journaliste est le centre de gravité des articles. Il est le premier responsable de sa propre sécurité. Ce qu'il publie peut être considéré comme motif d'agression, bien que celle-ci reste illégale. De même, ses opinions et ses convictions idéologiques, son genre et son orientation sexuelle peuvent être des motifs d'agression. Des faits d'agressions verbales (harcèlements, menaces) et des agressions physiques (violences et voies de fait, coups et blessure volontaires, homicides, etc.) liées au profil du journaliste se sont déjà produits à Madagascar.

Pour tout reportage comportant des risques, les dispositifs suivants peuvent être mis en place :

- ✦ avant, pendant, et après l'interview, se munir des matériels d'enregistrement (audio vidéo) discrets pour la constitution de preuves en cas d'agression ;
- ✦ avoir un réflexe d'archivage pour n'importe quel type d'agression (verbale ou textuelle, numérique) ;
- ✦ avoir un réflexe d'enregistrement et d'archivage de chaque appel téléphonique douteux ;
- ✦ au besoin, faire appel à un huissier de justice pour la transcription de ces éléments de preuves sous forme de procès-verbaux pour une recevabilité devant l'instance compétente ;

- une formation en self-défense s'avère être également un moyen de protection utile en cas de besoin.

Dans les déplacements

Au quotidien, durant lequel les risques sont au niveau le moins élevé (code jaune), les mesures de sécurité sont basiques. Toutefois, des habitudes de sécurisation devront être cultivées et suivies :

- les déplacements non cadrés devront se faire dans les heures raisonnables du travail (habitation-bureau, lieu de reportage) ;
- les déplacements en dehors des heures de bureau devront être organisés et se faire sous protection, notamment avec des véhicules mises à disposition par l'organe de presse ;
- l'inscription PRESSE doit être visible sur les véhicules fournis par l'organe de presse, permettant au véhicule de se faire identifier par les usagers de la route et les forces de l'ordre.

Dans les locaux

Les locaux doivent avoir des équipements pour offrir les mesures de sûreté minimales possibles aux journalistes : système anti-incendie (extincteurs, bornes d'incendie, etc.), indications d'évacuation (plan de masse, zone de regroupements, etc.) et indications facilitant l'identification des issues de secours. Des simulations d'incendies doivent être organisées périodiquement de manière à former les salariés aux dispositifs à suivre en cas d'incendie.

Dans certains cas spécifiques (durant des émeutes, par exemple), il est possible de faire appel aux forces de défenses et de sécurités (FDS) pour une mise à disposition de personnels armés pour la sécurisation des bâtiments.

Lors des reportages en extérieur, la confiance mutuelle entre journaliste et source d'informations est primordiale. Il y a donc lieu de mettre à l'aise son interlocuteur pour que tout aille naturellement. Certes, le journaliste évitera une exigence déplacée en termes de lieu de rencontre pour ne pas mettre son interlocuteur dans l'embarras. Toutefois, il doit rester vigilant et repérer le chemin le plus sûr à emprunter en cas de besoin.

Assurances : L'assurance n'est pas une pratique bien ancrée dans le management malagasy. Très peu de journalistes sont assurés par leurs organes de presse. Pourtant, les journalistes sont exposés aux risques physiques de tout genre. Il est conseillé ainsi aux patrons de presse de souscrire à une police d'assurance pour leurs employés.

1.4. Se protéger des dangers numériques

Les journalistes sont de plus en plus exposés à des menaces numériques : piratage, surveillance, désinformation, harcèlement en ligne. Ces attaques peuvent compromettre leur sécurité, celle de leurs sources ou la crédibilité de leur travail. Cette section propose des conseils de bases simples, pratiques et accessibles pour limiter ces risques.

Sécurisation des accès aux comptes

La métaphore courante compare les mots de passe au sous-vêtement :

- changez-la régulièrement ;
- ne la partagez à personne ;
- ne la laissez pas traîner à la vue d'autres personnes.

A cela s'ajoute un quatrième principe : utiliser un mot de passe différent pour chaque plateforme.

Astuces

- Contrairement à une pensée courante, on peut utiliser des espaces dans les mots de passe.
- Les mots de passe forts ne sont pas forcément difficiles à mémoriser. Il est possible d'utiliser des astuces comme la *mnémotechnique* (un modèle commun de votre choix dont vous pouvez vous souvenir facilement), la stéganographie (utiliser un texte public que vous pourrez retrouver et recopier facilement quand il le faut. Exemple : un verset biblique, un texte littéraire, etc.).

L'utilisation des applications

Parmi les outils les plus utilisés dans la collecte d'informations de nos jours figurent les applications numériques ou les plateformes de communication en ligne. A chaque fois que vous vous inscrivez sur une nouvelle plateforme ou que vous installez une application, la première chose à effectuer est la revue des paramètres de sécurité et de confidentialité (que ce soit dans les « paramètres » de l'application, ou dans celui de votre téléphone).

Cette revue doit inclure au moins ces rituels :

- restreindre la visibilité de vos coordonnées (email, numéro de téléphones) ;
- activer l'authentification à double facteur ;
- obtenir les codes de récupération à utiliser en cas d'oubli du mot de passe. (A garder dans un endroit secret, en dehors de la plateforme en question) ;
- activer les alertes de connexion (si option disponible).

Attention !

Cette revue est à effectuer régulièrement (tous les 6 mois au moins) car les applications et les plateformes peuvent changer leurs politiques et leurs paramètres par défaut à tout moment.

Les sources en ligne et le stockage d'informations

Des tentatives d'accès malveillantes peuvent cibler les journalistes à travers des actions anodines comme des clics sur des liens à priori légitimes ou des visites de sites malveillants. Cela peut se produire même dans des messages privés, envoyés naïvement par des proches. Les sources contactées peuvent également être l'auteur de ces attaques.

Voici quelques bonnes pratiques pour les éviter :

- rester systématiquement prudent et **ne jamais cliquer sur des liens inhabituels et/ou suspects :** mail de félicitations inattendues, notifications de paiements incohérents, loterie, informations suspectes, etc. Avant de cliquer sur un lien, survolez-le avec la souris (sur PC) ou appuyer longuement dessus (sur mobile), l'adresse de destination réelle va s'afficher. S'il ne s'agit pas de la destination attendue, n'ouvrez pas le lien ;
- **lire attentivement l'adresse internet avant d'ouvrir ou de taper des informations personnelles ou des mots de passe**. Les auteurs de *phishing* se servent souvent d'adresses ressemblant aux adresses qu'ils essaient d'usurper. Par exemple, pour imiter *facebook*, ils pourraient utiliser *faceboook.com* (il y a un "o" en trop), *facebook.co* (ce n'est pas un ".com" mais ".co") ;
- ne pas **transférer un email suspect, même pour prévenir les autres**. Si vous souhaitez prévenir les autres de se méfier d'un email suspect, envoyez plutôt une capture d'écran.

Il est également impératif de protéger les matériels face aux risques de vols de données ou d'intrusion de logiciels malveillants. En effet, s'il y a une pratique courante et pourtant dangereuse, c'est de laisser le matériel électronique sans surveillance ou librement accessible à un tiers : un ordinateur ou un téléphone non verrouillé pendant la pause-café, un téléphone prêté à quelqu'un pour un appel ou une connexion, un ordinateur chargé à un port USB public, etc.

