LA PRODUCTION MÉDIA EN ACTION MILITANTE

MISE À JOUR : 9/11/2023

Destiné aux équipe com et aux médiactivistes ce document n'a pas vocation à enseigner la photographie, la vidéo ou la communication. Il résulte d'une expérience de travail entre la production média et la com et a pour but de fluidifier ce travail collectif tout en le cadrant afin de protéger au mieux les militant.e.s et la coordination.

POUR L'ÉQUIPE COM

AVANT LE DÉPART EN ACTION

- Constituer l'équipe com et média et s'accorder sur un brief public à faire au reste des militants (informer sur la présence éventuelle d'un drone, indiquer la présence d'une équipe com' militante et comment l'identifier, rappeler les devoirs et méthodes d'anonymat...)
- Avoir un référent médiactiviste qui fera le lien entre la base arrière et avant.
- Création d'une boucle (Signal) com qui a vocation à briefer l'équipe, passer des commandes média et à recevoir le contenu. (Boucle non destinée aux stratégies de communication et info sensibles).
- Prévoir un ordinateur voir une personne en plus pour recevoir et traiter le contenu reçu.
- Prévoir un lien de dépose des images.
- Prévoir le jour J : une tente / des tables / électricité en supplément et séparée de la tente com pour les médiactivistes qui doivent bosser tout en préservant la confidentialité.
- Établir ou connaître les besoins pour les anticiper.
- Si possible, identifiez les moments et éléments clés.
- Se coordonner et se répartir le travail avec les autres membres de l'équipe en fonction des informations précédentes
- Pour les vidéastes : Envoyer les éléments graphiques (typo et logo) au monteur prévu.

⚠ ***Nombre des conseils de sécurité donnés aux médiactivistes sont utiles aussi pour les membres de l'équipe com.***

⚠ ***Les besoins photo et vidéo doivent être en adéquation avec les moyens disponibles. Il est important de se concentrer sur les images clés à avoir et ne pas viser un reportage exhaustif de l'action.***

⚠ ***Il est essentiel de pouvoir couvrir la multiplicité des actions et des gestes dans les moments de mobilisation, quel que soit le niveau d'offensivitée. Il y a une tendance générale à ce que les moments plus offensifs ou de confrontation aimantent les photographes et vidéastes. Personne n'échappe complètement au sensationnalisme ! Or après coup, on regrette souvent de n'avoir pas assez couvert les autres aspects des mobilisations. Avoir en tête cette donnée et se répartir dans les différents cortèges et ambiances pressentis peut permettre de corriger le tir. En revanche, il peut être déterminant dans des cas de violences policières et pour reconstituer des séquences d'avoir accès à des images. Si vous avez filmé certaines scènes de ce type, n'hésitez pas à entrer en contact avec la légal team tout en faisant particulièrement attention aux règles de sécurité sur ces fichiers »***

SUR SITE

Que faut-il avoir validé après le brief final ? (matin de l'action ou veille au soir)

- Les forces présentes et le matériel/compétences de chacun
- Savoir qui va où, pourquoi et quand ?
- Connaître au mieux les besoins photo et vidéos
- Quand et où livrer les photos en léger différé (et en quelle quantité)
- La stratégie en ce qui concerne l'anonymat et le floutage éventuel.

⚠ ***Il y aura des absents lors du brief, préparez un brief complet à mettre sur la boucle signal***

⚠ ***Profiter d'un brief public pour expliquer l'importance des images et la responsabilité de chacun dans l'anonymat.***

DURANT L'ACTION

- Maintenir le lien avec les médiactivistes
- Bien fait état de ses besoins
- Demandez des éléments de contexte afin de pouvoir produire les posts.
- Prendre soin de son équipe dans la manifs pour qui la situation peut-être stressante. Prendre soin de soi et la base arrière aussi.

APRÈS L'ACTION (soir même)

- Accueillir correctement son équipe (soin)
- Récolter les photos qui n'ont pu être envoyé en léger différée.
- Faire état des besoins et disponibilités des médiactivistes.

APRÈS L'ACTION (jours suivants)

- Bien vérifier la récolte de toutes les images nécessaires.
- Noter les contacts des médiactivistes motivés pour d'autres occasions.
- Toustes quitter la boucle signal avec des remerciements.


PAS

POUR LES MÉDIACTIVISTES

AVANT L'ACTION

- Connaître son niveau d'engagement, de disponibilité et de compétence et le partager à son contact
- Bien connaître le programme et les conditions
- Se tenir informer sur la boucle signal créée pour l'occasion.
- Préparer son matériel.
- Échanger avec d'autres médiactivistes et ne pas hésiter à poser des questions.

