CAPJC
المركز الإفريقي لتدريب الصحفيين و الإتصاليين
CENTRE AFRICAIN de PERFECTIONNEMENT des JOURNALISTES et COMMUNICATEURS

GUIDES PRATIQUES
DU JOURNALISTE TUNISIEN

SECURITE ET CYBERSECURITE POUR LES JOURNALISTES TUNISIENS

MEDIA UP
Programme d'Appui aux Médias en Tunisie

Table des matières

Table des matières

Table des matières

AVERTISSEMENT

Ce guide a été élaboré dans le cadre du Programme d'appui aux médias tunisiens (PAMT-MediaUp) de l'Union européenne, géré et mis en œuvre par le Centre africain de perfectionnement de journalistes et communicateurs (CAPJC), bénéficiant de l'assistance technique du consortium mené par Particip et comprenant France Médias Monde, Deutsche Welle, Ansa et Article 19 Tunisie.

Son contenu relève de la seule responsabilité de ses auteurs et n'engage ainsi en rien l'Union européenne, ses Etats membres, le CAPJC ou les différents membres du consortium.

Les auteurs tiennent ici à remercier sincèrement l'ensemble des interlocuteurs rencontrés pour leur disponibilité et la qualité de leurs contributions.

Ils s'excusent par avance de toute erreur qui, malgré leur vigilance, pourrait encore s'être glissée dans ce guide.

Il faut préciser enfin que le masculin est utilisé dans ce document de manière générique, sans discrimination de genre et dans le seul but d'alléger le texte.

- Mise en page : Smartic: www.smartictunisie.com / Tél (+216) 50 620 849
- Traductions en arabe : MM. Mohamed Ali Habachi, Lotfi Arfaoui, Ali Jelliti.

LES AUTEURS

Zied Dabbar

- Zied Dabbar est journaliste tunisien, spécialisé en sécurité des journalistes depuis 2011.
- Il a formé environ 500 journalistes dans la région MENA (Tunisie, Libye, Algérie, Mauritanie, Egypte, Palestine, Syrie et Liban) ainsi que dans plusieurs pays subsahariens, dont le Mali.
- Depuis 2017, il chapeaute le Centre de sécurité des journalistes qui relève du Syndicat national des journalistes tunisiens (SNJT). Il intervient également dans des séminaires et colloques internationaux sur la question de l'impunité des crimes commis contre les journalistes.
- Il travaille actuellement dans le cadre d'un partenariat entre la Fédération internationale des journalistes (FIJ), le SNJT et les établissements de médias de service public (Radio Tunisienne et Télévision Tunisienne) sur l'élaboration d'un protocole de sécurité pour leurs journalistes.
- Il est également membre du bureau exécutif du SNJT et vice-président de la Fédération africaine des journalistes (FAJ).
- Pour la période 2019-2021, il a été élu au comité exécutif de la Fédération internationale des journalistes (FIJ).

LES AUTEURS

Othman Ben Mansour

- Conçoit et anime des formations en ligne et en présentiel sur les enjeux et bonnes pratiques de la cybersécurité à destination des personnels non techniques.
- Il a une expérience de plusieurs années en gestion, conception et organisation de conseil et de formation pour les professionnels des médias, notamment dans le cadre de projets internationaux.
- Othman est fondateur et dirigeant de Paladax Cyber-Defense, entreprise basée à Paris spécialisée, entre autres, dans la dimension RH en cybersécurité.

LE SNJT ET LA SÉCURITÉ DES JOURNALISTES

Depuis 2011, le Syndicat national des journalistes tunisiens (SNJT) a entamé, en partenariat avec la Fédération internationale des journalistes (FIJ) un vaste programme en faveur de la sécurité des journalistes en Tunisie, à travers des formations dédiées aux journalistes tunisiens. Ces formations ont été organisées dans les différentes régions de la Tunisie (Tataouine, Médenine, Gafsa, Le Kef, Tabarka, Sfax, Monastir, Mahdia, Sidi-Bouzid, Kasserine, Tunis, Kairouan). Environ 200 journalistes ont ainsi été formés ces 8 dernières années. Depuis 2016, le SNJT a créé le Centre national pour la sécurité des journalistes. Ce centre comprend 4 unités (monitoring, documentation, assistance légale, formation). L'unité de monitoring, principale composante du centre, a pour mission d'établir une veille systématique et « en temps réel » des violations de la liberté de la presse, d'enquêter avec rigueur et impartialité sur ces violations, de rédiger et de diffuser des communiqués, cautionnés et appuyés par le SNJT, et de fournir les informations qui serviront de base aux actions en justice initiées par le syndicat. Elle comprend une coordinatrice, deux enquêteurs et un avocat.

Dans son travail, l'unité de monitoring procède par une méthodologie claire et rigoureuse et surtout indépendante. Un communiqué est publié à chaque agression, l'unité prouve un cas d'agression, d'attaques, etc. à l'encontre des journalistes. L'unité intervient également auprès des autorités (ministère de l'Intérieur, Défense nationale, et autres administrations) en cas d'agression des journalistes pour suivre l'affaire et surtout lutter contre l'impunité des agresseurs des journalistes. L'unité publie des rapports annuels recensant les cas de violations et l'évolution des textes, une note trimestrielle sur une thématique précise et un point mensuel sur les faits documentés par l'observatoire.

LE SNJT ET LA SÉCURITÉ DES JOURNALISTES

Mais ce travail méthodique mené par l'observatoire n'est que le recensement, en aval des problèmes liés à la sécurité des journalistes. Il nous a semblé utile de tirer de ces expériences, de ce vécu à la fois des journalistes et de ceux qui les défendent, les leçons, les règles, les bonnes pratiques qui permettront d'améliorer, de manière pratique, la sécurité des travailleurs de l'information en Tunisie. D'où la formule d'un « guide pratique », exposant clairement et concrètement ce qu'il faut faire – ce qu'il ne faut pas faire aussi –pour assurer dans de meilleures conditions la lourde tâche d'informer en Tunisie.

Ce guide est le produit de l'expérience de ses deux auteurs ; Zied Dabbar et Othman BenMansour ont aussi une très bonne connaissance de la question sécuritaire dans nombre d'autres pays, plus ou moins proches de la Tunisie. De nombreuses organisations nationales, internationales, régionales (Unesco, Fédération internationale des journalistes, Reporters sans frontières) ont publié des guides, rapports ou manuels sur la question. Celui que vous avez sous les yeux ne les ignore pas, s'en inspire parfois, mais il s'adresse avant tout spécifiquement aux journalistes tunisiens, en s'adaptant au contexte général tunisien, ou encore à celui de certaines régions, zones ou contextes culturels propres. Il se donne pour objectif de parler directement aux confrères et consoeurs tunisiens, toutes catégories confondues, pour leur apporter les réponses aux questions qu'ils ne se posent pas toujours sur leur sécurité, au quotidien ou dans les situations exceptionnelles qu'ils affrontent parfois.

Aussi, ce guide se donne l'ambition de donner à chacun les moyens d'assurer davantage sa sécurité dans l'exercice du métier, pour que, in fine, le nombre « d'accidents » et d'agressions diminue, mais aussi que ces dernières donnent davantage lieu à des poursuites contre leurs auteurs, afin qu'informer ne soit plus une activité dangereuse.

INTRODUCTION

Les journalistes tunisiens cibles d'attaques et d'agressions

Pas moins de 150 cas recensés, c'est en moyenne le nombre annuel d'agressions et d'attaques à l'encontre des journalistes en Tunisie. Pour la période d'octobre 2017 à novembre 2018, 194 journalistes ont été victimes de 136 agressions et attaques selon l'unité de monitoring du Centre national pour la sécurité des journalistes du SNJT. Pour les années 2011-2015, le SNJT a répertorié 450 agressions à l'encontre de journalistes.

Dans le rapport annuel 2018 de l'unité de monitoring du SNJT, il apparaît que les journalistes de terrain et parmi eux les photographes sont les plus ciblés par ces attaques, avec au moins 100 victimes. La tendance reste la même pour 2019 (220 journalistes agressés), avec notamment 79 cas relevés au cours du processus électoral, d'août à octobre. Les attaques connaissent parfois une légère baisse pendant deux ou trois mois consécutifs, mais, d'une façon générale, les journalistes tunisiens se trouvent de plus en plus menacés et attaqués.

Les types d'agressions répertoriés varient entre harcèlements verbaux, attaques physiques, menaces publiques et poursuites judiciaires sur la base de leurs opinions, leur travail d'investigation ou même pour la prise des photos dans des endroits publics ne nécessitant pourtant pas d'autorisation préalable.

De novembre 2018 à novembre 2019, la répartition géographique des agressions montre que près d'un tiers (88 sur 220) a eu lieu sur le « Grand Tunis ». Cela n'empêche pas d'observer des agressions qualifiées comme graves (attaques physiques et poursuites judiciaires) à l'encontre des journalistes dans plusieurs régions, à Sfax, Gafsa et Beja en l'occurrence.

INTRODUCTION

A vrai dire, ce phénomène devient de plus en plus répandu avec la persistance d'une culture d'impunité des agresseurs des journalistes. Ces agresseurs, en majorité des fonctionnaires, des policiers, mais aussi parfois des responsables politiques, bénéficient en général d'une impunité totale, le ministère public restant passif et réticent à ouvrir une enquête en cas d'attaques contre les journalistes.

La situation se complique encore avec le désengagement des entreprises médiatiques dans la sécurité de leurs journalistes. A commencer par l'absence des formations en la matière, par l'absence de protocoles de sécurité au sein des médias tunisiens et, pour finir, avec l'inexistence des matériels de protection des journalistes.

Ce guide se propose de traiter la sécurité sous trois aspects principaux : légale et juridique, physique et numérique.

CHAPITRE 1 : LA PROTECTION DES JOURNALISTES DANS LA LÉGISLATION TUNISIENNE ET LES DISPOSITIFS JURIDIQUES

Ce chapitre aborde la protection des journalistes tunisiens telle qu'elle est prévue par la législation nationale. La première partie est consacrée à la protection juridique du journaliste, de ses sources ainsi que de son droit à l'accès à l'information. La deuxième partie, présente les différentes étapes à suivre par un journaliste pour déposer plainte en cas d'agression. Le journaliste est appelé à suivre cette démarche s'il veut porter plainte contre toute agression ou encore pour mieux suivre la plainte déposée automatiquement par le SNJT en cas d'agression contre tout journaliste.

A - DÉFINITIONS ET DONNÉES DE BASE

Qui est journaliste ?

La définition du statut du journaliste en Tunisie est définie par la convention cadre du SNJT et par le décret - loi 115 - 2011.

La convention collective cadre pour les journalistes tunisiens du SNJT établit que « est considéré comme journaliste professionnel [...] toute personne physique dont la profession, d'où il tire ses principales sources de revenus, consiste à fournir des services, à une ou plusieurs entreprises, de manière permanente ou non, y compris la situation du journaliste indépendant. Son travail consiste, notamment, en la réalisation de contenus journalistiques, la rédaction, la contribution à la rédaction, les correspondances et la photographie de presse ».
L'article 7 du décret-loi 115 de 2011, définit également le statut de journaliste. (Voir annexe 2)

Le journaliste est-il protégé ?

D'après la législation en vigueur, le journaliste tunisien bénéficie d'une protection. La convention collective cadre pour les journalistes tunisiens du SNJT, dans son article 24 relatif à la santé et la sécurité professionnelle, évoque « la protection nécessaire des journalistes contre les agressions auxquelles ils risquent d'être exposés ». (Voir annexe 2).
Le décret-loi 115 de 2011 (article 14), en application jusqu'à aujourd'hui, procure une protection pour les journalistes dans l'exercice de leur métier. Toute agression ou même atteinte verbale à l'encontre d'un journaliste est considérée comme outrage à un fonctionnaire public assimilé. (Voir annexe 1).

Les sources du journaliste sont-elles protégées aussi ?

Les sources sont protégées sauf exceptions. Le décret-loi 115, dans son article 11, évoque la protection des sources pour les journalistes et même pour toute personne « contribuant à la confection de la matière journalistique ». Les enquêtes, ainsi que tout acte de recherches, d'investigations ou de mise sur écoute à l'encontre des journalistes [par les autorités] pour découvrir leurs sources sont considérées comme une violation. Néanmoins, pour des motifs impérieux de sûreté de l'État ou de défense nationale, le journaliste est dans l'obligation de révéler ses sources, et cela seulement sous contrôle de l'autorité judiciaire. (Voir annexe 1).

Ces exceptions sont également prévues dans l'article 37 de la loi organique relative à la lutte contre le terrorisme et la répression du blanchiment d'argent. (Voir annexe 2).

Un journaliste peut-t-il accéder à toute information ?

En Tunisie, l'accès à l'information est réglementé par la loi organique N° 2016-22 du 24 mars 2016, relative au droit d'accès à l'information. Les exceptions sont prévues dans le chapitre 4 de la dîte loi. (Voir annexe 2).

B - EN CAS D'AGRESSION

Que faire en cas d'agression ?