Ne pas laisser son matériel (PC, téléphone) **sans surveillance et/ou déverrouillés**. Par ailleurs, si possible il est préférable d'éviter les verrouillages biométriques : doigts, reconnaissance faciale car ils peuvent être utilisés à votre insu ou avec la force.

Astuces

- Pour éviter une perte définitive des informations et données en cas de vol de machines, le stockage dans un serveur en ligne (*drive, dropbox, icloud,* etc.) reste une pratique classique et efficace. Toutefois, des mesures de protection renforcée à leur accès doivent être prises avec un spécialiste en IT. Vous pouvez également préserver **la documentation de vos sources et de vos articles** à travers des captures d'écran, ou de préférences des services offrant l'archivage avec métadonnées et horodatage (exemples : archive.org).

Attention !

Apprendre à ne pas croire à **tout ce qui est publié sur internet** ; il faut redoubler de vigilance avec la prolifération des *deepfake*.

Conseils aux organes de presse

Avec les journalistes eux-mêmes, les organes de presse sont les premiers responsables de la protection numérique de leur personnel. Cette protection prend généralement deux dimensions : la promotion d'une culture numérique saine et l'investissement dans des dispositifs matériels, logiciels et organisationnels nécessaires. Dans tous les cas, il est souvent constaté que les moyens à disposition des organes de presse malagasy sont limités. Dans les propositions suivantes, nous trouverons quelques idées qui peuvent être réalisées sans se ruiner :

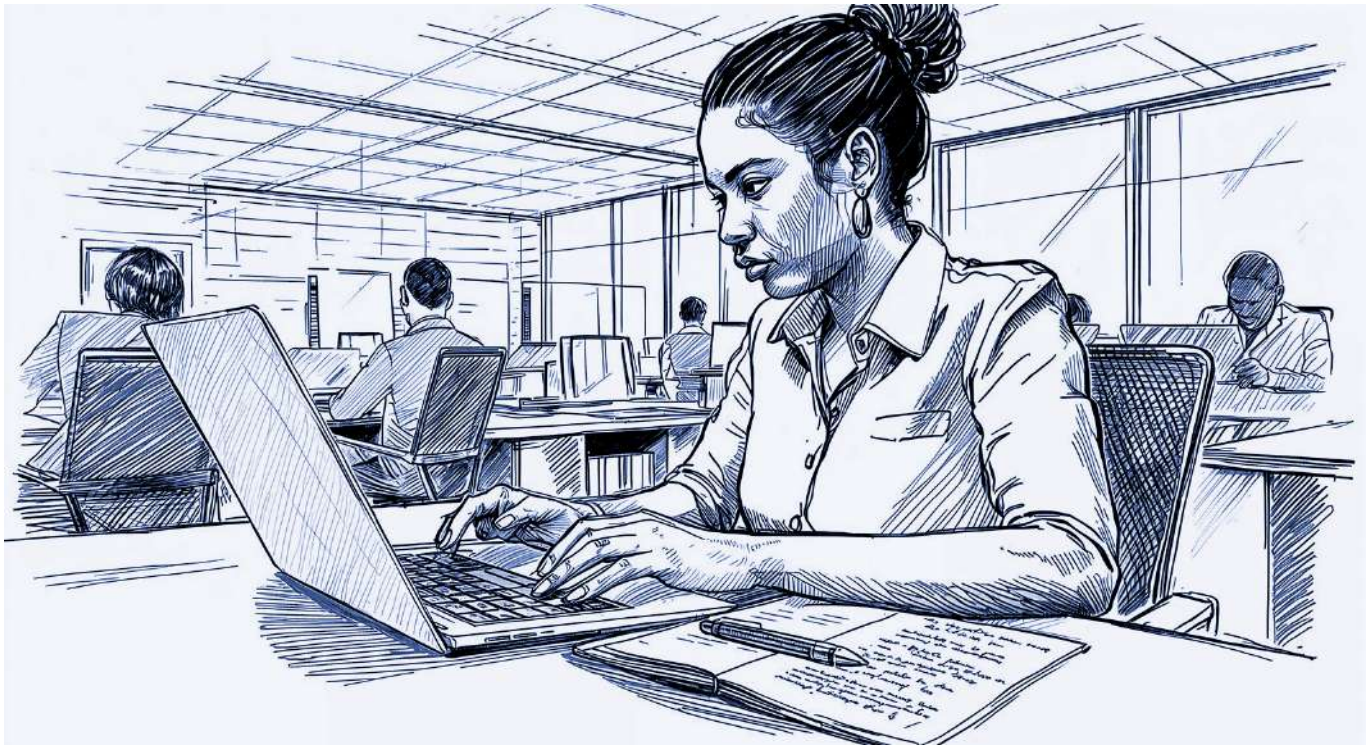
- inclure **l'initiation à la sécurité numérique et les simulations de crise** dans la formation de l'ensemble du personnel. Ces séances peuvent tout à fait être dispensées par le responsable informatique, s'il n'y a pas moyen d'appeler un expert du digital ;
- mettre en place une politique et des exigences minimales strictes en matière de sécurité numérique, à appliquer par tout l'ensemble du personnel.
- investir dans des **logiciels de confiance** (non *crackés*). Beaucoup de solutions open source peuvent être utilisées, à commencer par les systèmes d'exploitation (du système comme *linuxs* aux différents types de logiciels quotidiens de la vie du journaliste. Dans le même esprit, ne jamais oublier de renforcer régulièrement la **sécurité du réseau interne** (pare-feu, *VPN*, etc.)) ;
- investir dans des **outils de veille et d'alerte**. Exemple : *Meltwater, Talkwalker, Mention,* etc. pour surveiller régulièrement les discussions autour de votre nom, de votre média. Certains outils restent gratuits même s'ils sont moins performants ;
- **en cas d'attaque subie :** renforcer la protection et archiver toute information utile avec date et heure avec des outils d'archivages comme *archive.org* ou *ghostarchive.org*.

A faire impérativement

- ✔ Anticiper et mettre en place un protocole de réponse rapide en cas d'erreur dans une publication : fact-check, communiqué, mise au point, correction des procédures, etc.

Attention !

La technologie évolue en permanence. Ainsi les outils mentionnés en exemples peuvent évoluer ou être remplacés dans le futur. L'important est d'appliquer les règles de vigilance et de travailler régulièrement avec un professionnel du numérique.



Chapitre 2.
En missions sensibles

On entend par « missions sensibles » les activités exposant les journalistes à des risques élevés. Parmi les principales missions sensibles, on note les investigations touchant des intérêts importants, des reportages dans des zones non ou mal sécurisées, des suivis de missions policières ou militaires (comme dans les zones des « dahalo ») ainsi que des missions de déplacement risquées pour lesquelles les mesures de sécurité ne peuvent pas être prises d'une manière optimale.

Ces missions exigent des mesures de protection plus conséquentes et réfléchies. Ce chapitre traite de quatre dimensions sécuritaires des missions sensibles : les rituels de base, les bases légales à assimiler, les risques et protection contre les dangers physiques ainsi que les protections contre les dangers numériques.

2.1. Rituels de base

Pour se préparer d'une manière optimale aux missions sensibles, des rituels supplémentaires sont ajoutés aux rituels quotidiens déjà abordés dans les précédents passages (Voir : Évaluation systématique des risques et Rituels de base du Chap. 1). Ces pratiques permettent de réduire les risques et donc le stress que peut développer le journaliste. Il contribue ainsi à la qualité des résultats de la mission. Traité dans ce chapitre, ces rituels comprennent essentiellement : une meilleure connaissance du contexte permettant une évaluation plus approfondie des risques, une préparation matérielle et logistique répondant aux exigences des risques ainsi qu'une checklist des matériels de protection nécessaires.