PRÉPARATION DE L'EQUIPEMENT

Le matériel de captation :

- Faire léger (2 objectifs maximum) pour pouvoir se déplacer rapidement et longtemps
- Être adaptable en focal (de 24 à 200) pour ne rien rater. (Sans changer vos habitudes non plus)
- Prévoir large en batterie/carte mémoire
- Vidéo : ne pas oublier le micro
- Un bon téléphone (éventuellement, un téléphone uniquement pour l'action afin de garantir une meilleure sécurité)
- Un sac afin de mettre tout le matériel nécessaire et être le plus autonome possible (alimentation et eau).

Le matériel de protection :

Selon le niveau d'intensité, plusieurs éléments de protection (lunettes, casque, masque à gaz, bouchons d'oreille, sérum physiologique, maalox, gants, gilet éventuellement...) sont à prévoir, si possible tout en permettant la prise de vue, lorsque portés.

Le brassard "presse" et/ou la vignette sur le casque : surtout si ça vous met à l'aise, car ça peut aussi susciter la méfiance des militants. À poser/retirer facilement. C'est un choix personnel de vouloir être considéré et traité comme militant ou presse.

⚠ ***Bien qu'équipé.e de matériel de protection, ne vous mettez pas en danger pour une prise de vue. Aucune photo ou vidéo ne vaut une blessure.***

SOFTWARE

- Installer/tester/paramétrer les applications en amont de la mobilisation
- Installer Exif cleaner pour effacer les métadonnées (Signal supprime les métadonnées lors de l'envoi)
- Installer Lightroom ou autre applis de retouche.
- Installer Application de transfert d'image liée à la marque de l'appareil
- Supprimer les métadonnées de l'exportation et informations du boitier
- Signal pour partager les clichés sur la boucle com
- VPN (proton ou autre).

ⓘ ***Remarque : Une description précise de ce qui est attendu en terme de sécurité informatique est à retrouver dans l'annexe technique, à la fin de ce document.-***

⚠ ***Le médiactivisme requiert d'avoir son téléphone, il faut donc le protéger. Pour vous et les autres. Il faut donc un mot de passe fort sur un terminal crypté. Pensez à désactiver le déverrouillage biométrique (empreinte digitale ou reconnaissance faciale) pour éviter tout déverrouillage sous la contrainte. Pensez aussi à enlever les notifications des applications en mode verrouillage et tout ce qui peut-être disponible et gênant accessible sans déverrouillage.***

(Voir Annexe)

SUR SITE

- Prenez le temps de prendre vos marques.
- Ne sortez pas de boitier de suite, prenez le temps de ressentir l'ambiance et de prendre des repères.
- Ne pas aller voir l'équipe com, si inconnu mais se référer à son contact.
- Échanger et être ajouté sur la boucle signal si oublie.
- Prendre le plus d'information possible sur le lieu, le programme, la lutte.

⚠ ***Ne pas manquer le brief médiactivistes.***

PENDANT L'ACTION

Une bonne photo correspond à un besoin et illustre ce que l'on veut raconter. On fait ici de la com, pas du journalisme, il nous faut des images qui mettent en valeur notre action. D'autres médias sont sur place pour nous dévaluer. Notre travail est aussi un travail de contre propagande (contre nous).

⚠ ***Il est essentiel de fournir aussi des éléments de contexte par vocal dans la boucle afin que l'équipe com puisse pouvoir légender les images. Nous sommes aussi les yeux et les oreilles de la base arrière.***

⚠ ***Vous faites partie d'une équipe, restez donc connectés aux autres pour être certains que toutes les demandes soient traitées au mieux.***

CONSEILS GÉNÉRAUX

- Rompre la glace avec la foule en discutant avec les personnes présentes et en se présentant.
- Toujours demander le consentement explicite et éclairé quand cela est possible.
- Bien axer son sujet et penser les prises de vue en terme de légende (chaque plan/photo correspond à un propos particulier)
- Bien avoir les différentes valeurs de plan
- Rester mobile et prévoir ces déplacements de façon à garder un temps d'avance.

Quelques idées de plans usuels : La foule ; les banderoles et messages ; les éléments visuels marquants ; l'action et ses gestes (dans les limites de la sécurité de celleux qui les posent) ; la police et le dispositif de maintien de l'ordre ; les différentes personnes et éléments constituant le cortège.