En cas d'agression, le journaliste doit porter plainte (voir ci-dessous). Avant tout, il doit s'adresser au centre de sécurité des journalistes (unité de monitoring et l'unité d'assistance légale) du SNJT.

Les types d'agressions et types d'agresseurs

D'après les statistiques de l'unité de monitoring du Centre de sécurité des journalistes relevant du SNJT, il existe de nombreux types de violation et d'attaques contre les journalistes :

- Agressions physiques (attaques physiques) ;
- Agressions verbales (insultes, propos diffamatoires) ;
- Empêchements de travailler ;
- Saisies de matériel ;
- Dommages causés au matériel de travail ;
- Menaces à l'encontre des journalistes (menaces de poursuite judiciaires ou menaces d'agressions) ;
- Incitation à la haine à l'encontre des journalistes en raison de leurs opinions ou des informations qu'ils publient.

D'après les mêmes données communiquées par l'unité de monitoring, ces attaques contre les journalistes sont causées par:

- Des agents de sécurité ;
- Des fonctionnaires publics ;
- Des membres des partis politiques ;
- Des syndicalistes ;
- Publics sportifs (supporters).

C - COMMENT AGIR JURIDIQUEMENT APRÈS UNE AGRESSION ?

Un journaliste peut-il porter plainte en cas d'agression ? Comment ?

En cas d'agression dans l'exercice de son travail, le journaliste a le droit de porter plainte auprès du ministère public. La plainte peut être déposée personnellement par le journaliste ou à travers son avocat ou l'avocat du SNJT s'il est requis. C'est la première étape, indispensable, pour poursuivre les agresseurs.

La plainte doit inclure l'identité du journaliste (plaignant), son adresse, son numéro de téléphone. Elle doit être déposée au nom du procureur général du tribunal de première instance. La plainte doit inclure les faits et les détails de l'agression (les insultes, les menaces ou les équipements endommagés). En cas d'agression physique, la plainte doit être accompagnée de certificats médicaux (le journaliste peut prendre des photos des blessures).

Des preuves (vidéos, photos) de l'agression ainsi que l'identité d'éventuels témoins (journalistes ou non) pour qu'ils soient auditionnés. Enfin, le journaliste plaignant doit demander l'ouverture d'une enquête judiciaire à l'encontre du ou des agresseur(s).

Il faut tenir compte que les délais pour déposer une plainte varient selon la nature de l'agression. Pour un délit, la loi prévoit un délai de 3 ans à compter de la date de l'agression. Dans le cas des crimes (tentative de meurtre, incitation au meurtre, violence entraînant une incapacité physique permanente de plus de 20%), le délai de dépôt de la plainte est de 10 ans à compter de la date de l'attaque.

La plainte doit être déposée (en deux copies, avec les copies originales des preuves) auprès du procureur général tout en tenant compte du principe de la compétence territoriale. C'est-à-dire elle doit être déposée au tribunal couvrant géographiquement l'endroit où le crime a été commis, ou le lieu où la personne a été localisée, ou encore le lieu où elle a été retrouvée. Avant de déposer sa plainte, le journaliste blessé doit recueillir les preuves, l'identité des témoins, l'identité de l'agresseur ou des agresseurs, et fournir un dossier médical, si nécessaire.

Le journaliste plaignant doit avoir une copie de la plainte qui comprend la date, le numéro de la plainte avec un tampon du tribunal. Cette copie peut servir comme décharge.

Si le journaliste est agressé dans une zone rurale ou éloignée, il peut soumettre sa plainte au tribunal cantonal compétent de la même manière et dans les mêmes conditions.

Le sort de la plainte

Le journaliste peut contacter à tout moment le secrétariat du procureur général pour connaître le sort de sa plainte.
Après avoir examiné la plainte, le procureur général ou son assistant peuvent prendre l'une des décisions suivantes :

- Refuser la plainte (absence de crime ou pour son caractère civil, etc.) ;
- Demander au journaliste plaignant de fournir certaines données complémentaires (adresse du plaignant, preuves, etc.) ;
- Renvoyer la plainte aux forces de sécurité (police en zone urbaine et garde nationale en zone rurale) ;
- Le procureur général peut transmettre la plainte également à un juge d'instruction au cas où l'agresseur est une personne inconnue. L'objectif est de dévoiler l'identité de l'agresseur ;
- Dans certains cas, le ministère public peut procéder à l'audition du journaliste plaignant. Par la suite, l'assistant du procureur prendra en charge l'audition du plaignant. Le juge cantonal peut également mener les investigations.

Le journaliste doit recevoir du secrétariat du procureur général le numéro de la plainte, sa date ainsi que le service de police judiciaire en charge de l'enquête.
En cas de besoin, le journaliste pourra s'adresser à l'organe chargé de l'enquête (brigade criminelle, garde nationale) pour demander à être auditionné afin d'accélérer les procédures.

Procès-verbaux de police judiciaire

Le journaliste doit avant tout respecter les délais de convocation pour être auditionné par la police judiciaire.
Le journaliste plaignant peut faire amener les témoins. Il peut également exiger leur audition s'ils s'abstiennent.
Le journaliste, en sa qualité de plaignant, peut exiger la présence de son avocat lors de son audition, conformément à la loi N° 5/2016 du 16 février 2016.

Les propos du journaliste plaignant, son identité, ses coordonnées doivent être incluses dans un procès-verbal (PV) portant un numéro, une date, ainsi que l'identité de l'officier de police judiciaire.
Le journaliste plaignant doit signer le PV après vérification de ses propos. De même que son avocat, l'officier de police judiciaire ainsi que l'agent chargé de l'écriture du PV.

Que contient un procès-verbal ?

D'une façon générale, le PV doit inclure :

- La présentation de la plainte, les différentes procédures ; le PV sera transmis au ministère public ;
- Le procès-verbal de l'audition du plaignant.

Il peut inclure, selon les cas :

- Le procès-verbal de l'audition des témoins ;
- Le procès-verbal de l'audition du présumé agresseur ;
- Le procès-verbal de saisie de matériel ;
- Le procès-verbal pour saisie médicale au cas où le plaignant n'a pas consulté un médecin ;
- Le procès-verbal de la confrontation entre le journaliste plaignant et le présumé agresseur ;
- Le procès-verbal relatif à la reconnaissance de l'agresseur, si le journaliste ne le connaissait pas préalablement.

Après l'achèvement de son travail, l'officier judiciaire doit renvoyer le dossier au ministère public qui décidera quelle suite à donner. Les décisions peuvent être les suivantes :

- Classer l'affaire pour preuves insuffisantes ;
- Poursuivre l'enquête en cas de crime ;
- Renvoyer l'affaire au tribunal de première instance en cas de délit ;
- Procéder à des investigations complémentaires auprès de la police judiciaire.

En tout cas, le journaliste ou son avocat doit assurer le suivi du dossier. Et si l'affaire est classée par le procureur de la République, quel qu'en soit le motif, le journaliste plaignant ou son avocat ont le droit de demander au procureur que l'affaire soit renvoyée au juge d'instruction ou encore d'engager la procédure pénale devant le tribunal compétent.

Le classement de l'affaire n'empêche pas le journaliste de procéder à une demande écrite. Dans ce cas, en se constituant partie civile, le journaliste plaignant peut demander l'ouverture d'une information auprès du juge d'instruction ou au tribunal chargé du litige. Par contre, le journaliste ne peut plus être entendu comme témoin.
Le journaliste peut revendiquer la réparation par des dommages et intérêts.
Bien noter que si une décision de non-lieu est prononcée, l'inculpé peut demander réparation du dommage occasionné par la mise en mouvement de l'action publique, sans poursuites pénales.

Le jugement

Le tribunal rend un jugement dans l'affaire qui comprend deux branches :

- Pénale, qui comprend la peine infligée au contrevenant ;
- Civile, qui détermine les amendes et les indemnités accordées à la victime. La personne lésée peut ensuite extraire une copie du jugement pour la remettre à la juridiction d'exécution pour le recouvrement des amendes.

Le journaliste et son avocat peuvent procéder à un appel.

CHAPITRE 2 : AVANT LES MISSIONS MÉDIATIQUES (PRÉPARATION)

Ce chapitre montre les étapes à suivre pour préparer toute mission médiatique, afin d'assurer au maximum sa protection. Dans une première partie, il présente au journaliste les techniques et les bonnes pratiques de préparation, de planification ainsi que les actions à suivre pour assurer son déplacement-voyage. L'objectif est de faire une évaluation raisonnée et appropriée du risque avant son départ.

A - PRÉPARATION ET PLANIFICATION

Toute mission journalistique nécessite de la préparation, même les missions les plus faciles, simples ou routinières. Avant de partir, tout journaliste doit se préparer physiquement, mentalement. Il doit aussi préparer son équipe, ses équipements, ses contacts, son budget et même ses vêtements.

Une préparation, c'est un travail de recherche et de collecte d'information. C'est un travail de vérification et d'évaluation du risque. Le journaliste doit se préparer à des scénarios auxquels il pourrait faire face durant son travail sur le terrain.
Pour cela, il faut connaître parfaitement et par détail la mission médiatique : l'endroit, les dates prévues.

Préparer un emploi du temps détaillé pour toute la mission.

Ce plan comprend :

- point de départ et point d'arrivée ;
- agenda (dates et horaires).

Définir les fonctions des membres de l'équipe

Établissez une liste nominative de l'équipe avec les tâches pour chacun.
Vous devez savoir avec qui vous allez travailler et ce que chacun aura à faire.

	Equipier	Tâche (avec précision)	Contacts
1			
2			
3			

Connaître les coordonnées et données personnelles des membres de l'équipe

Regroupez le maximum d'informations sur les membres de l'équipe.

Informations médicales				
Informations utiles en cas d'incidents ou d'intervention médicale				
Groupe sanguin	Medicaments	Maladies	Allergies	Régimes alimentaires

Éléments à prendre en considération

Météorologie et géographie

Il faut connaître et prévoir les conditions climatiques (température, pluie, sècheresse, zone montagneuse ou non) pour savoir comment s'habiller et se préparer face aux conditions climatiques (moyenne de consommation d'eau en précaution contre la déshydratation, pluie, froid...).

Faîtes-vous une idée sur la qualité des routes et des pistes qui mènent vers le lieu de la mission.
Le climat des régions montagneuses (nord-ouest tunisien) diffère du climat du sud (Sahara). La préparation est donc différente.

Contexte politique local

Etablissez une idée précise de la situation politique. Des tensions politiques si elles existent, foyer de tension religieuse ou extrémisme violent, milieu conservateur ou non ?
Evitez d'exposer les logos des médias.

Contexte socio-économique

Renseignez-vous sur le climat social de la région à parcourir dans le cadre de votre travail. Les grèves sont-elles fréquentes ou non ? Le niveau de prix est-il élevé ou non pour préparer le budget nécessaire et pour savoir quelle somme d'argent emporter.

Situation sécuritaire :

Connaître l'historique sécuritaire de la zone du travail pour les trois derniers mois : historique d'attaques contre les journalistes, incidents sécuritaires...
Ces informations serviront à évaluer les risques sécuritaires.

Approche genre :

La situation de la femme dans la zone où le journaliste va travailler est-elle favorable ? Si non, que faire pour éviter les problèmes ?
Pour une femme journaliste, porter une bague peut faire comprendre qu'elle est mariée par exemple.
S'habiller pareillement aux femmes locales pour éviter d'attirer l'attention.
Se voiler pendant la mission si le contexte l'exige.
Ne pas fumer en public.
Éviter le chewing-gum.

Traditions et religions :

Connaître les traditions des autres pour éviter les situations désagréables (les mots, phrases et expressions à éviter, codes vestimentaires, cigarettes, boissons alcoolisées).
Etre prudent. Certains comportements peuvent vous causer des problèmes dans certaines régions du pays. Exemple : tendre la main à une femme, fumer pendant le Ramadan, boire de l'alcool en public...

B - EVALUATION DES RISQUES

Il existe deux types de risques. Des risques liés à la mission ou aux lieux où la mission est programmée et des risques liés au journaliste lui-même ou l'un de ses collaborateurs (fixer, chauffeur, caméraman).

Risques liés à la mission

- **Épidémie :** en cas de couverture d'une épidémie ou d'une catastrophe naturelle, vérifier les risques épidémiologiques auprès du ministère de la Santé ou du centre Pasteur, prendre les vaccins nécessaires et suivre les précautions sanitaires préconisées par les autorités.

- **Mines :** sont concernées les zones frontalières, ainsi que les régions touchées par les actions anti-terroristes (mont Chambi, mont Smana...). Avant une mission, contacter le ministère de la Défense et celui de l'Intérieur qui vous communiqueront les zones minées, les zones militaires fermées, ainsi que les autorisations préalables indispensables avant tout départ..Si une route est présumée minée, prendre sans hésitation un autre itinéraire plus sécurisé.
  Sur place, ne jamais tenter de manipuler une mine.