Connaissances du contexte

Une mission sensible implique de nouveaux paramètres par rapport à ce que l'on recense au quotidien : éventuellement une nouvelle zone de mission, des déplacements plus conséquents et peut-être plus périlleux, une période particulière (exemple : période de recrudescence d'insécurité), de nouvelles sources d'information, des résultats attendus plus exigeants, etc. En ce sens, les mesures sont également exceptionnelles. Pour ce faire, nous pouvons utiliser une liste non-exhaustive des points d'informations à réunir, sous forme de questions comme présentée ci-après :

Soi-même	■ Quel est mon rapport avec les intérêts touchés ? ■ Mes orientations (opinion, conviction, genre, orientation sexuelle) ne constituent-elles pas un frein au bon déroulement de la mission ?
Autour du sujet traité	■ Quels sont les intérêts touchés ? ■ A qui sont ces intérêts ? ■ Quelles autorités sont concernées ?
Conditions de mission et système de protection disponible	■ Quelles sont les mesures mises en place par l'organe de presse ? ■ Ai-je un soutien au niveau de la rédaction en cas de besoin ? ■ Qui sont mandatés pour la mission et constituent l'équipe ? ■ Quels sont les matériels disponibles ? (voir checklist plus bas) ■ A-t-on alloué assez de ressources financières pour la mission, (éventuellement des indemnisations classiques relatives aux risques à prendre en cas de déplacement) ?
Sources d'information	■ Ai-je en main un minimum de contacts de sources d'informations ? ■ Quel est le degré de confiance à accorder à chaque source ? ■ Sont-elles en sécurité en se mettant en contact avec moi ?
Si déplacement : zone de travail et conditions locales	■ Y a-t-il un/des contacts (fixeur, guide, traducteur, etc.) sur place ? ■ Quelle commodité est disponible sur place (hôtel, service de restauration, etc.) ? ■ Quel est le niveau de danger des mouvements sur place (exemple : proximité avec les dahalo, niveau d'implication des FDS, etc.) ? ■ Quelles mesures de sécurité peut-on prendre sur place au besoin ? ■ Quel temps fera-t-il durant la mission ?
Si déplacements	■ Comment on se déplace vers, dans et au retour de la zone ? ■ Quelles mesures de sécurité sont prises durant les déplacements ?
Durée de la mission	■ Le temps alloué est-il trop court / trop long par rapport aux risques à prendre ? ■ A-t-on assez de ressources pour le temps alloué ?
Motivation des proches	■ Les proches sont-elles motivées pour laisser le journaliste effectuer la mission ?

A éviter impérativement

✘ Il est fortement déconseillé de travailler seul sur des missions sensibles. La rédaction fera le nécessaire pour mettre au moins un binôme sur le sujet, sinon il est conseillé d'engager un consultant ponctuel pour travailler avec le journaliste (journaliste freelance, fixeur, etc.).

⚠ Attention !

Si à la plupart de ces questions vous avez donné plus de réponses négatives que positives, il est nécessaire de développer des mesures de sécurité largement plus conséquentes ou sinon, d'abandonner la mission, de manière préventive.

Checklists des matériels de base

Une liste de matériels classiques du journaliste est présentée dans le Chap. 1 (voir Checklist des matériels au quotidien). Il englobe les matériels permettant d'assurer généralement des reportages sécurisés pour une journée. Pour une mission sensible, le reportage peut dépasser la journée ou nécessiter un déplacement. L'objectif lié à la sécurité réside dans l'intention de rester autonome dans la mission et donc d'éviter de devoir demander de l'aide ou pire, rater l'archivage des informations utiles au reportage ou, le cas échéant, à sa propre défense.

Ainsi, à ces matériels classiques peuvent s'ajouter :

- plus de **dispositifs en énergie électrique :** chargeurs des appareils électroniques, *powerbank*, rallonge et multiprise, etc. ;
- plus de **capacité de stockage de données :** disques durs, cartes mémoires, clés USB pour des déplacements de données, etc. (voir les sections numériques pour la sécurisation de ces matériels de mémoire) ;
- des **matériels d'enregistrement embarqués** et discrets (de type *Gopro*) peuvent également faciliter la tâche et aider à obtenir des résultats particuliers. Ces appareils peuvent également fournir des preuves pouvant permettre d'écarter les responsabilités des journalistes face à tout type de dérapages ou de débordements.

Checklists du système de protection

La protection devrait se trouver au premier plan des préoccupations dans les missions sensibles. Pour se rassurer et pour garantir une mission sûre et sans incidents, des rituels et des matériels spécifiques devront être à portée de main. Ils concernent autant le physique du journaliste que le numérique. Ci-après quelques indications de base en ce sens :

Protection physique

Il n'existe pas encore de normes spécifiques pour la sécurité physique des journalistes. Certes, l'UNESCO, la RSF ou encore l'IFJ éditent des textes sur la sécurité des journalistes sur le terrain mais les réalités sont différentes pour chaque localité et chaque mission. Toutefois, des mesures communes reviennent dans chaque manuel, à savoir :

- la mise en place d'une équipe d'entraide : elle peut se matérialiser à travers la création d'un binôme de travail, le recrutement temporaire d'une aide sur le lieu de travail ou la composition d'une vraie équipe multidisciplinaire. Ce système doit être autonome, auto organisée et quelquefois auto-évolutif ;

- la mise en place d'un système de signalement de danger ou de détresse : localisation en permanence de position via le téléphone (donc via un téléphone connecté avec système GPS ou alarme personnelle), appel d'urgence facilité chez les proches et la rédaction (mise en place de raccourcis dans le téléphone), appel d'urgence préparé chez les forces de sécurité et de défense (raccourcis également à mettre en place) ;

Astuces

- Au besoin, il peut être nécessaire d'avoir sur soi un équipement de protection tels que les sprays au poivre, les teasers, les lampes tactiques, les stylos tactiques, les balles de défenses, etc. à utiliser à bon escient et toujours dans une situation de légitime défense. Attention : certaines zones ne permettent pas le port de ce genre d'accessoires (aéroports, ambassades, etc.)

Protection numérique

- vérifier systématiquement les paramètres de confidentialité de vos comptes et applications et désactiver la géolocalisation automatique (sauf pour les nécessités du système de signalement évoqué précédemment) ;
- si possible, utiliser un téléphone et un numéro de téléphone "secondaire" dédiés à vos communications sensibles. Il peut s'agir, soit d'un téléphone sécurisé, soit au moins un téléphone basique (un *dumbphone* ou *foza*) ;
- une cache (un ruban adhésif de type *Barnadher* fera l'affaire) ou un interrupteur matériel (*kill-switch*) pour caméra/micro sur votre ordinateur ou téléphone afin de couper physiquement l'accès à ces périphériques ;
- au besoin : un disque dur externe *crypté* (que vous débranchez après chaque usage, parlez avec votre responsable IT pour la question de cryptage) pour vos rushes, entretiens, sources sensibles. Pour certains cas, il pourra même s'agir d'un disque avec un système spécialisé de type *Tails OS* (système d'exploitation *open source, dédié à l'anonymat et la protection des sources*).