CONSEILS VIDÉO

- Prises de paroles publiques
- Une ou deux interviews qui expliquent en quelques phrases l'action et le contexte (un.e représentant.e de la lutte locale par exemple)
- Plans de transition/B-roll
- Un plan d'introduction et un plan de fin
- Avoir un plan de chaque étape significative (rassemblement/marche/action/violence policière/ blessé/joie)
- Avoir plusieurs valeurs de plan (large/serré/gros plan/abstrait)

⚠

- ***Penser à faire des plans assez longs et stables pour mettre éventuellement du texte dessus.***
- ***La stabilité permet la lisibilité, mais un plan de fuite, mal cadré, peut être très signifiant, surtout si le son est explicite.***
- ***Toujours préférer filmer un peu trop plutôt que pas assez.***
- ***Penser aux entrées/sorties de champ : elles permettent de vous assurer que le plan sera montable.***

LIVRABLE PHOTO

Dans le cadre d'un transfert direct sur téléphone : Choisir fichier 2M (environ) et non-fichier source pour gagner du temps.

2 options :

1. Envoi direct pendant l'action dès qu'un moment propice se présente.
2. Livraison le plus rapidement possible à l'équipe com en lien avec son contact.

Format web - 1500 / 1500 - 140DPI - 85% qualité (supprimer toutes les métadonnées)

Titrage : SDT_Action_Blase_Numéro de sequence_Date_WEB

Exemple : SDT_macadam_N_001_211023_WEB

LIVRABLE VIDEO

HD1080 / Débit 20 16/9 ou 9/16 à valider avec équipe com

Monter la vidéo et être disponible pour les modifications.

APRÈS L'ACTION

- Transmettre une sélection travaillée des photos le plus rapidement possible voir transfert de carte
- Sécuriser ses fichiers sources (voir annexe)
- Débriefer avec l'équipe com si besoin.
- Préciser à son contact si disponibilité pour d'autres actions

Annexe technique

Quelques conseils et remarques concernant la prise de vues et les fichiers qui en résultent

La prise de vue en tant que telle :

Si vous documentez une action ou tout autre évènement militant, veillez à demander systématiquement aux personnes concernées.e.s leur autorisation. Les photographies peuvent constituer un danger pour les militants. C'est pourquoi les photographies sont interdites en AG. En dehors de ce cadre, le respect du droit à l'image est primordial. Sans consentement explicite et éclairé possible (foules, vues d'ensemble...): si des photos avec visage.s identifiable.s (ou éléments distinctifs comme les tatouages) sont prises, il faut les anonymiser et détruire les photos non traitées si elles ne sont pas stockées sur un volume chiffré (pour chiffrer un volume/dossier spécifique, utiliser VeraCrypt. Pour chiffrer l'ensemble de son disque, utiliser BitLocker ou Veracrypt sur Windows et FileVault sur Mac). Pour cela vous pouvez utiliser l'outil "doigt" sur Photoshop ou apposer un aplat (rectangle) sur les parties sensibles (tatouages, visage...), qui sont préférables au floutage pouvant parfois être contourné par certains logiciels. Sur un appareil mobile, vous pouvez utiliser Obscura Cam.

La gestion des fichiers post-pdv

Effacer les métadonnées : ces informations qui nous trahissent

Les métadonnées sont un ensemble de données associé à un fichier (une image, une vidéo, un document texte, un PDF, un tableau Excel, etc.). Ces données varient mais révèlent quantité d'informations sur le contexte de création et d'utilisation du fichier, permettant aux personnes ayant accès à ce fichier de potentiellement remonter à son auteur.ice. Cela peut par exemple être les coordonnées GPS de l'appareil ayant pris une photo, les dates de création et de modification d'un fichier ou encore des informations permettant d'identifier l'appareil ayant créé le fichier. Avant de partager un fichier à d'autres personnes, il est donc absolument crucial de supprimer ces métadonnées. Plusieurs méthodes existent. Tout d'abord, Signal supprime automatiquement les métadonnées des images envoyées, pas besoin de s'en faire de ce côté-ci. Pour les autres fichiers partagés sur Signal, il faudra supprimer les métadonnées en amont. Pour ce faire, vous pouvez utiliser ExifCleaner.

⚠ ***Attention : ExifCleaner nettoie les fichiers PDF que partiellement!***

Pour supprimer les métadonnées d'une image depuis un smartphone Android, vous pouvez utiliser ImagePipe, cet outil permet également de réduire la taille d'une image pour la partager plus facilement. Pour d'autres fichiers, il est recommandable d'utiliser la fonction mat2. Ce programme est directement intégré dans Tails, il suffit alors de faire un clic droit sur le fichier en question puis cliquer sur «Remove metadata», une nouvelle version du fichier avec l'extension «.cleaned» apparaîtra et correspondra à la version du fichier sans métadonnées.