Risques liés au journaliste

- **Vol :** prendre connaissance de la situation sécuritaire (taux de criminalité, petite délinquance...).
  Prendre soin des équipements électroniques (smartphone, caméra), les dissimuler, ne pas les exposer quand ce n'est pas nécessaire.
  Éviter les bijoux, les colliers et les vêtements inappropriés par exemple dans des quartiers pauvres pour ne pas attirer l'attention.

- **Harcèlement :** ne jamais se déplacer seul(e). Éviter les vêtements de couleurs voyantes (rouge, jaune, blanc...).

- **Embuscade :** se renseigner sur la sécurité des routes avant de les prendre. Éviter les routes dangereuses (accidents fréquents, blocages réguliers, barrages...)
  Changer d'itinéraire en cas de danger. Il faut ainsi prévoir un autre chemin (itinéraire bis) dans votre planning.

- **Arrestation :** Savoir répondre, toujours se montrer coopératif avec les agents des forces de sécurité.
  Dans un premier temps, décliner le statut de journaliste, contacter la rédaction centrale et le cas échéant le SNJT.
  Dans un second temps, contacter un avocat.
  Montrer les autorisations pour les zones militaires fermées.
  Ne jamais prendre sans autorisation une photo des casernes, stations de polices, prisons, tribunaux...

Sources d'informations pour préparer la mission

Les sources d'informations varient entre :

- **Sources ouvertes :** rapports publiés, travaux journalistiques publiés, responsables de départements presse, portes paroles officiels nationaux ou régionaux (département police, garde nationale, gouvernorats), guides de voyages...

- **Sources fermées :** sources personnelles, membres de familles, collègues et confrères...

Équipements personnels :

- Sac à dos multi poches
- Une bouteille d'eau
- Des aliments énergétiques
- Trousse de secours
- Médicaments génériques (calmants), anti-diarrhée, antiallergique, etc....
- Power bank
- Lampe torche
- Mousquetons
- Lingettes hygiéniques
- Un T-shirt compressé
- Masques à gaz, gilets de presse et gilets pare-balles : les correspondants des médias internationaux sont équipés de ces matériels. Les médias, privés et publics tunisiens, devraient eux aussi les mettre à disposition de leurs journalistes partant en zones dangereuses. Ce n'est pourtant pas le cas aujourd'hui. Aussi, dans ces situations, les journalistes concernés peuvent aviser le centre de sécurité dépendant du SNJT qui tentera de trouver une solution adaptée.

Vêtements :

- Chaussures confortables et solides (baskets ou chaussures de marche)
- Pantalon léger avec couleur neutre
- T-shirt ou chemise large pour femme
- Blouson en cas de froid
- Pas d'objets de valeurs (montre, bague, lunettes)
- Sifflet de signalisation à utiliser en cas d'agression

Documents (prévoir 2 photocopies) :

- Carte de presse
- Carte adhérent SNJT
- Permis de conduire
- Autorisation (pour drone, tournage pour sociétés de production),
- Cartes routières, plan des villes
- Carte regroupant les informations de santé (groupe sanguin, allergies, médicaments)
- Ordonnance médicale pour justifier l'utilisation de vos médicaments
- Préparer une liste des contacts d'urgence (rédaction, autorités, hôpitaux, assistance, etc.). Dissimuler cette liste.
- Répartir la monnaie en plusieurs petites sommes, dans plusieurs poches.

NB :

- **Ne partez dans une zone dangereuse que si vous êtes en bonne santé (physique et psychologique)**
- **Évaluez les risques liés à votre mission**
- **Préparez-vous au pire**

C - LES TRAJETS

Choix du véhicule

- Choisissez si possible un véhicule adéquat pour la mission. Exemple : un 4X4 pour les zones montagneuses et de désert. Eviter les voitures luxueuses.
- En cas de possibilité de choisir un modèle de véhicule, il est conseillé de prendre le modèle le plus vendu dans la région ou l'endroit de la mission de manière à passer le plus inaperçu possible.
- Vérifiez vous-même l'état du véhicule (pneus, freins, roues, niveau d'huile, cric, triangle, gilet fluorescent).
- Les journalistes travaillant dans les médias de service public sont obligés de prendre des véhicules parfois inadaptés ; il est conseillé de contacter l'administration et l'alerter. Refuser la mission en cas de risque.

Les taxis

- Ne prenez les taxis qu'en dernier recours. Ne prenez jamais un taxi clandestin. Réservez un taxi en prenant toutes les précautions de confidentialité. Etvitez de prendre le même taxi plusieurs fois.
- Parlez au minimum avec le chauffeur si ce n'est pour obtenir de lui des informations, mais ne lui dévoilez rien à propos votre mission et de votre qualité de journaliste.

Choix d'un chauffeur n'appartenant pas à votre médias

- Si le chauffeur est celui de votre média, briefez-le avant le départ.
  Dans l'autre cas, s'il n'appartient pas à votre entreprise médiatique, votre chauffeur doit être choisi en fonction de son expérience, son état de fatigue, son sérieux et ses habitudes personnelles (jamais d'alcool ou de drogues).

- Excluez les chauffeurs sans permis de conduire. Assurez-vous qu'ils disposent de leur permis et que leur profil est irréprochable (pas d'antécédents avec la police, pas de mauvaise réputation...) Utilisez votre réseau de sources pour valider son profil.

- Insistez sur une conduite sécurisée (pas d'excès de vitesse, respect du code de la route).

- Pour un chauffeur et un véhicule inconnus, prenez une photo d'ensemble (chauffeur et véhicule avec plaque d'immatriculation apparente) et transmettez à votre responsable hiérarchique.

A bord du véhicule

- Négociez le prix avant le départ.

- Fixez des règles : vitesse maximale à ne pas dépasser, respect du code de la route, arrêts fréquents, une distance de sécurité par rapport au véhicule devant.

- Ne divulguez que les informations nécessaires

- Contrôlez la situation en évitant la musique

- Évitez au maximum de parler avec le chauffeur et surtout au téléphone avec vos collègues, vos supérieurs ou même vos proches.

- Évitez au maximum de parler avec le chauffeur et surtout au téléphone avec vos collègues, vos supérieurs ou même vos proches.
- Les portières et vitres du véhicule doivent être fermées.
- Exigez la ceinture de sécurité.

Plan de déplacement

- Identifiez parfaitement l'itinéraire avec le détail des villes à traverser, lieux pour se restaurer et se reposer, stations pour carburant, hôpitaux.
- Découpez la distance totale à parcourir par tronçons et nommez-les. Par exemple découpez une distance de 200 km en 5 fragments et attribuez une lettre pour chaque 40 km (tronçons A, tronçon B, etc.). Informer régulièrement votre rédaction de votre position.
- Des applications comme Google Maps ou Earth sont très utiles.
- Une fois arrivé, évitez de vous garer dans des lieux non surveillés.

Sécurité durant le déplacement

- Essayez de ne pas voyager seul(e).
- Respectez le plan de déplacement.
- Evitez la routine dans vos horaires, les routes et les endroits à traverser.

Passage des points de contrôle (check points) :

- Roulez doucement.
- De nuit, éteignez les phares (mettez en veilleuse) de la voiture et allumerz la veilleuse intérieure.
- Baissez la vitre à l'avance.
- Gardez les mains stables et visibles sur le volant, pas de mouvement brusque pour ne pas provoquer les agents (militaires, garde nationale, police).
- Informez la rédaction en cas de problème.
- Informez après le passage.

Consignes lors du déplacement

- Vérifiez la réservation de votre moyen de transport en cas de recours au transport en commun
- Soyez prudent lors de vos communications téléphoniques
- Évitez les logos (média) et les slogans qui peuvent provoquer des réactions préjudiciables ;
- N'utilisez jamais les écouteurs et les casques car ils vous privent de votre concentration ;
- Préparez une copie, sur un papier, de vos contacts nécessaires pour votre mission (codée et bien cachée) ;
- Identifiez clairement les personnes qui vous accorderont un soutien en cas de besoin ;
- De préférence ne voyagez pas seul. Dans le cas contraire, soyez prudent.

NB : Changez souvent de trajet de sortie et d'entrée. En cas de risque, changez d'itinéraire.

D - SÉCURITÉ DURANT LA MISSION

Principes de sécurité personnelle

- Vous êtes le responsable de votre sécurité : un reportage, une enquête ou une photo ne valent pas votre vie.
- La sécurité personnelle dépend d'une bonne planification.
- Evitez l'excès de confiance.
- Restez modeste et raisonnez comme si chaque mission était la première.
- Anticipez les risques et posez toujours des questions.
- Restez attentif et prudent et évitez l'excès de curiosité.
- Changez de trajet d'entrée et de sortie de son bureau, lieu d'hébergement.
- Identifiez d'avance la meilleure couverture réseau de télécommunications pour savoir quel opérateur utiliser.

Comportement personnel

- Ne publiez jamais les informations de votre mission sur les réseaux sociaux.
- Préparez les documents nécessaires, la carte de presse, les autorisations et l'ordre de mission prêts à être montrés...

- Informez votre famille ou l'un de vos proches de votre mission. En cas de mission critique, ne les informez qu'après avoir terminé la mission.
- En cas de déplacement vers une ville ou village autre que le vôtre, informez l'un de vos collègues, amis ou proches, habitant dans cette ville pour vous aider dans votre mission ou même agir comme fixer si vous en avez les moyens.
- Vous pouvez lui demander de l'aide sans lui annoncer les détails de votre mission. Vous pouvez lui apporter un cadeau comme geste de sympathie avec lui.
- Si vous prenez un fixer, faites le bon choix. Il faut bien se renseigner sur son métier s'il en a un, sa réputation, s'il est discret ou non. Ne prenez jamais un policier ou un membre des forces armées comme fixer.
- Préparez l'argent nécessaire et suffisant et prévoyez deux portes-feuilles ; gardez toujours un « argent de précaution » bien dissimulé.

Choix de l'hébergement

- Il est conseillé d'être attendu lors de votre arrivée (aéroport, zone de travail, ville à visiter) par un ami, collègue, votre fixer...
- Vous avez plusieurs options d'hébergement : hôtel, foyer privé, amis, collègues...
- Le premier critère de sélection de l'hébergement doit être la sécurité.
- Évitez les immeubles ou les hôtels isolés, ou éloignés de l'endroit où vous travaillez.

- Dans certaines villes, vous avez la possibilité de louer une maison pour un certain nombre de nuits. Négociez bien les prix et réservez votre hébergement avant de partir. Ne donnez jamais votre qualité de journaliste au loueur. Évitez les cités et les quartiers de mauvaise réputation ou connus pour les troubles et la criminalité.

- Situation : le lieu d'hébergement doit se situer dans une zone calme, sécurisée et accessible.

- La réputation de l'hôtel vis-à-vis la population locale : dans les régions connues comme très conservatrices, évitez les hôtels qui servent de l'alcool.

- Choisissez un hôtel sécurisé avec un contrôle d'accès (réception 24-24 et un scanner, avec un éclairage extérieur).

- Évitez les chambres situées au rez-de-chaussée et avec balcon pour parer tout risque d'intrusion. Exigez une chambre entre le premier et le troisième étage. et l'avant-dernier étage. En cas d'incendie ou d'attaque, vous disposerez ainsi de davantage de temps pour réagir et vous dégager.

- Ne pas choisir le dernier étage : l'absence de fréquentation du personnel et des clients favorise le cambriolage ou la « visite » de votre chambre.

Une fois installé dans la chambre d'hôtel

- Rangez vos documents et affaires personnelles dans votre valise bien fermée ;

- Derrière la porte se trouve le plan de l'hôtel. Il faut y jeter un coup d'œil pour repérer l'accès et la sortie de secours. Allez personnellement repérer la sortie de secours et les escaliers ;

- Accrochez le panonceau « ne pas déranger » à l'extérieur de votre porte. Si quelqu'un frappe, il faut en déduire que ce n'est pas un membre du personnel de l'hôtel. Si vous n'attendez pas de visite, n'ouvrez pas la porte et informez-vous auprès de la réception. En tout, la réception doit vous prévenir par téléphone si quelqu'un souhaite vous voir.

- Vous pouvez utiliser une cale pour bloquer la chambre de l'intérieur. Une fourchette peut faire l'affaire.
- N'affichez jamais votre numéro de chambre en public (restaurant, bar, café), faîtes attention à ne pas laisser votre clé de chambre visible sur votre table...
- Fermez bien les rideaux ;
- Tenez votre chambre bien rangée ; cela vous permettra de découvrir et remarquer toute intrusion ;
- Si vous êtes dans une zone où le risque d'attentat est élevé , fixez du scotch-collant sur les fenêtres. Utilisez le minimum de lumière dans la chambre et fermez totalement les rideaux ;
- En cas de situation dangereuse, dormez avec vos vêtements et mettez votre sac à dos à la portée de main (prise facile en cas d'urgence) ;
- N'utilisez pas le coffre-fort ou autre garantie de confidentialité mis à disposition dans votre chambre. Sachez simplement que votre intimité n'est pas protégée ;
- Vérifiez toujours si vous êtes suivi à l'intérieur de l'hôtel. Si vous êtes suivi, changez d'hôtel ou allez dans un autre endroit identifié à l'avance ;
- Essayez de ne pas prendre l'ascenseur seul, restez avec un groupe quand c'est possible.