2.2. Rester dans la légalité

Pendant les missions sensibles comme le traitement des dossiers touchant d'importants intérêts économiques ou susceptibles de provoquer un trouble à l'ordre public, le journaliste doit redoubler de vigilance pour s'assurer de rester dans la légalité. Pendant ce genre de mission, une erreur peut avoir des conséquences encore plus graves qu'en temps normal. Il faut donc bien veiller à faire ce que la loi permet et surtout ne pas faire ce que la loi interdit.

Ce que la loi permet :

- ✔ le journaliste a droit à l'accès à l'information (art. 11 de la Constitution, art. 6 du Code de la communication). Cet accès reste toutefois relatif dans la mesure où la loi ne définit pas assez les modalités d'accès à de nombreux types d'information, notamment provenant de l'administration publique ;
- ✔ le devoir d'informer le journaliste devient encore plus important (art. 58 du Code de la communication).

Ce que la loi interdit :

- ✘ ne pas inciter à violer la loi : pas d'incitation à la haine, à la violence, au meurtre, à la discrimination, etc. (art. 26 et 27 du Code de la communication);
- ✘ ne pas inciter les policiers/militaires à désobéir (art. 28 du Code de la communication) ;
- ✘ ne pas porter atteinte à l'unité nationale/l'intégrité territoriale (art. 26 du Code de la communication) ;
- ✘ ne pas porter atteinte à l'intimité de la vie privée : (art. 20 et 58 du code de la communication).

Attention !

Par ailleurs, la loi interdit les publications pouvant porter atteinte à l'honneur des institutions publiques et de leurs responsables sans délimiter clairement les frontières entre ce qui est permis et ce qui ne l'est pas. La vigilance reste ainsi de mise.

2.3. Se protéger des dangers physiques

Se protéger des agressions physiques en mission sensible est très délicat. Le risque peut apparaître pendant un moment de vulnérabilité. Il revient ainsi au journaliste de limiter ces moments de vulnérabilité et de redoubler de vigilance dans les moments les plus dangereux (rencontres sensibles, lieux dangereux, etc.). Pour ce faire, quelques pratiques sont conseillées sur la question d'évaluation des risques sur place, des personnes fréquentées, des transports et déplacements et des locaux fréquentés.

Evaluation des risques dans la zone

En plus de l'évaluation effectuée avant le déplacement, des évaluations permanentes doivent se faire sur place : compréhension de l'environnement où la zone de collecte d'information sera effectuée (interne/externe, sécurisé/non sécurisé, comportement des habitants, etc.), une brève observation et interprétation permettant de comprendre le tempérament de chaque personne rencontrée (si la personne risque de réagir avec une agression verbale ou physique).

Sur les lieux de rencontre

Les lieux d'interview restent une dimension délicate des missions sensibles puisque le journaliste y est généralement étranger. Voici des comportements à développer et à appliquer systématiquement sur place :

- ✦ observer les personnes sur place dont des accompagnants qui ne sont pas prévus, les issues les plus proches comme les plus éloignées ainsi que les objets visibles qui peuvent représenter des dangers ;
- ✦ rester près de l'issue et si possible garder une certaine distance (ni trop proche, ni trop loin) par rapport à l'interlocuteur ;

- ne sortir que les matériels nécessaires ;
- garder un ton neutre et professionnel même dans des moments délicats ;
- autant que possible, éviter de boire ou de manger des nourritures offertes ;
- au besoin et en cas de souci, sortir immédiatement et contacter discrètement l'équipe d'accompagnement.

Transports et déplacements

Les véhicules mis à disposition des journalistes doivent permettre d'assurer la sécurité des journalistes dans leurs déplacements. Ainsi ils doivent :

- être en bon état, en règle avec l'administration et faire l'objet d'entretien régulier ;
- disposer d'un verrouillage centralisé et des éclairages fonctionnels à l'intérieur comme à l'extérieur ;
- comporter une indication « PRESSE » à afficher au besoin ;
- être disponibles à tout besoin, sous condition de contrat ;
- être conduits par des professionnels, briefés sur la délicatesse de la mission ; de préférence, formés à la conduite défensive.
- si besoin : disposer d'un équipement de géolocalisation et de caméra embarquée.

Par ailleurs, la maison de presse doit se préparer avec son prestataire à la disponibilité d'un véhicule de secours en cas de panne.

2.4. Se protéger des dangers numériques

Durant les missions sensibles, le numérique reste une technologie très sollicitée et vitale. Il est naturel de maintenir une relation de qualité avec vos matériels, d'en prendre soin (comme il s'agissait d'un coéquipier !). Il est également primordial de rester vigilant face aux dangers que vos ennemis peuvent développer avec leur utilisation. Voici quelques conseils à suivre pour cela :

Communication : réception et envoi d'informations

- utiliser des canaux de communication sécurisés et anonymes : pour les échanges écrits et même vocaux, préférez les applications simples et réputées comme *Signal, Jami, Tox* ; pour l'adresse mail, la webmail *Protonmail* offre des fonctionnalités renforcées par rapport aux plateformes classiques ; enfin, autant que possible éviter d'échanger des informations sensibles par SMS ou messagerie non sécurisée (*Messenger* par exemple)
- se protéger des messages comportant des attaques : les pièces jointes, les QR codes, les liens même d'un contact connu feront l'objet d'attention particulière, il est conseillé de désactiver les prévisualisations de liens dans les messageries (*Whatsapp, Telegram, Signal, etc.*) pour éviter les attaques *zero-clicks* ; même chose pour la prévisualisation des messages sur écran verrouillé.

Les sources en ligne

- pour éviter d'être espionné en ligne, certaines navigations sensibles devront rester privées en utilisant des navigateurs sécurisés (exemple : *Tor*), les sources doivent être documentés (où, quand, comment, etc.), l'entrée en contact avec des sources inconnues doivent être faite avec prudence et de préférence connue de la rédaction ;
- autant que possible, pour protéger vos sources : ne pas écrire leur nom réel dans les documentations ni sur les canaux sécurisés.

Le stockage et traitement des informations

Tout ce qui a été dit à propos des stockages de fichiers est plus que jamais en vigueur ici : stockage sur des disques déconnectés et protégés, ouverture d'une session spéciale pour les dossiers sensibles, utilisation de l'ordinateur personnel, ouverture limitée de fichiers sensibles (notamment les PJ). L'application spécialisée *Tella* facilite le stockage sécurisé des informations sensibles et leur dissimulation dans un smartphone ; sur PC, le système Tails-OS permet de dédier un stockage crypté persistant.

Important : l'adoption de ces outils spécialisés ne garantit pas à elle seule une sécurité à 100%, elle doit s'accompagner de changements d'habitudes.

Les publications

Les précautions restent importantes même pendant la publication : nettoyage des métadonnées, protection (floutage de visage, déformation des voix ou reconstitution) des sources mises en avant, copie horodatée de l'article tel que publié.

Astuces

Pour renforcer la sécurité du journaliste, ci-après **quelques bonnes pratiques pour les organes de presse :**

- Investir dans des appareils de protections supplémentaires : téléphone secondaires (sécurisés ou *dumbphone/foza*) et numéro dédié, messagerie protégée (*Protonmail*), accès *VPN*, *USB data blocker*, clés USB chiffrées ;
- Interdire l'utilisation de numéros ou mails pro sur les réseaux sociaux ou les plateformes à risque ;
- Établir un protocole clair de signalement des compromissions ;
- Privilégier les accessoires câblés plutôt que ceux branchés par *bluetooth* ou *wifi* (claviers, souris, etc.) ;
- Établir un plan de réponse en cas d'attaque du journaliste en mission. À tout moment, **la sécurité physique et psychologique du journaliste reste la priorité.**

Attention !