ⓘ ***Remarque : Les métadonnées ne sont pas à confondre avec les cookies ou autres fichiers temporaires qui sont des traces laissées par vos activités sur votre ordinateur. Ces dernières méritent cependant notre attention car elles pourraient être compromettantes (sauf sur Tails, construit de telle façon que ces préoccupations ne s'appliquent pas). Pour effacer ces traces, CCleaner est un outil de choix.***

Supprimer correctement un fichier : la corbeille vous joue des tours

Lorsqu'on clique sur «supprimer ce fichier», on ne l'efface pas réellement, on le rend simplement invisible à l'utilisateur : il est désindexé, comme si un chapitre d'un livre n'était plus accessible après la suppression de sa mention dans le sommaire, bien que les pages correspondantes existent toujours. Les données correspondantes sont toujours gravées dans le disque dur ou la mémoire flash du SSD. Un accès physique à votre machine (en cas de perquisition par exemple) pourrait permettre de mettre au jour ces données. Pour remédier à cela, il faut utiliser Eraser sur Windows ou Permanent Eraser sur Mac.

Pour ces considérations, il est prudent de limiter au maximum le téléchargement de documents en lien avec l'activisme sur votre ordinateur personnel, afin d'éviter d'oublier de supprimer correctement les fichiers en question, au profit du partage de liens (CryptDrive notamment).

Protéger son ordinateur et téléphone.

Sur l'action, vous devrez avoir votre téléphone pour envoyer les images en direct et recevoir les infos et commandes de l'équipe de com. Il est donc indispensable que votre téléphone soit sécurisé.

Sur Android : Création d'un mot de passe de 16 chiffres ou lettres et signes.

Sur Iphone : Choisir dans les options (ID et mot de passe) un mot de passe alphanumérique et noter sa passe phrase.

Pendant l'action : Définir la demande de mot de passe à chaque verrouillage ou 1 minute. Si on appuis sur les boutons pour éteindre le téléphone, le mot de passe sera demandé. Au quotidien vous pouvez allonger cette durée pour rendre la logistique moins chronophage.

Création de la pass phrase : Utilisation d'un dés et d'une liste de mots ou d'un générateur de passe phrase. 5 mots de 5 chiffres minimum. Voir https://diceware.fr

Le logiciel Keepass vous permet de conserver des mots de passe en les protégeant mais aussi de générer des mots de passe ou passe phrase. https://keepass.info/

Ordinateur : Mettre sa passe phrase ou autre mot de passe puissant en ouverture de session. Ne pas avoir un nom d'utilisateur en relation avec sa vraie identité. Pensez à cleaner les informations accessibles sans mot de passe comme le nom de la session.

Connexion internet : Afin d'être mieux protéger et en supplément du VPN, il est possible d'utiliser un routeur (boitier comme un gros disque dur. prix : Entre 100 et 200 euros). Celui ci permet une conection internet sécurisée et anonyme.

Configuration de Signal pour éviter les failles :

Minimum syndical à configurer pour un smartphone (certains points ne sont pas possibles sur iphone + certains points impossible à configurer sur pc)

Appliquer le guide du bon usage de Signal :
- Forcer le clavier en mode privé (confidentialité -> Clavier incognito)
- Mettre le timer à 1 semaine par défaut pour les nouvelles conversations (confidentialité -> Minuterie pour les nouvelles conversation = 1 semaine)
- Mettre en place un PIN pour protéger son compte (confidentialité -> Verrou d'écran)
- Toujours activer le relais via les serveurs Signal pour les appels (confidentialité -> avancés -> toujours relayer les appels)
- Changer l'icône Signal dans son téléphone (Apparence -> icone de l'appli)
- Empêcher la prévisualisation des liens (Conversation -> Décocher "Générer des aperçus de lien)

Comment protéger ses disques durs avec Veracrypt

Afin de protéger les images que l'on stocke sur nos disques durs et qui sont des images non floutées car brut (fichier raws / catalogue lightroom ou autres). Il est nécessaire de protéger nos disques.

Utiliser Veracrypt en utilisant sa passe phrase comme mot de passe. : https://www.youtube.com/watch?v=_hP3_vmVRWc

Attention : Le disque dur doit être vierge car il sera formaté durant l'opération.

Pour ouvrir la partition protégée, il vous faudra toujours Veracrypt.

Autres ressources

Des infos diverses sur la com et autre : https://lutteslocales.fr/documenter-la-lutte/

Les bases de la photographie : https://www.naturephotographie.com/debuter-en-photographie/

Avec rage et détermination