NB : Soyez prudent, discret et évitez de parler à des inconnus dans l'hôtel. Concentrez-vous sur la mission et assurez-vous que vous êtes en sécurité. Changez de chambre ou même d'hôtel en cas de danger.

Rendez-vous avec vos sources

- En cas de rendez-vous avec l'une de vos sources, assurez-vous bien que vous n'êtes pas surveillé ; pour une source sensible, ne lui donnez pas rendez-vous à l'hôtel ;
- Fixez vous-même l'heure et l'endroit de la rencontre. Par exemple si votre source vous demande à quelle heure et à quel endroit vous voulez la rencontrer, ne jamais répondre « Comme vous voulez ». Proposez-lui un endroit et un horaire que vous avez vous-même déterminés ;
- Établissez une photographie de votre lieu de rencontre : sa clientèle, sa position, accès et sortie... (Par exemple éviter de se rendre dans des endroits où la clientèle peut être ciblée par des agressions et attentats) ;
- Prévoyez un budget (consommations) pour ce type de rendez-vous ;
- Ne consommez pas d'alcool pendant les entretiens, pour des questions de sécurité mais également de concentration ;
- Ne laissez jamais votre boisson seule pour éviter qu'on y verse des produits chimiques (psychotropes, somnifères, Viagra...)
- Essayez de ne pas rencontrer vos sources seul (e), si possible, sa uf si votre source l'exige pour des questions de confiance ;
- Soyez prêt à ce que votre source change brusquement le lieu de la rencontre ; n'acceptez qu'après avoir contrôlé le niveau de risque de ce nouvel endroit ;
- Ne faites jamais des interviews dans des maisons, toujours dans des endroits fréquentés et choisis sur la base d'une étude approfondie des risques (voir chapitre 1)

CHAPITRE 3 : SITUATIONS SUR LE TERRAIN

Après une bonne préparation, voilà le moment de vous lancer dans votre mission médiatique... Vous trouverez ici recensées une série de situations rencontrées sur terrain - manifestations, émeutes, attaques armées, enlèvements - où le journaliste est confronté à des enjeux sécuritaires de divers degrés. Les conseils préconisés ici proviennent de l'expérience de journalistes du monde entier et correspondent au mieux aux situations que l'on peut rencontrer en Tunisie.

A - DURANT LES MANIFESTATIONS, ÉMEUTES ET MOUVEMENTS SOCIAUX

Durant les manifestations, les journalistes sont souvent attaqués ou ciblés pr des attaques. Vous devez vous préparer à toute manifestation, même lorsqu'elle vous paraît facile et routinière. Faites attention : une manifestation pacifique peut se transformer rapidement en affrontement violent ou même en émeute.

Préparez bien votre mission par une bonne planification. (Voir chapitre 1)

Établissez un profil de la manifestation : type, timing et contexte

Types manifestation	Organisateurs	Historiques	Lieu-Timing	Remarques
Politique				
Syndicale				
Sportive				
Sociale				

Dressez un profil de la manifestation :

Une manifestation peut être politique, religieuse, syndicale, sociale ou sportive. Tentez de la cadrer au mieux.

Qui est l'organisateur ? Parti politique (interdit ou non), gouvernement, syndicat (lequel) groupe religieux (interdit ou non), public sportif. Essayez d'entrer en contact avec des personnes que vous connaissez et qui vont participer à la manifestation. Elles peuvent vous faciliter le travail.

Il vous faut donc collecter le maximum d'informations à la fois pour votre sécurité, mais également pour rédiger vos articles et comptes rendus

- Historique (attaques contre journalistes, interventions policières...) des dernières manifestations ainsi que leurs revendications.

- Recensement des interventions précédentes des forces de l'ordre. En cas d'intervention il faut savoir les causes (manifestation non autorisée ou jet de projectiles aux policiers...)

- Les figures qui vont participer (exemple : la présence de certaines personnalités - politiques, religieuses, syndicales) servent d'indice. Par exemple : la présence d'un chef du parti au pouvoir, le Président de la République implique une présence sécuritaire massive. Dans ces cas, a priori pas de risque d'intervention policière. Par contre, une manifestation de l'opposition peut être réprimée et le risque d'attaque contre les journalistes est alors élevé: ce fut le cas lors des manifestations du 9 avril 2012 à Tunis).

- Les revendications de la manifestation sont un indice sur d'éventuelles attaques. Exemples : manifestations contre un projet de loi, manifestations contre une décision d'un chef d'État, etc.

- **Prenez en considération les réactions** de la manifestation (médias, réseaux sociaux.)
- **Faîtes-vous à l'avance une idée** sur le site de la manifestation. Faîtes une évaluation du risque lié au site (chapitre 1).
- **Repérez** à l'avance **l'accès** et le point de sortie de la manifestation.
- **Vos vêtements doivent être adaptés** au lieu et aux conditions de la manifestation (vêtements sombres, imperméable en cas de pluie,)
- **Faîtes-vous une idée sur les armes** et les moyens utilisés par les forces de l'ordre. D'une façon générale, les forces de l'ordre utilisent les bâtons, gaz lacrymogène, le jet d'eau, pour enfin recourir aux munitions, d'abord caoutchouc et parfois, réelles.
- Les manifestations peuvent se prolonger jusqu'à la nuit. Prévoyez des endroits pour être logé en cas de besoin.
- **Visitez préalablement le lieu** de la manifestation, une journée avant de préférence.
- **Prévoyez des cartes Sim** de différents opérateurs au cas où les réseaux de télécommunications connaîtraient des perturbations.
- **Les téléphones et le matériel** (appareil photo, caméra) doivent être chargés.
- **Prévoir un chargeur** externe (« power bank »).

Sur le terrain

- Vous êtes journaliste. Vous ne pouvez pas être également manifestant. Il ne faut **jamais crier les slogans** et les revendications de la manifestation.

- Soyez sur place **au moins une demi-heure avant le début** de la manifestation - Informez-vous sur la présence **des forces de l'ordre.**

- Prenez contact avec les forces de l'ordre et **identifiez-vous auprès d'elles comme journaliste**, avant de commencer à travailler.

- **Cherchez des indices** comme pierres, cocktails Molotov, armes blanches : la présence d'un ou de ces indices laisse supposer une issue violente.

- Identifiez la présence des **manifestants cagoulés** : ils peuvent être derrière des troubles ou des provocations des forces de l'ordre.

- **Travaillez en groupe.** Les manifestations peuvent être particulièrement dangereuses, pour les femmes journalistes. Soyez solidaires entre confrères et consoeurs.

- Prévoyez **un lieu de regroupement** en cas de dispersion de votre groupe. Et même un second lieu de regroupement si le premier n'est pas accessible.

- **Parlez avec les manifestants** et demandez-leur leurs revendications, seulement si la situation est calme. Évitez de parler avec les manifestants lors des accrochages avec les forces de l'ordre.

- Pour les photographes et les cameramen, prévoyez **plusieurs cartes mémoire**. Vous pouvez prendre des photos au début de la manifestation, changez de carte et cachez-la. Vous avez ainsi la garantie de conserver au moins une partie de votre travail, au cas où votre matériel serait cassé ou confisqué.

- Faîtes attention au **logo du média** pour lequel vous travaillez, car il peut causer des problèmes. Dans un contexte général de défiance des journalistes en Tunisie (cf. manifestations anti-journalistes après le second tour de la présidentielle 2019, il est raisonnable de ne pas afficher les logos des médias.)

- Essayez de prendre **une petite pause toutes les 45-60 minutes** pour souffler et faire le point avant de reprendre le travail.

- **N'attirez pas l'attention de la foule**. Par exemple, ne préparez pas votre matériel devant les manifestants.

- Ne jamais **visualiser vos photos** devant la foule.

- Durant le travail, **restez concentré**.

- Suivez l'évolution des slogans ainsi que l'état de la foule. Une foule en effervescence est un indice d'escalade vers la violence. Les changements des slogans, les jets des projectiles (bouteille d'eau) contre les forces de l'ordre sont des **indices précurseurs d'une intervention policière.**

- Ne vous postez jamais **entre les manifestants et les forces de l'ordre**. Choisissez un camp, au sens physique.

- Observez les mouvements des forces de l'ordre. Si les policiers ou militaires commencent à se réorganiser en rangées et s'ils commencent à enfiler leurs casques, attendez-vous **à une intervention policière.**

- **Informez immédiatement votre rédaction** en cas de violence.

Equipements et vêtements

- Les vêtements doivent être adaptés aux endroits, au timing et aux conditions climatiques (pluie, froid, chaleur).
- Évitez les vêtements chics (costume).
- Chaussures confortables et adaptées à la course.
- Prévoyez un casque, un gilet presse ou gilet anti-armes blanche
- Préparez un sac à dos qui contient eau, biscuits secs, barres protéiniques, sucre rapide, jus, citronnade ou vinaigre (voir ci-dessous encadré sur la protection contre bombe lacrymogène), sérum physiologique pour rinçage des yeux touchés par les gaz lacrymogènes, masque à gaz, écharpe, foulard, trousse de premiers secours.

Conseil face aux gaz lacrymogènes

- Prévoyez un masque à gaz. A défaut de masques professionnels, vous pouvez vous procurer les masques utilisés dans l'agriculture et l'industrie. Prenez en compte qu'il est difficile de courir avec.
- Enlevez vos lentilles oculaires en cas de contact avec le gaz.
- Des lunettes de natation pourront protéger les yeux.
- Ne pas vous frotter les yeux.
- Évitez les maquillages et les crèmes (protection solaire).
- En cas de contact, lavez-vous le visage avec de la citronnade ou de l'eau vinaigrée.
- Une écharpe pliée contenant du charbon de bois pourra remplacer le masque à gaz.
- En cas de fuite, courez contre le vent.
- Une fois rentré et en sécurité, laissez les vêtements imprégnés de gaz sécher durant 24 heures avant de les laver.

En cas de violence

- Restez calme
- Si dans l'évaluation préalable de risques existe une possibilité de tirs d'armes à feu, essayez de vous procurer un gilet pare-balles et un casque balistique.
- Tenez-vous prêt à courir
- En cas de dispersion, rejoignez les collègues vers un endroit déterminé à l'avance.
- Les munitions à blanc peuvent être utilisées par les forces de l'ordre pour disperser les manifestants.
- Courez vite pour vous protéger. En cas d'incapacité de courir, rester accroupi.
- En cas d'utilisation d'armes à feu, cherchez immédiatement à vous protéger derrière un abri solide. Sinon couchez-vous au sol.

B - PROTECTION CONTRE LES MENACES BALISTIQUES

Armes de petits calibres

- Au cas où les menaces balistiques figurent dans l'évaluation du risque, exigez un casque et un gilet pare-balles affichant le terme « presse »
- Les médias internationaux en Tunisie disposent de ce matériel.
- Les médias nationaux peuvent en obtenir après une autorisation douanière.
- Les journalistes indépendants peuvent faire appel à des ONG (voir contacts utiles en annexe P. 79) qui procurent ce type de matériel. En cas de déplacement en convoi avec l'armée nationale, vous obtiendrez ce matériel de leur part.
  Ce matériel vous protège des armes à petits calibres.

Si vous êtes pris comme cible :

- Couchez-vous.
- Cherchez un abri statique comme buttes de terres, fossés, murs, arbres ou rochers
- Ne quittez l'abri qu'après le retour au calme.
- Avant de quitter l'endroit, identifiez d'autres abris accessibles. Essayez de courir en zigzag, d'un abri à un autre, le plus vite possible. Les distances entre les abris ne doivent pas dépasser 10 mètres.

- Rampez vite vers un abri, au cas où les tireurs sont à une distance de 300 mètres, au délà de laquelle le danger d'être touché est nettement moindre.

Armes lourdes

- Evitez de pénétrer dans une zone ciblée par l'artillerie ou les frappes aériennes. En Tunisie, c'est uniquement l'armée nationale qui y a recours dans la guerre contre les groupes terroristes installés en montagne (régions du Mont Châambi, Mont Arbata, Salloum...).

Risque d'explosion

- Les bombes sont souvent utilisées par les groupes terroristes, dans des attentats-suicides, par des colis postaux, etc.
- L'expérience (Irak, Afghanistan, Syrie) montre qu'après une première explosion, une seconde est provoquée au même endroit par les terroristes, destinée à faire davantage de dégâts. Pour cette raison, ne vous approchez jamais du lieu de l'explosion.
- Respectez le périmètre de sécurité d'au moins 100 m autour du lieu de l'explosion.
- Soyez coopératif avec les membres des forces de l'ordre. Dans ces circonstances, ils deviennent plus nerveux et agressifs.
- Protégez votre matériel.

Identifier un kamikaze

Vous pouvez identifier un kamikaze à travers plusieurs indices :

- Personne qui marche sans direction précise, à l'allure perturbée ;
- Personne angoissée qui transpire beaucoup et évite les regards d'autrui et parfois jette son regard sur les passants ;
- Personne habillée d'une manière large, pouvant cacher des explosifs ou armes ;
- Informer la police en cas de soupçon ; ne jamais s'approcher de la personne suspecte : si le kamikaze se sent découvert, il se fera exploser le plus vite possible.
- Suspecte : si le kamikaze se sent découvert, il se fera exploser le plus vite possible.