En plus des attaques de hameçonnages classiques, les journalistes peuvent être la cible de *whaling* : il s'agit d'une attaque similaire au phishing mais très ciblée, très personnalisée destinée à atteindre une personne ou un groupe de personnes en particulier, dont les journalistes travaillant sur un sujet sensible. Si vous êtes à risque ou travaillez sur un sujet à risque, prenez l'habitude de confirmer physiquement avec les personnes avec qui vous êtes en contact lorsque vous recevez des documents.

Exemple d'un whaling :

Chapitre 3.
En situations exceptionnelles : manifestations et émeutes

Les manifestations et émeutes font partie de l'histoire de la démocratie dans le monde. Leur couverture est une mission légitime et essentielle pour tout média. Madagascar jusque-là vit un cycle de mouvements populaires et/ou militaires conséquents sensiblement à chaque décennie. Par ailleurs, des mouvements de grève et des protestations populaires ponctuent la vie sociopolitique, avec quelquefois des affrontements verbaux et physiques, des arrestations, des condamnations, des harcèlements, des menaces d'agression, etc. L'objectif de ce chapitre est de préparer le journaliste à faire face à ces mouvements avec une protection optimale et garantir la meilleure sérénité possible. Comme dans les précédents chapitres, on retrouve ici des rituels simples, des connaissances de base du cadre légal, des mesures de protection physique et des dispositifs de protection numérique.

3.1. Rituels de base

Pour se préparer d'une manière optimale aux missions en situations exceptionnelles, des rituels supplémentaires sont également ajoutés aux rituels quotidiens (Voir : Évaluation systématique des risques et Rituels de base du Chap. 1). Comme pour les missions sensibles, ces pratiques permettent de réduire les risques et donc le stress que peut développer le journaliste. Il contribue ainsi à la qualité des résultats de la mission. Pour reprendre les mêmes contenus, nous retrouverons dans cette section les informations à savoir autour du contexte et les différents matériels et dispositifs à mettre en place.

Connaissances du contexte

Le contexte présente des dimensions particulières, étant donné que le déroulement du mouvement n'est pas souvent écrit à l'avance. Comme tous les acteurs sur place, le journaliste sera ainsi en mode « découverte » et s'adaptera à la situation. Les situations exceptionnelles mettent ainsi le journaliste dans des conditions doublement difficiles : d'abord l'objectif de collecter de faits aussi pertinents que complets, ensuite de pouvoir se protéger de toutes formes d'agression généralement imprévues.

Pour y faire face, il est conseillé de compléter les informations en main suivant les questions suivantes :

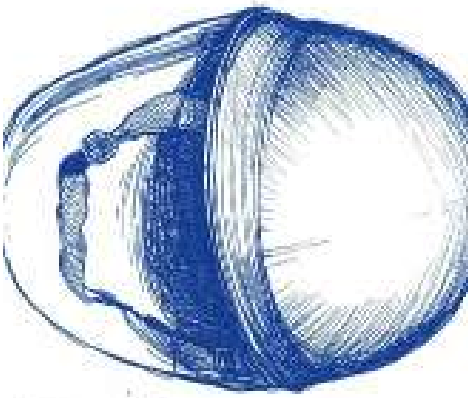
Autour du sujet traité	▪ Quels sont les intérêts touchés ? ▪ A qui sont ces intérêts ? ▪ Quelles autorités sont concernées ?
Conditions de mission et système de protection disponible	▪ Quel niveau de mesure de gestion de l'ordre est prévue par les FDS ? ▪ Quel est le niveau d'agressivité des manifestants ? ▪ Quelles sont les mesures mises en place par l'organe de presse ? ▪ Qui sont mandatés pour le reportage et former l'équipe ? ▪ Quels sont les matériels disponibles ? (voir checklist plus bas)
Sources d'information	▪ Les sources sont-elles en sécurité en se mettant en contact avec moi ? ▪ Ai-je en main les contacts des responsables des FDS mobilisées ?
Si déplacement : zone de travail et conditions locales	▪ Quel est le niveau de dangerosité des mouvements (selon les acteurs prévus se mobiliser) ? ▪ Quelles mesures de sécurité peut-on prendre sur place au besoin ?
Si déplacements	▪ Comment on se déplace ?
Durée de la mission	▪ Les exigences de la rédaction en termes de rapport sont-elles raisonnables (exemples : devoir faire des « live ») ?

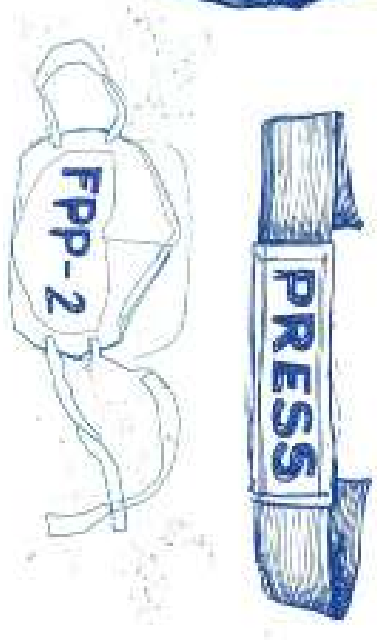
A éviter impérativement

✘ Comme dans une mission sensible, il est fortement déconseillé de travailler seul pour le reportage des mouvements délicats quel que soit le statut du journaliste (rédacteur, caméraman, photographe, etc.). En plus des mesures de constitution d'équipe par la rédaction, les entraides entre journalistes sur place facilitent énormément le travail. Ainsi ne pas hésiter à s'organiser !

Attention !

Si à la plupart de ces questions vous avez donné plus de réponses négatives que positives, il est nécessaire de développer des mesures de sécurité largement plus conséquentes ou sinon de refuser la mission, à titre préventif.





Checklist des matériels de base

Une liste de matériels classiques du journaliste est présentée dans le Chap. 1 (voir Checking des matériels ordinaires). Il englobe les matériels permettant d'assurer généralement des reportages sécurisés au quotidien. Lors d'une situation exceptionnelle, d'autres matériels et quelques dispositifs de sécurité doivent être mis en place. L'objectif est de s'assurer de mener des exercices de reportage sécurisant pour le journaliste et pour ses accessoires. Ainsi, à ces matériels classiques peuvent s'ajouter :

- des dispositifs supplémentaires électriques : un *powerbank* chargé fera l'affaire ;
- des dispositifs de renforcement des mémoires électroniques : plusieurs cartes mémoires pour la quantité mais également pour protéger (cacher, faire des copies, etc.) les données récoltées ;
- il est conseillé de partir léger : ainsi si vous disposez d'un téléphone secondaire, laissez votre téléphone principal ;
- il est conseillé de partir en reportage avec un contenant léger (sac de petite ou moyenne taille) et bien fixé auprès du corps pour regrouper et sécuriser les matériels non-sollicités en permanence. Il facilitera largement les déplacements du journaliste.

Checklist du système de protection supplémentaire

A ces matériels de base, dont gilet et brassard (voir Chap. 2), s'ajoutent des matériels de sécurité essentiels à une protection aux risques évidents. Il s'agit non-exhaustivement de :

- casque anti-émeute floqué « PRESSE » ;
- masque à gaz ou à défaut masques de type *FFP2 ;*
- chaussures à semelles robustes mais permettant des déplacements rapides ;
- visière et lunettes de protection (optionnelles) ;
- au besoin : imperméable facilitant l'identification floqué « PRESSE ».

3.2. Rester dans la légalité

En cas de manifestation ou d'émeute, le devoir d'informer pour le journaliste est plus que jamais essentiel. Mais le danger devient également une menace réelle. Pour se protéger durant ces manifestations, mais aussi se protéger juridiquement, le journaliste a le devoir de rester dans la légalité, un devoir qui devient ainsi une nécessité de sécurité et obligation légale.

Ce que la loi permet :

- ✔ filmer, photographier, envoyer en direct ou différé (art. 58 du Code de la Communication) ;
- ✔ faire des interviews (art. 58 du Code de la Communication) ;
- ✔ ni les forces de l'ordre ni les manifestants n'ont le droit d'agresser le journaliste ni d'endommager ou prendre son matériel (art. 11 de la Constitution, art. 6 du Code de la communication).

Ce que la loi interdit :

- ✘ ne pas inciter les policiers/militaires à désobéir (art. 28 du Code de la communication) ;
- ✘ ne pas inciter à la haine ou à la violence (art. 26 du Code de la communication) ;
- ✘ ne pas porter atteinte à l'honneur des personnes ou des Institutions (art. 23 du Code de la communication et art. 20 de la loi sur la cybercriminalité) ;
- ✘ ne pas porter atteinte à la dignité humaine. Par exemple : ne pas publier les photos des parties intimes d'une personne blessée (art. 20 et 58 du code de la communication), des photos d'enfants sans le consentement de ses parents, des photos explicites de personnes mortes de blessures sans le consentement de leur famille, etc.

3.3. Se protéger des dangers physiques

A ce stade, le code de maintien de l'ordre utilisé par les FDS est au niveau orange, voire rouge. Le danger est donc réel et le journaliste se trouve en milieu hostile. Il gardera pour objectif essentiel de rester sain et sauf malgré la mission qui lui est confiée. Pour ce faire, il doit faire attention aux acteurs présents, à l'environnement et à ses déplacements.

Personnes fréquentées

Le premier réflexe du journaliste est de repérer et catégoriser les personnes présentes : les alliés, les neutres et les éventuelles sources de dangers.

- ✦ Les alliés : il s'agit d'abord des confrères présents sur place et éventuellement des personnes présentes avec qui on a établi des confiances (fixeurs, riverains, etc.).
- ✦ Les neutres : globalement les riverains et les badauds sont neutres. Ils peuvent toutefois devenir des acteurs potentiellement alliés mais quelquefois aussi des sources de piège (qui choisissent de ne pas réagir) même dans des moments difficiles.
- ✦ Les sources de danger : puisque la place des journalistes reste essentiellement du côté des FDS, les premières sources de danger restent les manifestants malgré eux. Par ailleurs, les FDS dans le feu de l'action peuvent également devenir intentionnellement ou non une source d'agression pour les journalistes.

Relations avec les manifestants

A cause du phénomène de foule, les manifestants sont imprévisibles. Toutefois, des comportements habituels peuvent être observés dans les débuts des manifestations : attroupement progressif, émergence ou apparition de leaders, tentative de négociation avant l'affrontement. Pour bien se préparer voici quelques conseils :

- ✦ identifier les leaders de la manifestation ou au moins un proche des leaders ;
- ✦ établir une relation avec le leader des manifestants ou lui demander des informations sur la suite pour mieux anticiper l'évolution de la manifestation ;
- ✦ sonder les manifestants de manière à établir une prévision de l'évolution de la manifestation : température, comportements partagés, nouvel objectif, etc.

Relations avec les Forces de Défense et de Sécurité

Les FDS devront rester des alliés des journalistes. Ce sont leurs premiers protecteurs. Toutefois, les expériences ont montré que sur un terrain sensible, des frictions, voire des altercations peuvent se produire entre les deux corps. A Madagascar, une convention de coopération a été signée entre l'OJM, les FDS et le Ministère de la justice sans pour autant entrer dans les détails relatifs à la gestion des manifestations. En ce sens, il revient à chacun de faire l'effort de collaborer. Voici quelques indications à suivre pour le corps des journalistes :

- si les conditions sont encore favorables : rencontrer les leaders ou des adjoints des FDS et demander des informations préliminaires sur les mesures qui seront prises ;
- durant les moments difficiles, s'intégrer dans les dispositifs des FDS assurerait déjà la sécurité à 70 % ;
- autant que possible : garder une communication constante avec le leader des FDS durant les évènements.

Emplacement et abri

Des règles de base restent en vigueur dans toute manifestation pour un journaliste :

- ne jamais se placer du côté des manifestants ;
- autant que possible, le mieux est de se placer derrière les FDS ;
- face à des attaques plus dangereuses : éviter des abris de faible épaisseur (portière, fenêtre, table, etc.) et favoriser ceux d'épaisseur plus conséquente (comptoir, moteur de la voiture, mur épais, tronc d'arbre, etc.). Il en va de même pour la dureté des abris choisis (choisir les objets en pierre, en fer ou en métal épais à la place des matériaux en bois, en plastique ou en verre)

A éviter impérativement

- ✘ Se placer entre FDS et manifestants. Même si la tentation d'avoir de belles images et de scoops est forte, c'est l'endroit le plus dangereux de la zone, même pendant les instants d'accalmie.

Transports et déplacements

Suivant l'évolution du mouvement, les déplacements peuvent être nécessaires. Ils peuvent se faire soit à pied, soit via un moyen de locomotion, dépendant de la distance à parcourir et des dangers encourus. Il est conseillé à l'organe de presse de mettre à disposition du journaliste un moyen de déplacement permanent et disponible à tout moment au cours d'un mouvement social. Pour une ou deux personnes, les motos sont les plus pratiques à Madagascar ; pour le déplacement groupé de toute une équipe de trois personnes ou plus, une voiture est nécessaire. Dans tous les cas, quelques instructions restent valables :

- les moyens de transport et de déplacement doivent être visibles et identifiables. Ainsi, les motos et les véhicules de transports doivent porter l'écriteau « PRESSE » ;
- l'écriteau doit être visible, lisible de nuit comme de jours et en temps pluvieux;

- dans des situations où les besoins de déplacement d'urgence peuvent être réels, le conducteur restera en alerte avec le matériel roulant au plus près possible du journaliste.

Disposition à prendre en cas d'attentat à la bombe :

Si ce cas se présente, respecter scrupuleusement les points suivants :

- toujours considérer le fait que ladite bombe peut exploser à tout moment ;
- la zone d'impact dépend du volume de l'explosif, plus le volume est grand, plus la zone d'impact est grande ;
- ne jamais s'approcher de l'explosif, ne jamais violer le périmètre de sécurité ;
- seuls les personnels de l'armée peuvent avoir l'habilité à manipuler un engin explosif, seul un personnel de l'armée sera apte à proclamer un désamorçage effectué, dans le cas contraire, ne pas y prêter attention.

3.4. Se protéger des dangers numériques

Dans des situations instables, les journalistes peuvent rapidement devenir des cibles d'un côté comme de l'autre. Parmi les pratiques les plus constatées durant les manifestations : la confiscation ou la détérioration de matériels, l'obligation d'effacement de données ainsi que les menaces sont courantes. Or, en cas de perte ou de confiscation de matériel (qui est illégale), vous mettriez à risque l'ensemble de votre travail et celui de votre organisation.