Colis piégés ou empoisonnés

C'est une technique utilisée par les groupes terroristes. Le ministère de l'Intérieur a déjoué en mars 2019 une série d'attentats terroristes par colis postaux, ciblant 19 personnalités y compris des journalistes sur la base de leurs opinions.
Vous pouvez découvrir un colis piégé à travers plusieurs indices comme :

- Poids lourd et rigidité excessive ;
- Emballage bizarre (trop d'emballage, trop de couleurs, absence d'adresse...)
- Colis présentant un message de type personnel, votre nom qui n'est pas correctement écrit, emballage taché (faisant suspecter la présence de substances chimiques mortelle par un simple contact, l'anthrax en l'occurrence).
- Si vous n'êtes pas habitué à recevoir des colis, faîtes attention. Vérifiez le nom, l'adresse et les détails sur l'expéditeur avant tout. Rappelez l'expéditeur et vérifiez si c'est bien lui qui vous a envoyé le colis. Sinon appelez la police ; n'essayez jamais d'ouvrir le paquet.
- Si l'expéditeur est inconnu, prenez le temps pour vérifier son identité. Vous êtes journalistes et vous êtes joignable par plusieurs moyens (téléphone, mail, réseaux sociaux). Pour quelle raison vous envoie-t-on un colis ? Même si pensez que ce sont peut-être des documents très confidentiels envoyés par quelqu'un qui ne veut pas dévoiler son identité.
- N'utilisez pas votre téléphone ;
- Évacuez les lieux et faîtes établir un périmètre de sécurité d'au moins 100 mètres ;
- Informez la police.

Embuscade

- Si vous êtes en déplacement et que, dans votre évaluation des risques figurent ceux d'une embuscade, préparez-vous à l'éventualité et surtout parlez avec les gens qui vous accompagnent pour intégrer un maximum d'informations
- En déplacement dans un convoi militaire ou sécuritaire, vous pouvez être cible d'une embuscade.
- Si vous êtes embarqué avec l'armée ou autres forces officielles, parlez avec eux avant de commencer la mission et demander leurs conseils en cas d'embuscade. Ils vous diront comment agir en cas de danger.
- Si vous êtes dans votre propre véhicule en convoi, gardez une distance de sécurité de 50 m entre les véhicules. En cas de danger, sortir rapidement de la zone. Il faut prévoir cela dans votre planification. Au cas où la route serait bloquée, quittez le véhicule du côté opposé aux tirs et mettez-vous à l'abri.
- Dans les villes, essayez de vous rapprocher au maximum des autres véhicules et soyez vigilants en cas d'arrêt du convoi.

NB : Si vous êtes en reportage dans un véhicule avec des contrebandiers, ou groupes armés, prenez en considération que vous pouvez être pris comme cible si le véhicule ne s'arrête pas à un poste de contrôle. Essayez par conséquent de vous déplacer dans un véhicule séparé.

C - ARRESTATIONS ET KIDNAPPINGS

De plus en plus les journalistes deviennent des cibles pour les groupes terroristes. Il faut donc se protéger du risque de kidnapping, utilisé pour des raisons financières, impliquant une demande de rançon, ou encore motivés par leurs opinions et écrits.

Vous pouvez également être séquestré arbitrairement par les forces de police ou de sécurité pour la simple raison que vous avez filmé une manifestation, un accident ou une catastrophe naturelle.
Dans tous ces cas, vous devez savoir comment vous comporter.

En cas d'arrestation

- Restez calme ;
- Prévenez immédiatement votre rédaction, le centre de sécurité du SNJT ;
- Demandez avec calme à vos agresseurs les raisons de l'arrestation ;
- Préparez les autorisations, l'ordre de mission, vos papiers d'identité (carte de presse ou de membre du SNJT) ;
- Demandez la présence d'un avocat (contacter le SNJT) et ne répondre aux questions qu'en sa présence, en vertu de la dernière réforme du Code de procédure pénale (article 13 bis al. 5, voir chapitre 1).
- Demandez un examen médical en cas de violence policière.
- En cas de confiscation de votre téléphone ou de votre ordinateur par la police, ne révélez jamais les mots de passe sans autorisation d'un juge.

En cas de kidnapping

Toute personne peut être cible d'un kidnapping.
Si dans votre appréciation de la mission il existe un risque de kidnapping, il est conseillé de reporter ou d'annuler la mission.
Si vous décidez de maintenir la mission, il faut suivre les conseils ci-dessous pour éviter d'être victime de kidnapping et y parer.

Dans votre planification (chapitre 2), posez-vous ces questions :

- Y a-t-il eu des cas de kidnappings dans la zone où vous allez travailler ?
- Si oui, quelles ont été les cibles ? (police, armée, institutions de l'Etat , bergers.)
- Si non, est-ce qu'il y a un risque de kidnapping ?
- Quelles sont les parties qui peuvent procéder à une prise d'otage ? (Groupe terroristes, contrebandiers, manifestants pour attirer l'attention nationale et internationale en séquestrant des journalistes, des touristes, des officiels...)

Prévention avant la prise d'otages

- Changez régulièrement vos trajets : modifiez le temps de sortie et de retour à votre lieu d'habitation et de votre lieu de travail.
- Changez vos habitudes. Si vous êtes habitués à prendre un café-verre dans un endroit, changez souvent de fournisseur ;

- Soyez discret et surtout évitez d'être exposé au public (éviter les espaces isolés) si vous êtes en déplacement;
- Déplacez-vous de préférence en groupe. Le groupe minimise le risque d'être pris en otage ;
- Sur le terrain, évitez d'être seul, et ne dépassez pas 40 minutes de travail sur terrain ;
- Soyez prudent et méfiant. Ne faites pas confiance à des personnes que vous venez de connaître ;
- Evaluez la menace : pour connaître ses moyens et connaître par la suite les moyens pour assurer votre sécurité. Un groupe terroriste diffère d'un gang en termes de moyens et de techniques ;
- Si vous êtes ciblé par un groupe terroriste ou autre, appelez immédiatement les autorités officielles puis le SNJT (unité de monitoring), mais avant tout mettez-vous en sécurité.

En cas de prise d'otages ou de privation de liberté :

On connaît 4 étapes dans tout acte de kidnapping :

a- La capture
b- La privation de liberté, l'arrestation
c- La libération
d- L'après-kidnapping

a- La capture de la cible

Si vous êtes rendu à cette phase, c'est-à-dire que vous étiez pisté et que vous n'avez pas remarqué l'existence de vos agresseurs, c'est que vous avez échoué dans votre appréciation du risque. Donc et avant tout, planifiez votre mission, préparez-vous bien et suivez les consignes préalables, pour ne pas vous retrouver dans cette situation.
Mais si malgré tout vous êtes victime d'un enlèvement...

Lors de la capture :

- Préparez-vous mentalement à être menacé par des armes, attaqués ou violé(e)s ;
- Soyez ou tentez de paraître calme ;
- Les agresseurs sont eux aussi agités et pressés. Evitez la panique et ne résistez pas. Votre réaction peut les agiter davantage et la situation empirer ;
- N'essayez de fuir que si vous êtes absolument sûr de réussir.

b- La privation de liberté (ou séquestration)

- Soyez prêt à ce que votre séquestration soit longue ;
- Essayez de mémoriser les détails : noms des agresseurs, langues, voix. Les bruits de train, de véhicules, donnent des indices de localisation ;

- Préservez au maximum votre santé. Acceptez la nourriture, l'eau ;
- Pratiquez une activité physique : pompes, flexions, assouplissements ;
- Soyez coopératif avec vos surveillants ;
- Essayez de dialoguer avec eux ;
- Essayez de demander avec politesse des journaux, stylos, papiers, radio, musique ;
- Habituez-vous aux menaces et aux promesses des ravisseurs, mais n'y croyez jamais ;
- Créez votre routine quotidienne ; par exemple sport le matin, écriture le reste de la journée, lecture le soir ;
- Vous êtes journaliste. Imaginez comment raconter votre histoire plus tard ;
- Restez optimiste, cela vous aidera à rester en bonne santé ; si votre santé se détériore, votre valeur marchande baisse pour vos agresseurs. Ils pourraient penser à se débarrasser de vous...
- Attendez-vous à ce qu'on vous demande de faire un enregistrement vidéo ou audio ou écrire un message au public. Acceptez. Si on vous donne un texte (déjà préparé par votre kidnappeur) lisez le tel qu'il est ; ne contestez pas.

c- La libération

- Durant une opération de libération assurée par des forces armées, il y aura certainement des tirs. Ne tentez jamais de participer ou d'intervenir. Protégez-vous, couchez-vous au sol ;
- Après la fin de l'opération et le retour au calme, divulguez votre identité aux forces de sécurité ;
- En cas de libération (après paiement de rançon), restez calme et ne manifestez aucune réaction ou joie face à vos ravisseurs.

d- Après la libération

- Consultez vos médecins pour examen médical ;
- Préparez-vous à des interrogatoires indispensables par les forces de sécurité et de renseignements ;
- Attendez-vous à devoir faire des déclarations à la presse. Soyez attentif à vos propos et suivez avec mesure les conseils des forces de sécurité, des autorités publiques avant toute déclaration ; vous n'y êtes pas contraint ;
- Après une telle expérience, vous courez un risque de troubles post-traumatiques. Consultez les spécialistes, psychologues. Là encore le SNJT pourra vous fournir les ressources nécessaires.

CHAPITRE 4 : LA CYBERSÉCURITÉ

Ce chapitre vise à sensibiliser le journaliste aux enjeux de sa sécurité numérique et à lui donner un panorama des techniques et outils à sa disposition pour bien se protéger. Il est cependant impossible d'y détailler toutes les mesures et d'en donner des tutoriels. Ainsi le lecteur est-il invité à effectuer les recherches nécessaires

Les pages qui suivent donnent dans un premier temps les techniques et réflexes que tout un chacun, journaliste ou pas, doit mettre en pratique pour ne pas subir les attaques « standards » dans le monde numérique.
Dans un second temps sont exposées les techniques davantage adaptées aux journalistes, en particulier travaillant dans les zones ou sur des sujets sensibles, comme cela peut être le cas en Tunisie.

A - RÈGLES DE « CYBER-HYGIÈNE » POUR TOUS

À l'image de la bonne hygiène qui nous aide à nous protéger des maladies, ou bien du respect du code de la route qui nous aide à nous protéger des accidents de la circulation, il est nécessaire d'adopter des bonnes pratiques de sécurité numérique pour se protéger des actes malveillants toujours plus nombreux dans le cyber-espace.

L'usager ne peut se contenter d'une utilisation non sécurisée des outils numériques, en profiter tout en espérant ne pas être la prochaine victime d'un vol d'identité, siphonnage de compte bancaire, sabotage, acte d'espionnage...

Avant d'aller plus loin dans les techniques de protection spécifiques à des métiers et situations, il est d'abord nécessaire d'être sensibilisé aux bons réflexes de sécurité numérique à l'ère du tout connecté et de les adopter pour un usage responsable du cyber-espace.

Notez dans un premier temps une règle de base à observer : le matériel connecté personnel doit rester personnel. Un smartphone par exemple, contient de très nombreuses données à caractère privé. C'est également un véritable ordinateur doté d'une multitude de capteurs qu'il est possible de transformer en mouchard. Vous ne devez donc jamais le prêter ou le laisser sans surveillance lorsqu'une tierce personne risque d'y accéder (il suffit d'un court instant pour le compromettre).

Protégez vos comptes en ligne

L'extension de vos vies dans le cyber-espace prend souvent la forme de comptes en ligne tel que comptes e-mail (Gmail, Yahoo par exemple), comptes de réseaux sociaux (Facebook par exemple) ou bien compte de commerce électronique (Amazon, Jumia...). Ces comptes en disent long sur vous et doivent impérativement être correctement protégés.

Mots de passe

Pour ce faire, vous devez les verrouiller par des mots de passe forts : il s'agit de mots de passe longs et complexes. Longs parce qu'ils dépassent 10/12 caractères et complexes car ils contiennent des majuscules, des minuscules, des chiffres et des caractères spéciaux (#/&...).

Exemple : Ps1js10mY@T!

Ce mot de passe respecte les conditions de longueur et de complexité évoquées et semble dénué de sens. Cependant il reste relativement facile à mémoriser car en réalité il dérive de la phrase ci-dessous :

« Prudent sur internet je suis dit maître Yoda à Tatooine! »

Les premières lettres de chaque mot ont été juxtaposées. Certaines ont été remplacées par des chiffres ou caractères spéciaux (i -→ 1 ; dit -→ 10 ; à -→ @).