Ainsi, il est important de prendre des mesures de protection supplémentaires :

- Lorsque vous allez partir, convenez d'un protocole de communication avec le superviseur et les proches : "Je vous contacterai à xx heure, à partir de tel canal, [depuis le numéro xxx, ou sur *Whatsapp*, …]", "Si je ne suis pas joignable d'ici xx heures, contactez xxxxx". Il peut être une bonne pratique d'apprendre aux membres de votre famille à localiser votre téléphone en cas de besoin ;
- Activer le verrouillage automatique court (30 sec max) sur votre appareil ;
- Configurer l'option d'appel d'urgence (bouton panique) si votre téléphone le permet, et familiarisez-vous avec son utilisation ;
- Désactiver les options de déverrouillages biométriques (empreintes digitales, reconnaissance faciale ou vocale).

Attention !

Il est souhaitable de supprimer préalablement les informations sensibles de vos profils publics (adresses, opinions politiques, informations familiales, etc.) pour éviter que des personnes voulant vous nuire y trouvent des raisons et des moyens pour vous attaquer.

Chapitre 4.

En cas de convocation ou d'arrestation

Il arrive que des particuliers, des institutions publiques ou des structures privées portent plainte contre les journalistes auprès de la police, de la gendarmerie ou au Parquet (tribunal). C'est un droit que chacun peut exercer. En cas de plainte, de convocation ou d'arrestation, le journaliste a droit à une protection. Il doit connaître ces droits ainsi que les bases de la procédure légale applicable. Il doit aussi être capable de faire face à une violation de procédure.

4.1. Suivre les procédures classiques

Le processus habituel suit les étapes ci-après :

Etape 1 :

Une plainte déposée à la police/gendarmerie ou au Parquet par le plaignant.

Étape 2 :

Convocation par écrit ou quelquefois via un appel téléphonique du journaliste par l'entité chargée de la plainte. Souvent, le motif d'une convocation est « une affaire vous concernant » / « raharaha mahakasika anao ».

Etape 3 :

Le journaliste/la rédaction contacte son avocat. Celui-ci sera impliqué dans la gestion de la situation. L'avocat doit demander à l'enquêteur de préciser si la personne convoquée est témoin ou soupçonnée, effectivement un témoin n'a pas besoin d'avocat/défenseur.

Etape 4 :

- Il peut y avoir citation directe qui permet de convoquer le directeur de publication à comparaître devant le tribunal.
- Il peut aussi y avoir : enquête préliminaire (police/gendarmerie), suivi d'un déferrement au Parquet, puis audience au tribunal.
- Pour les infractions graves, il peut y avoir instruction (par le juge d'instruction) avant l'audience au tribunal.
- Une garde à vue dure normalement 48 heures.
- Après enquête ou déferrement, la personne soupçonnée peut être libérée ou détenue :
  - elle peut être libérée et ne pas être poursuivie (classement sans suite) ;
  - elle peut aussi être mise sous contrôle judiciaire (libre mais sous certaines conditions : se présenter régulièrement à la police/gendarmerie/au tribunal, ne pas quitter la localité, s'abstenir d'actions liées à l'infraction, etc) ;
  - elle peut aussi être détenue en attendant la suite de l'enquête ou le procès.

Attention !

- Pendant l'enquête, l'avocat/défenseur a le droit d'assister aux interrogatoires, aux confrontations et aux perquisitions. Il peut faire des observations, qui sont consignées dans le PV.
- Le journaliste a le droit à une visite médicale pendant la garde à vue, à la demande du journaliste ou de son avocat.
- Tout ce qui a été envoyé sur internet à un moment donné doit être considéré comme public ou risque de devenir public.
- Les outils de stockage maintiennent des traces des données stockées même après leurs suppressions. Ces données peuvent être récupérées.
- La communication entre l'avocat et son client est couverte par le secret professionnel. Les conversations, messages, fichiers, images, sons, vidéos, etc. échangés entre l'avocat et son client sont confidentiels. Le matériel électronique, les documents, les bureaux, les véhicules appartenant à l'avocat sont inviolables. L'avocat a fait serment de préserver le secret professionnel.

A éviter impérativement

✘ Laisser ou déverrouiller son téléphone avant d'en avoir discuté avec un avocat ;

✘ Se connecter à ses comptes numériques avant d'en avoir discuté avec un avocat.

Astuces

Dans la reconstitution des faits, le journaliste dispose l'avantage de détenir des preuves enregistrées. Si cela l'aide dans la défense, il est donc possible, voire conseillé, de :

- visionner et analyser les enregistrements réalisés avec les matériels d'enregistrement ;
- en cas de bavure enregistrée, procéder à un constat d'huissier (constater dans un procès-verbal).

4.2. En cas de violations de procédures

Il se peut qu'une ou des violations de procédures se produisent. La défense dispose du droit d'en faire le constat et de les utiliser. L'avocat (ou une cellule de protection) devra en être informé. Ci-après les situations par lesquelles ces violations peuvent arriver :

✦ l'enquêteur n'a pas évoqué l'article 53 du Code de Procédure Pénale, ou le juge l'article 53 bis : sur le droit d'avoir un avocat ou un défenseur ;

✦ le Procès-Verbal n'est pas conforme avec le contenu de l'enquête. Nota : toujours demander à bien lire le PV et à apporter des modifications – si nécessaires – avant de signer ;

- une demande de dépôt de pièces justificatives n'a pas été acceptée ;
- les perquisitions et les saisies n'ont pas été approuvées par écrit par l'inculpé ou par deux officiers de police ou par deux témoins ;
- un garde-vue dépassant les 48 heures. Noter quand même que : au-delà de 48 heures, si le magistrat n'est pas présent, elle peut durer jusqu'à 3 jours. (Si l'arrestation a eu lieu loin du lieu d'enquête, on peut ajouter 1 jour par 25 km, sans dépasser 12 jours au total.)

Attention !

- Sans forcément se référer à des articles de loi, il faut aussi faire preuve de bon sens, surtout dans les situations difficiles (dossier sensible, émeutes, manifestations). En principe, le journaliste est protégé par la loi et les forces de l'ordre ont l'obligation de l'assister dans cette protection.
- Cependant, *« nul ne peut se prévaloir de sa propre turpitude »* : cet adage signifie simplement que si le journaliste se met délibérément en danger, il peut se retrouver non seulement hors de la protection de la loi et des forces de l'ordre, mais peut-être même être en danger physiquement.

Conclusion

Protéger les journalistes n'est pas un luxe. C'est une condition de survie — pour eux, pour les médias, et pour la démocratie elle-même. Ce manuel a voulu donner des repères concrets, applicables au quotidien, face à la diversité des risques que rencontrent les professionnels de l'information à Madagascar.

Dans un environnement souvent instable — marqué par la précarité des moyens, les tensions politiques, les défis technologiques et parfois l'hostilité de certains acteurs — la sécurité du journaliste ne peut pas dépendre du hasard. Elle repose sur des réflexes clairs, des rituels constants et une culture de la prévention. Chaque rubrique de ce manuel insiste sur un point essentiel : la protection ne se décrète pas, elle se construit, pas à pas, avec méthode.

Au quotidien, cela commence avec des rituels de sécurité simples au desk. En mission sensible, il s'agit d'aller plus loin : comprendre le terrain, anticiper les comportements, renforcer les dispositifs de sécurité physique et numérique. En situation de crise — manifestations, émeutes, tensions sociales — la vigilance devient absolue. L'émotion, la rapidité, la pression ne doivent jamais effacer les principes de base : rester légal, rester lucide, rester vivant.

Mais la protection du journaliste n'est pas seulement une affaire d'individus prudents. C'est aussi une responsabilité collective. Tout acteur interne comme externe est concerné. Les dirigeants de presse en particulier doivent instaurer des protocoles internes, fournir des formations, souscrire des assurances, et créer un climat où la sécurité n'est pas perçue comme un frein au travail, mais comme une condition de performance.

À l'ère du numérique, la vigilance doit aussi se digitaliser. Sauvegardes sécurisées, communications chiffrées, gestion rigoureuse des sources : chaque clic compte. L'exposition numérique d'un journaliste peut le rendre vulnérable bien au-delà de la salle de rédaction.

Enfin, en cas de convocation ou d'arrestation, la connaissance des procédures légales et des droits fondamentaux est une arme. La peur recule quand on sait comment réagir, qui contacter, et sur quels textes s'appuyer.

Ce manuel n'a pas la prétention de tout couvrir, mais il trace un cadre de référence. À chacun maintenant d'en faire un outil vivant, évolutif, partagé. Car protéger les journalistes, c'est protéger le droit du public à être informé. Et ce droit, lui, n'a pas de prix.

Annexes

Annexe I.
Les bonnes pratiques numériques

A faire impérativement

- ✔ Limiter la diffusion d'informations personnelles au strict nécessaire.
- ✔ Si vraiment nécessaire, décaler la publication d'informations sur les déplacements (voyages, trajets, absences, etc.).
- ✔ Maintenir une veille active concernant vos informations clés pour être alerté en cas de fuite : nom, adresse postale, numéro de téléphone, adresse email.
- ✔ Utiliser systématiquement les paramètres de sécurités renforcés sur les comptes numériques (authentifications à double facteur, alertes de connexion).
- ✔ Mettre à jour le système et les applications régulièrement.
- ✔ Utiliser un anti-malware de confiance et scanner régulièrement.
- ✔ Restreindre les autorisations des applications au strict minimum (micro, caméra, localisation).
- ✔ Si vous suspectez une infection : déconnecter l'appareil d'Internet, alerter l'équipe sécurité/IT de votre organisation.

A éviter impérativement

- ✘ publier emails, numéros de téléphone, et adresses physiques. Si vous avez réellement besoin de mettre publiquement un numéro de téléphone ou une adresse email, acheter un numéro de téléphone dédié, et créer une adresse email spécialement pour l'occasion.
- ✘ installer des applications obtenues en dehors des dépôts officiels (Play Store, App store).
- ✘ brancher une clé USB inconnue, utiliser de câbles de téléphone inconnus, charger son téléphone sur des ports USB publics. Se connecter sur les réseaux Wifi publics. Et si c'est vraiment nécessaire, penser à utiliser un réseau VPN.
- ✘ croire que les attaques numériques (phishing, usurpations, deepfakes) « n'arrivent qu'aux autres » ; ainsi ne jamais sous-estimer la vitesse de diffusion d'un faux contenu.

⚠ Attention !

- Quelquefois, la divulgation des informations personnelles provient de notre entourage. D'où l'importance de sensibiliser également amis et familles.
- Pour les personnes de notoriété, ayant besoin d'avoir une visibilité publique de certaines informations, il est peut-être nécessaire de renforcer la protection en investissant dans des mesures plus poussées (Exemple : vérifications de comptes sur les réseaux sociaux).

Annexe II.
Les structures de protection à Madagascar
(fonctionnelles en 2025)

Cellule de protection des Journalistes – Projet « Manehoa » - ILONTSERA

Lancé en **octobre 2024** et **pour une durée de 03 ans**, ce projet vise à **protéger les journalistes** à travers une **cellule de veille médiatique** sur les violations de la liberté de la presse et d'expression. Il offre également un **soutien psychologique**, ainsi qu'un **accompagnement juridique et judiciaire** aux journalistes concernés.

Contacts : 038 11 181 54 / manehoa.ilontsera@gmail.com

Projet « A-Viavy » – ILONTSERA

Mis en œuvre depuis **décembre 2024**, ce projet cible spécifiquement les **femmes journalistes à Madagascar**. Il vise à les protéger contre les **menaces** et les **pressions**, en leur fournissant une **assistance juridique** (conseils et accompagnement pour la constitution de dossiers).

Contacts : 038 43 345 25 / gmdf.ilontsera@gmail.com

Cellule de conseil juridique de l'Ordre des Journalistes de Madagascar (OJM)

Cette cellule assure un **soutien juridique** aux **journalistes en danger** et œuvre à la défense de leurs droits professionnels.

Contacts : bureau@ojm.mg

Projet MAIKA – Transparency International Initiative Madagascar (TI-MG)

En **juin 2025**, TI-MG a organisé des formations sur la sécurité physique et la sécurité des données destinées aux **journalistes d'investigation**, notamment ceux du **réseau Malina**.

Contacts : 034 96 418 79 / contact@transparency.mg

The Committee to Protect Journalists (CPJ)

Organisation internationale qui **promeut la liberté de la presse** et **défend les droits des journalistes** à travailler sans crainte de représailles. Le CPJ intervient dans le monde entier pour **protéger la libre circulation de l'information**.

Pour en savoir plus : https://cpj.org/about/video / info@cpj.org

Le Service International pour les Droits de l'Homme (ISHR)

L'ISHR agit à l'échelle mondiale pour **défendre les droits humains** de manière **globale et inclusive**, en soutenant notamment la protection des défenseurs des droits et des journalistes.

Pour en savoir plus : https://ishr.ch/fr/notre-travail / information@ishr.ch

Association des Femmes Journalistes (AFJM)

L'AFJM œuvre pour la **promotion et la protection des femmes journalistes** à Madagascar, en soutenant leurs droits professionnels et leur sécurité dans l'exercice du métier à travers des formations ou conseils.

Contacts : nadiaraonimanalina@gmail.com / https://www.facebook.com/profile.php?id=100095284580346

Annexe III.
Autres contacts utiles

Service de la cybercriminalité de la Police Nationale :

Contact : 034 05 703 76

Service de la cybercriminalité de la Gendarmerie Nationale (Toby Ratsimandrava) :

Contact : 034 14 006 55

Le journaliste est invité à se procurer et à mettre à jour :

- les contacts des principaux responsables de la sécurité publique et de leurs adjoints de la localité où le journaliste exerce ou va exercer ;
- les contacts des principaux responsables et adjoint des leaders de l'Etat-Major Mixte Opérationnel (EMMO) avec celui du Préfet de police dans la localité où il exerce ou va exercer ;
- le contact d'avocats et d'huissiers de la localité où le journaliste exerce ou va exercer ;
- le contact des centres hospitaliers où le journaliste exerce ou va exercer.

ILONTSERA
Media Matters Madagascar
Observatoire des Médias et de la Communication
Ivompandalnana ny fantolom'ny sehasera marolafika eto Madagasikara

ONG ILONTSERA

Près lot VS 124 Miandrarivo Ambanidia, Antananarivo - Madagascar
Tel. +261 38 13 130 79 / +261 38 29 053 89 / +261 38 44 605 82
E-mail : mediamattersm@gmail.com - communication-manager@ilontsera.mg
Web : www.ilontsera.mg

Internews
Local voices. Global change.

Financé par
l'Union européenne