Gestionnaires de mots de passe

Il est impératif d'avoir un mot de passe différent pour chaque compte. Ainsi si l'un vient à être compromis, les autres restent protégés.
Évidemment, cela pose le problème de la mémorisation de nombreux mots de passe complexes.
Le gestionnaire de mots de passe est une solution à cela : il s'agit d'une application qui permet de sauvegarder vos mots de passe de façon sécurisée. Le gestionnaire est lui-même verrouillable par un mot de passe maître, qui devient le seul à mémoriser.
Il en existe plusieurs, gratuits et payants, qui peuvent s'installer sur votre ordinateur, smartphone, tablette... Ex : Dashlane, LastPass, 1Password, Keepass...

Il est déconseillé de permettre aux navigateurs d'enregistrer les mots de passe, surtout s'il s'agit d'un ordinateur partagé ou public (qu'il faut en général éviter pour consulter vos comptes en ligne).

Authentification à deux facteurs

Afin d'ajouter un niveau de sécurité important à la protection de vos comptes, il vous faut activer l'authentification à deux facteurs (vérification en deux étapes) lorsque cette option est disponible. Après l'activation de l'authentification à deux facteurs, vous devez désormais renseigner un code à usage unique valable pour un court laps de temps en plus de l'identifiant et du mot de passe. Ces derniers seront donc insuffisants pour accéder au compte en ligne protégé par l'authentification à deux facteurs.
Ce code jetable supplémentaire est généralement communiqué par SMS, mail ou généré dans une application dédiée (Authenticator par exemple).
L'activation de l'authentification à deux facteurs se fait en principe dans les paramètres de sécurité du compte. Des instructions guident l'utilisateur pour, le cas échéant, installer l'application qui génère les codes et la coupler avec son compte en ligne.
L'authentification à deux facteurs est une mesure de protection des comptes en ligne importante. Elle complique drastiquement la tâche des pirates.

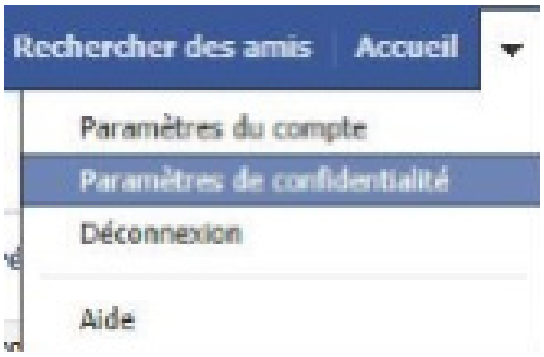
Se protéger de l'ingénierie sociale (« social engineering »)

L'ingénierie sociale est l'exploitation des informations disponibles sur une personne afin d'en dresser le profil le plus précis possible.
En effet, avec la multiplication des services en ligne et de leurs usages, il est possible de trouver un grand nombre d'informations sur les individus, tels leur apparence physique (photos de profil de réseaux sociaux), leurs parcours éducatif et professionnel (Linkedin, publications universitaires...). Il est même possible d'obtenir de nombreuses informations sur leur famille, leurs lieux de vacances, leurs opinions politiques...

L'ingénierie sociale est également un levier très utile pour la réussite des actes malveillants. Par exemple, un cambrioleur peut savoir que le logement visé est vide grâce aux photos de vacances de la victime postées sur les réseaux sociaux. Il est donc primordial de se protéger d'ingénierie sociale.

Pour cela, vous devez vous assurer que les paramètres de confidentialité de vos réseaux sociaux sont correctement réglés pour limiter l'audience des posts (qui peut voir les photos postées par l'intéressé ou par ses amis par exemple). Vous devez explorer ces réglages afin de les rendre restrictifs.

Vous devez aussi éviter d'accepter les demandes d'amitiés/ connexions de profils qui ne sont pas reconnus ou qui vous paraissent suspects.



En règle générale, gardez à l'esprit la menace d'ingénierie sociale et faîtes l'économie des publications qui peuvent dévoiler des informations privées sur votre famille et surtout votre travail... Cela est d'autant plus vital lors de vos missions en zone sensible.

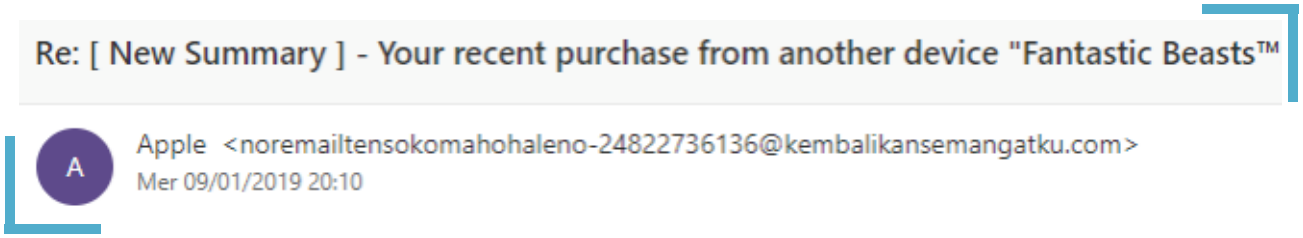
Soyez vigilant face au phishing

Le phishing est constitué de techniques qu'utilise un pirate informatique pour amener sa victime à divulguer une ou des informations (identifiant/mot de passe à un compte en ligne par exemple) ou à lui faire télécharger un virus informatique.

C'est un piège qui s'appuie sur la psychologie humaine : curiosité, appât du gain, peur... et il exploite tout type de messageries (Whatsapp, e-mail, SMS, Messenger...).

Le phishing est une menace globale et permanente que vous devez toujours avoir à l'esprit. Ainsi, vous devez systématiquement réfléchir avant de cliquer sur un lien ou télécharger un fichier. Interrogez-vous sur la forme et le fond du message reçu :

Au niveau de la forme, on s'intéresse au vecteur (pourquoi ce message vous parvient-il sur WhatsApp ?), au ton (pourquoi cette administration semble vous menacer ?), au style (pourquoi votre banque vous écrit-elle avec des fautes de langue ?). Toujours sur la forme, il est utile d'examiner l'adresse de l'expéditeur et celle du ou des liens éventuellement contenus dans le message afin de vous assurer qu'ils se rapportent bien aux acteurs annoncés. Attention aux adresses d'expéditeur ou url qui se rapprochent par ruse à ceux prétendus. Par exemple www.tunısair.com n'est pas l'adresse réelle de Tunis Air car le « ı » de Tunis a été remplacé par un caractère turcique qui lui ressemble.



Au niveau du fond, intéressez-vous à la plausibilité du message, à sa cohérence. Méfiez-vous notamment :

- Lorsque c'est trop beau pour être vrai (une entreprise qui distribue des cadeaux par exemple) ;
- Face à une demande d'informations confidentielles (identifiants, mots de passe...) ;
- Face à une annonce de décision impactante pour l'usager, suivie d'injonctions à agir sans délai (votre compte va être désactivé demain) ;
- Face à un message menaçant émanant de forces de l'ordre ou autres institutions et demandant des paiements immédiats ;
- Face aux histoires dont la trame commune est que le destinataire avance une petite somme d'argent pour en débloquer une plus grosse qui sera partagée avec lui.

Harponnage (spear-phishing)

Avec les bons réflexes face aux messages reçus, les tentatives de harponnage/phishing envoyées en masse aux internautes peuvent être mises en échec.

Cependant, il faut redoubler de vigilance pour se prémunir du spear-phishing, un phishing spécifiquement adressé à la victime, s'appuyant sur l'ingénierie sociale (page 57) pour mieux la piéger. En effet, un message de harponnage s'appuie sur un scénario crédible pour la victime, personnalisé car contenant des éléments qui lui sont familiers. Il devient plus difficile de s'en méfier. À la moindre suspicion, il ne faut pas hésiter à faire les vérifications nécessaires (par exemple appeler par téléphonel'expéditeur pour s'assurer qu'il est bien à l'origine du message...) et s'abstenir de donner suite, en particulier, à des demandes de partage d'informations sensibles ou à des demandes d'argent.

Méfiez-vous des connexions publiques

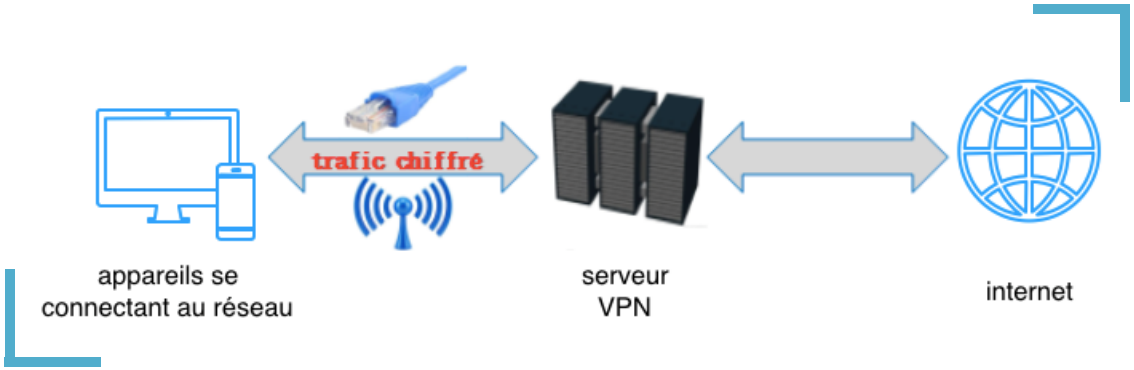
Connecter un appareil à un réseau wifi ou un réseau câblé signifie que l'ensemble du trafic Internet de cet appareil passe par les équipements de ce réseau. Les administrateurs de ce dernier ou bien toute personne y ayant un accès administrateur (autorisé ou non) peut visualiser ce trafic.

Si les connexions Internet effectuées ne sont pas chiffrées, l'ensemble des informations échangées seront visibles à celles et ceux qui contrôlent le réseau. Si les connexions utilisent un protocole sécurisé (https pour le web par exemple) seuls les métadonnées (date, heure, appareil émetteur, destination) seront visibles.

Afin de rendre le trafic complètement privé, il convient de le faire passer via un VPN (Virtual Private Network). Pour un tel usage, il s'agit d'un service permettant au trafic Internet sortant d'un appareil de se diriger dans un premier temps et de façon chiffrée vers un serveur distant avant d'être re-routé vers les serveurs de destination souhaités. De cette manière, l'ensemble du trafic passant par le réseau sur lequel est connecté l'appareil, se fait avec un serveur de façon chiffrée. C'est la seule information visible à la personne qui contrôle le réseau en question.

Concrètement, se doter d'un VPN est aussi simple qu'installer une application VPN sur son appareil (smartphone, tablette, ordinateur). Il en existe une multitude (ProtonVPN, NordVPN...), gratuits et payants et de nombreux articles sur internet les comparent.

Note : un pirate peut créer à l'aide de son ordinateur un point d'accès wifi dans un lieu donné afin de piéger les personnes qui y recherchent une connexion Internet. Il peut le nommer « WIFI_GRATUIT » ou bien du nom du lieu où il se trouve (café, aéroport...) et réalise ainsi l'attaque « man-in-the-middle » (le trafic de la victime transite par l'ordinateur du pirate).



B - MESURES DE PROTECTION EN ZONE SENSIBLE

En complément des bonnes pratiques de cyber-sécurité à l'usage de tous, en tant que journaliste travaillant sur des dossiers ou zones sensibles, vous devezpouvoir aller plus loin pour assurer votre sécurité numérique.

Avant de passer en revue les techniques et outils disponibles pour avancer dans la cybersécurité, rappelons d'abord une première règle de base : il faut se protéger des regards indiscrets (sur les écrans qu'il faut idéalement couvrir d'un filtre de confidentialité, film qui limite la vision de l'écran au seul utilisateur) et oreilles indiscrètes. La sécurité numérique est d'autant mieux pratiquée que le bon sens, l'esprit critique et l'esprit sécuritaire sont en permanence mobilisés. Dans le domaine de la sécurité, la paranoïa est une qualité.

Matériel/comptes de mission

De la même manière qu'une mission en zone sensible se prépare d'un point de vue éditorial et sécurité physique (voir chapitres précédents), elle se prépare également d'un point de vue numérique. Quel matériel, quelles précautions et dispositions à prendre une fois sur place ?

Matériel

Tout d'abord, ne partez qu'avec le nécessaire en termes de données. Il vous faut donc prévoir un matériel spécifique à votre mission (ordinateur, tablette, smartphone). En effet, le risque de surveillance et de cyber-attaque étant élevé lors de ces missions, votre matériel habituel risque d'exposer l'ensemble de votre travail et votre vie privée de journaliste en cas de perte ou de compromission.
Le matériel de mission est un matériel effacé (attention, les fichiers mis à la corbeille ne disparaissent pas du disque dur, même si la corbeille est vidée) qui n'est chargé que des données nécessaires. Ses paramètres sont revus pour être adaptés aux exigences de sécurité : mots de passe fort, pare-feu activé et restrictif, antivirus installé et à jour, navigateurs paramétrés pour ne pas retenir les mots de passe et ne pas conserver d'historique de navigation.

Vos logiciels et votre système d'exploitation doivent être à jour (il est déconseillé d'installer des mises à jour ou d'accepter de nouveaux réglages en mission car cela peut être un vecteur d'infection). Votre prévisualisation des messages sur écran verrouillé doit être désactivée.

Il ne vous faut en outre jamais accepter de matériel connecté en cadeau (téléphone, clés USB...) et ne jamais brancher de périphériques de stockage externes (clefs USB, disques durs...) inconnus. De même qu'il ne faut jamais prêter vos chargeurs ou les laisser sans surveillance (idéalement, il convient de les marquer).

Chiffrement de vos disques

Puisque le contenu de votre ordinateur, même protégé par un mot de passe, peut être lu directement depuis son disque dur, il faut procéder au chiffrement de votre disque.
FileVault est l'outil de MacOS permettant de chiffrer le disque. BitLocker est celui de Windows. Il existe des applications tierces de chiffrage de disque telles que TrueCrypt ou VeraCrypt (existent pour MacOS, Windows et Linux).
Attention, notez bien le mot de passe et, le cas échéant, les codes de récupération, car sans possibilité de les déchiffrer, vos données seront irrémédiablement perdues.

Plus généralement, il est utile de savoir chiffrer des fichiers ou des disques externes comme des clés USB. Les données stockées dans un volume chiffré à l'aide d'un standard moderne sont extrêmement bien protégées.

Effacement smartphones/tablettes

En cas de perte du smartphone ou de la tablette, il est nécessaire de pouvoir effacer les données contenues dans l'appareil perdu.
Les appareils sont gérés pas un compte Google si leur système d'exploitation est Android ou bien par un compte iCloud si leur système d'exploitation est iOS.
Qu'ils soient sous iOS ou Android, il vous est possible en vous connectant au compte Google ou iCloud associé à l'appareil, de le localiser (si la fonction a été préalablement autorisée dans les réglages de l'appareil) ou bien d'effacer son contenu.

Il est indispensable de découvrir et maîtriser ces procédures afin de pouvoir réagir rapidement en cas de perte ou vol de l'appareil.

En outre, iOS permet de régler l'appareil pour qu'il s'efface suite à 10 tentatives de déverrouillage à l'aide d'un code erroné. Il vous est donc nécessaire, pour être paré à assurer des missions sensibles, de passer un certain temps dans les menus de vos appareils, ou de consulter les tutoriels correspondant sur Internet.

Connectivité des appareils

Les appareils connectés, qu'ils soient ordinateurs, smartphones, tablettes ou autres objets telles que les smartwach, cherchent en permanence à établir des communications sans fil. Il s'agit principalement de communications radio wifi ou Bluetooth. Ce faisant, ces appareils se dévoilent et dévoilent d'autres informations telles que le « nom de l'appareil », les points d'accès auxquels ils sontconnectés...

Par conséquent, il est important de n'activer la connectivité qu'en cas de besoin. Vous devez systématiquement avoir le réflexe de sortir avec des appareils dans leur mode le plus discret (pas de wifi allumé, Bluetooth, partage de connexion, Airdrop... dans les cas extrêmes « mode avion » complètement activé pour éviter le pistage via la connectivité GSM).

Remarque : sur iOS, il faut privilégier la désactivation du wifi et Bluetooth depuis le menu « Réglages » et non depuis les raccourcis d'écran verrouillé. En effet, sur ce dernier, wifi et Bluetooth ne sont pas totalement coupés.

Aussi, il est utile de changer dans les réglages de l'appareil son « nom » afin qu'il ne dévoile pas l'identité de son propriétaire (souvent l'appareil s'attribue automatiquement le nom de son propriétaire, « iPhone-de-Malika » par exemple). Codez votre identité.

Comptes de mission

Les comptes habituels de e-mail, réseaux sociaux, WhatsApp... contiennent un grand nombre d'informations sur votre travail de journaliste et votre vie privée. Il convient donc de créer des comptes spécifiques à la mission en zone sensible afin de laisser à l'abri ces données.
Les comptes spécifiques devront être communiqués aux collaborateurs et partenaires de missions, en premier lieu vos éditeurs rédacteurs en chef à la rédaction.. Des réponses automatiques d'injoignabilité pourront être programmées sur les comptes habituels.

Une fois la mission terminée, vous transmettez ou faîtes transmettre les informations sur vos comptes habituels et vos comptes provisoires sont abandonnés. Vous en recréerez ou ferez recréer de nouveaux à chacune de vos missions sensibles.

Sécurité des communications

Il existe une multitude de services de messageries utilisant des standards et technologies variées. Le niveau de sécurité et de confidentialité qu'ils offrent est tout aussi varié. En mission en zone sensible, vous devez atteindre un niveau élevé de sécurité des communications en choisissant les services les plus adaptés.

E-mail

Les e-mails professionnels de vos rédactions sont rarement chiffrés. Il en va de même pour des services e-mail connus comme Gmail ou Yahoo !. Il existe des services mail chiffrés gratuits ou encore payants comme ProtonMail, FastMail, StartMail...

L'usage d'une application d'e-mail chiffré ne diffère pas des services classiques. L'installation, édition, envoi et fonctionnalités sont similaires et à la portée de tous.

Il faut s'assurer que le destinataire possède un compte dans le même service afin de garantir une communication chiffrée de bout en bout. Certains services comme ProtonMail proposent d'envoyer un mail chiffré qui, à réception, s'ouvre dans une page web sécurisée par mot de passe.

En plus de créer un compte mail de mission, à n'utiliser pour envoyer et recevoir que pendant la durée de celle-ci, il est possible, si le niveau d'exigence de confidentialité le requiert, de créer des boîtes email pour des communications spécifiques et ponctuelles, de l'ordre de quelques heures ou même d'un seul échange.

Messagerie

De la même manière, il existe des applications de messageries chiffrées et développées dans un esprit de sécurité. C'est le cas par exemple des applications Signal ou Telegram, gratuites et disponibles dans l'Appstore d'iOS et Playstore d'Android. Leur installation et usage sont intuitifs et ne diffèrent généralement pas des autres applications de messagerie.

Navigation web

Tor browser est un navigateur sécurisé (basé sur Mozilla Firefox). Il utilise le réseau Tor et la technologie dite de l'oignon pour anonymiser l'origine de la requête en établissemant des connexions chiffrées avec une série de relais en amont du serveur de destination souhaité.

En général, il est recommandé d'utiliser un VPN pour se connecter à Internet (depuis ordinateurs ou mobiles) et d'éviter les connexions depuis des ordinateurs publics ou partagés ou en se connectant à des wifi publics.

Aussi, pensez à configurer les navigateurs de façon restrictive (pas de conservation d'historique...). Note : sur mobile, Firefox Focus possède un bouton (icône en forme de poubelle au niveau de la barre d'adresse) pratique pour supprimer immédiatement les données de navigation (historique, cookies).

Téléphone

Le smartphone est un ordinateur embarquant de nombreux capteurs. Il présente de ce fait des risques de sécurité importants. Votre smartphone de mission doit être correctement configuré pour la sécurité ; n'emportez que le nécessaire en termes de données et d'applications. Parmi ces dernières, les applications de communication sécurisées mentionnées plus haut.

La communication via réseau GSM (appels téléphoniques, SMS) peut faire l'objet de surveillance. De plus les connexions des téléphones aux antennes relais révèlent leurs positions géographiques. Adoptez donc des règles de sécurité sur la partie GSM également. Notamment prévoyez des cartes SIM sans identité à usages ponctuels, n'activez le GSM que pour passer l'appel (de préférence d'une position géographique différente des positions habituelles). Lorsqu'il s'agit de téléphone GSM classiques, préférez le stockage de données (comme les contacts) sur la carte SIM, car plus facilement destructible plutôt que dans la mémoire du téléphone lui-même.

Note : N'hésitez pas à compléter les moyens techniques par des astuces de brouillage humain comme convenir avec vos collaborateurs de codes linguistiques pour échanger des informations. De la même manière, les mails et messages peuvent être déguisés pour avoir une allure anodine (adresse, nom et objet peuvent mimer un message de démarchage marketing par exemple). Faîtes preuve d'imagination et de complicité entre journalistes.

Adaptation des mesures à l'environnement

Dans certains environnements, les mesures de cybersécurité doivent pouvoir rester discrètes. En effet, ces mesures peuvent attirer l'attention sur le journaliste qui les pratique et dans certains cas se heurter à des législations qui les prohibent. Dans ces environnements, optez pour une approche segmentée avec d'une part un comportement numérique « normal », par lequel transitent vos données non sensibles et d'autre part des îlots de confidentialité sécurisés où transitent au besoin vos données sensibles.

Afin de masquer les productions sensibles, il peut être utile, dans certaines situations, d'avoir des leurres, des données de travail journalistiques peu sensibles qui pourront être trouvées en cas d'inspection. Les données sensibles pourront, elles, être stockées sur des supports chiffrés et cachés. Par exemple, le logiciel de chiffrement Veracrypt vous offre la possibilité de créer un volume caché au sein d'un volume chiffré. Ainsi dans le cas où le propriétaire est forcé de déchiffrer son volume chiffré visible, il n'y aura, en théorie, aucun moyen de prouver l'existence d'un autre volume chiffré à l'intérieur de celui-ci. Dans la même veine, Tails est un système d'exploitation conçu pour la sécurité qui tient sur une clé USB ou un DVD. Vous pouvez le démarrer sur n'importe quel ordinateur et il ne laissera aucune trace sur ce dernier. Il force toutes les connexions entrantes et sortantes à passer par le réseau Tor et contient de nombreuses autres fonctionnalités de sécurité.

Le brouillage humain évoqué dans les pages précédentes est propice dans les contextes hostiles aux moyens techniques de sécurité. Il peut devenir le seul recours lorsque le contrôle des équipements est intrusif et très poussé.

ANNEXE 1

Décret-loi 115 (extraits)

Article 7

Est considéré journaliste professionnel conformément aux dispositions du présent décret-loi, toute personne détenant au moins une licence ou un diplôme scientifique équivalent, dont l'activité consiste en la collecte et la publication des informations, des opinions, des idées et leur transmission principalement au public de façon régulière, au sein d'un ou de plusieurs établissements d'information audiovisuelle ou d'information électronique et à condition d'en tirer ses principales ressources.
Est aussi considéré journaliste professionnel, le correspondant en Tunisie ou à l'étranger, à condition qu'il remplisse les conditions mentionnées au précédent paragraphe. Sont assimilés aux journalistes professionnels mentionnés au paragraphe 1er ci-dessus : leurs assistants directs, comme les rédacteurs, les traducteurs, les documentalistes, les dessinateurs, les photographes, les cameramans, à l'exception des agents publicitaires et de tous ceux qui ne présentent qu'une aide occasionnelle, quelle que soit sa forme

Article 11

Sont protégées les sources du journaliste dans l'exercice de ses fonctions, ainsi que les sources de toute personne qui contribue à la confection de la matière journalistique. Il ne peut être procéder à la violation du secret de ces sources directement ou indirectement que pour un motif impérieux de sûreté de l'Etat ou de défense nationale et sous le contrôle de l'autorité juridictionnelle. Est considérée comme violation du secret des sources, toutes enquêtes, tous actes de recherche et d'investigation, toutes écoutes de correspondances ou de communications, effectuées par l'autorité publique à l'encontre du journaliste pour découvrir ses sources ou à l'encontre de toute personne entretenant avec lui des relations particulières.

Le journaliste ne peut faire l'objet d'aucune pression, de n'importe quelle autorité et il ne peut être également exiger d'un quelconque journaliste ou d'une quelconque personne participant à la confection de la matière journalistique de révéler ses sources d'information , sauf autorisation du juge judiciaire compétent et sous réserve que ces informations soient relatives à des infractions présentant
un risque grave pour l'intégrité physique d'autrui, que leur divulgation soit nécessaire pour prévenir la commission de telles infractions et qu'elles soient du type d'informations ne pouvant être obtenues par tout autre moyen.

Article 12

L'opinion exprimée par le journaliste ou les informations qu'il publie, ne peuvent justifier l'atteinte à sa dignité ou la violation de son intégrité corporelle ou morale.

Article 13

Un journaliste ne peut être poursuivi pour avoir publié une opinion, des idées ou des informations conformément aux us et à la déontologie de la profession et ne peut être poursuivi pour son travail à moins que sa violation des dispositions du présent décret-loi soit prouvée.

Article 14

Quiconque enfreint les articles 11, 12 et 13 du présent décret-loi et quiconque humilie un journaliste ou lui porte atteinte verbalement, par des gestes, par des agissements ou par des menaces entravant l'exercice de son travail, est passible de la peine encourue pour outrage à un fonctionnaire public assimilé, mentionnée à l'article 123* du Code pénal.

ANNEXE 2

Convention collective cadre pour les journalistes tunisiens du Syndicat National des Journalistes Tunisiens : santé et sécurité professionnelle

Article 24

Les entreprises adoptent toutes les mesures nécessaires et appropriées pour la protection de la santé des journalistes et la prévention contre les risques professionnels. Elles s'engagent aussi à leur garantir la protection nécessaire contre les agressions auxquelles ils risquent d'être exposés pendant leur travail et qui peuvent les atteindre dans leur dignité, leur intégrité physique ou leurs biens. Les entreprises médiatiques leur apportent aussi l'appui nécessaire pour mener les procédures indispensables pour les défendre lorsqu'ils font face à de telles agressions ou lorsqu'ils font l'objet de poursuites judiciaires en raison de l'exercice de leur métier.

ANNEXE 3

Loi organique n° 2015-26 du 7 août 2015, relative à la lutte contre le terrorisme et la répression du blanchiment d'argent

Article 37

"Sont également exceptés, les journalistes conformément aux dispositions du décret-loi n° 2011- 115 du 2 novembre 2011, relatif à la liberté de la presse, de l'imprimerie et de l'édition. Ces exceptions ne s'étendent pas aux informations dont ils ont pris connaissance et dont le signalement aux autorités aurait permis d'éviter la commission d'infractions terroristes dans le futur"

ANNEXE 4

(Des exceptions au droit d'accès à l'information)
Loi organique n° 2016-22 du 24 mars 2016, relative au droit d'accès à l'information

Article 24

L'organisme concerné ne peut refuser l'accès à l'information que lorsque ceci entraînerait un préjudice à la sécurité ou la défense nationale ou les relations internationales y liées ou les droits du tiers quant à la protection de sa vie privée, ses données personnelles et sa propriété intellectuelle.
Ces domaines ne sont pas considérés comme des exceptions absolues au droit d'accès à l'information. Ils sont soumis au test de préjudice à condition que ce dernier soit grave quel qu'il soit concomitant ou postérieur. Ils sont aussi soumis au test de l'intérêt public de l'accessibilité ou l'inaccessibilité à l'information quant à chaque demande. La proportionnalité entre les intérêts voulant les protégés et la raison de la demande d'accès, sera prise en compte.
En cas de refus, le demandeur d'accès sera informé par une lettre motivée. L'effet de refus prend fin avec l'expiration des motifs exprimés par la réponse à la demande d'accès.

Article 25

Le droit d'accès à l'information ne comprend pas les données relatives à l'identité des personnes ayant présenté des informations pour dénoncer des abus ou des cas de corruption.

Article 26

Les exceptions prévues à l'article 24 de la présente loi, ne s'appliquent pas :
- aux informations dont la divulgation est nécessaire en vue de dévoiler des violations graves aux droits de l'Homme ou des crimes de guerre ou les investigations y liées ou la poursuite de ses auteurs, à condition de ne pas porter atteinte à l'intérêt suprême de l'Etat,
- en cas d'obligation de faire prévaloir l'intérêt public sur le préjudice pouvant toucher l'intérêt à protéger, en raison d'une menace grave pour la santé ou la sécurité ou l'environnement ou par conséquent à la commission d'un acte criminel.

Article 27

Si l'information demandée est partiellement couverte par l'une des exceptions prévues aux articles 24 et 25 de la présente loi, l'accès à cette information n'est permis qu'après occultation de la partie concernée par l'exception, autant que cela est possible.

ANNEXE 5

Nouvelle charte éthique de la Fédération Internationale des Journalistes (FIJ)
Charte éthique mondiale des journalistes

[La charte d'éthique mondiale des journalistes de la FIJ a été adoptée lors du 30e congrès mondial de la FIJ à Tunis, le 12 juin 2019.Elle complète le Code de principes de la FIJ sur la conduite des journalistes (1954), dit «Déclaration de Bordeaux ».]

Préambule

Le droit de chacun.e à avoir accès aux informations et aux idées, rappelé dans l'article 19 de la Déclaration Universelle des Droits Humains, fonde la mission du journaliste. La responsabilité du/de la journaliste vis-à-vis du public prime sur toute autre responsabilité, notamment à l'égard de ses employeurs et des pouvoirs
publics. Le journalisme est une profession, dont l'exercice demande du temps et des moyens et suppose une sécurité morale et matérielle, indispensables à son indépendance. La présente déclaration internationale précise les lignes de conduite des journalistes dans la recherche, la mise en forme, la transmission, la diffusion et le commentaire des nouvelles et de l'information, et dans la description des événements, sur quelque support que ce soit.

1. Respecter les faits et le droit que le public a de les connaître constitue le devoir primordial d'un.e journaliste.

2. Conformément à ce devoir le/la journaliste défendra, en tout temps, les principes de liberté dans la collecte et la publication honnêtes des informations, ainsi que le droit à un commentaire et à une critique équitables. Il/elle veillera à distinguer clairement l'information du commentaire et de la critique.

3. Le/la journaliste ne rapportera que des faits dont il/elle connaît l'origine, ne supprimera pas d'informations essentielles et ne falsifiera pas de documents. Il/elle sera prudent dans l'utilisation des propos et documents publiés sur les médias sociaux.

4. Le/la journaliste n'utilisera pas de méthodes déloyales pour obtenir des informations, des images, des documents et des données. Il/elle fera toujours état de sa qualité de journaliste et s'interdira de recourir à des enregistrements cachés d'images et de sons, sauf si le recueil d'informations d'intérêt général s'avère manifestement impossible pour lui/elle en pareil cas. Il/elle revendiquera le libre accès à toutes les sources d'information et le droit d'enquêter librement sur tous les faits d'intérêt public.

5. La notion d'urgence ou d'immédiateté dans la diffusion de l'information ne prévaudra pas sur la vérification des faits, des sources et/ou l'offre de réplique aux personnes mises en cause.

6. Le/la journaliste s'efforcera par tous les moyens de rectifier de manière rapide, explicite, complète et visible toute erreur ou information publiée qui s'avère inexacte.

7. Le/la journaliste gardera le secret professionnel concernant la source des informations obtenues confidentiellement.

8. Le/la journaliste respectera la vie privée des personnes. Il/elle respectera la dignité des personnes citées et/ou représentées et informera les personnes interrogées que leurs propos et documents sont destinés à être publiés. Il/elle fera preuve d'une attention particulière à l'égard des personnes interrogées vulnérables.

9. Le/la journaliste veillera à ce que la diffusion d'une information ou d'une opinion ne contribue pas à nourrir la haine ou les préjugés et fera son possible pour éviter de faciliter la propagation de discriminations fondées sur l'origine géographique, raciale, sociale ou ethnique, le genre, les mœurs sexuelles, la langue, le handicap, la religion et les opinions politiques.

10. Le/la journaliste considérera comme fautes professionnelles graves le plagiat, la distorsion des faits, la calomnie, la médisance, la diffamation, les accusations sans fondement.

11. Le/la journaliste s'interdira de se comporter en auxiliaire de police ou d'autres services de sécurité. Il/elle ne sera tenu de remettre à ces services que des éléments d'information rendus publics dans un média.

12. Le/la journaliste fera preuve de confraternité et de solidarité à l'égard de ses consoeurs et de ses confrères, sans renoncer pour la cause à sa liberté d'investigation, d'information, de critique, de commentaire, de satire et de choix éditorial.

13. Le/la journaliste n'usera pas de la liberté de la presse dans une intention intéressée, et s'interdira de recevoir un quelconque avantage en raison de la diffusion ou de la non-diffusion d'une information. Il/elle évitera – ou mettra fin à – toute situation pouvant le conduire à un conflit d'intérêts dans l'exercice de son métier. Il/elle évitera toute confusion entre son activité et celle de publicitaire ou de propagandiste. Il/elle s'interdira toute forme de délit d'initié et de manipulation des marchés.

14. Le/la journaliste ne prendra à l'égard d'aucun interlocuteur un engagement susceptible de mettre son indépendance en danger. Il/elle respectera toutefois les modalités de diffusion qu'il/elle a acceptées librement, comme «l'off », l'anonymat, ou l'embargo, pourvu que ces engagements soient clairs et incontestables.

15. Tout-e journaliste digne de ce nom se fait un devoir d'observer strictement les principes énoncés ci-dessus. Il/elle ne pourra être contraint-e à accomplir un acte professionnel ou à exprimer une opinion qui serait contraire à sa conviction et/ou sa conscience professionnelle.

16. Reconnaissant le droit connu de chaque pays, le/la journaliste n'acceptera, en matière d'honneur professionnel, que la juridiction d'instances d'autorégulation indépendantes, ouvertes au public, à l'exclusion de toute intrusion gouvernementale ou autre.

ANNEXE 6

Recommandations pour la couverture médiatique en temps de crise (Snjt-Haica-médias) - mai 2016

Les mesures de sécurité à prendre ou à respecter lors d'une couverture médiatique

L'entreprise médiatique est responsable de l'intégrité physique de ses journalistes. Elle doit prendre toute disposition ou mesure pour assurer leur sécurité lors de l'exercice de leurs fonctions en zones dangereuses. Le rédacteur en chef doit garder un contact permanent avec les journalistes sur le terrain et identifier leur position pour intervenir rapidement en cas de blessure ou de disparition.

L'entreprise médiatique doit former ses journalistes à la couverture médiatique dans un contexte de violence et d'hostilité, aux premiers secours et leur fournir les moyens de communication adéquats pour les zones non couvertes par la téléphonie mobile. Le média met à disposition des journalistes des équipements de protection adaptés et un kit de premiers secours. Former les journalistes à la protection de leurs données.

L'entreprise médiatique doit assumer la couverture des soins médicaux et le suivi psychologique de ses correspondants en cas de choc psychologique résultant d'actes de violence.
(.....)

Traiter les manifestations violentes ou incitant à la violence

Le journaliste évalue la situation et prend les précautions nécessaires pour assurer sa sécurité physique et la sécurité de ses collègues pendant la couverture médiatique.

En cas de diffusion en direct, des dispositions doivent être prises pour empêcher la diffusion des discours attentatoires à la sécurité des citoyens ou incitant à la violence et à la haine. Le débat en direct peut être interrompu si les participants commettent des dépassements.

Si la présence du journaliste ou du média attisent les violences pendant la couverture d'une manifestation, marche de protestation ou autre, le journaliste et le média doivent évaluer la situation et, le cas échéant, se retirer des lieux.

La couverture d'une manifestation ne doit pas comporter d'images ou d'enregistrements sonores attentatoires à la vie privée et à la dignité humaine, qui peuvent mettre en danger la sécurité des personnes et des institutions.

S'assurer de ne présenter que des informations contextualisées répondant aux critères d'un traitement professionnel de l'information.

Présenter les faits ayant une plus-value informationnelle sans nuire aux opérations militaires ou sécuritaires en cours

Se limiter aux informations officielles et indiquer l'origine des informations non officielles. Vérifier la crédibilité de l'information par une multiplication des sources. Ne diffuser que les informations ayant une plus-value informationnelle qui ne nuit pas aux opérations en cours

Se limiter lors de la couverture en direct des opérations sécuritaires, des poursuites et perquisitions, aux images prises à distance sans identification des agents sécuritaires. Ne pas décrire de manière détaillée les lieux afin de ne pas mettre en danger les personnes et les infrastructures. Se limiter aux informations diffusées par des sources officielles lors d'opérations sécuritaires.

Limiter la couverture à sa dimension informative. Les médias doivent enrichir le débat public en favorisant un échange entre différents intervenants une fois l'opération terminée.
(...)

Gérer les messages de menaces ou incitant à la violence

Le journaliste ou le média doivent transmettre aux forces militaires et sécuritaires toute information faisant état de l'imminence d'une attaque terroriste.

S'abstenir de diffuser des informations pouvant propager la panique et la peur auprès de la population.

Le traitement des cas d'enlèvement et de prises d'otages

Ne pas diffuser ou publier en direct les messages des ravisseurs. Les enregistrements des ravisseurs doivent être remis aux autorités qui décideront des mesures les plus adéquates.

Ne pas diffuser les enregistrements des ravisseurs avec des otages implorant leurs ravisseurs ou en situation de désespoir. Se limiter en dernière nécessité à un nombre limité de plans fixes sans usage du son. Les extraits doivent être choisis en fonction de leur plus-value informationnelle.

Ne pas diffuser des extraits d'exécution d'otages afin d'éviter de servir ainsi l'objectif des terroristes visant à semer la peur et la terreur parmi la population.

ANNEXE 7

Contacts utiles :

Organisations travaillant sur la sécurité des journalistes

Syndicat national des journalistes tunisiens (SNJT) :
14 rue des Etats-Unis 1002 Tunis
Tel : 71 833 395
Unité de monitoring du Centre de sécurité des journalistes SNJT :
Khaoula Chabah : 93 281 067
Faten Hamdi : 94 870 596
Mahmoud Laaroussi : 98 478 433
http://protection.snjt.org

Bureau Unesco Tunis
App B1, Immeuble Saray, Rue du Lac Huron, Tunis 1053
Téléphone : 71 655 000

Haut commissariat des Nations-unies aux droits de l'Homme (HCDH)
La maison bleue, Rue du Lac Windermere, Imm. Prestige, bloc D- Les Berges du Lac I, 1053 Tunis
Tél. : 71 286 215/303/114

Reporters sans frontières
Adresse : 3, Rue des entrepreneurs- 1000 Tunis
Tél : 71 24 76 78
Courriel : afn@rsf.org