Sécurité et encryption: Réflexions et conseils sur la photographie militante et la défense collective

Jo

Mai 2024

TLDR

- Respectez le consentement des gens, et soyez pas des rapaces à vous jeter sur les moindre trucs sensationels, au dépit des camarades qui peuvent être dans le mal, ou peuvent être entrain de prendre des risques.
- Floutez toutes les photos, même si rien d'illégal ne semble apparaitre dessus.
- Trouvez des techniques par rapport aux GAV et perquisitions pour éviter de donner les photos pas floutées aux flics.
- *selon moi* ne prenez pas toujours votre appareil photo, parfois profitez d'une manif sans prendre de photos.

Introduction

On voit de plus en plus de photographe professionnel et amateur aussi bien dans les manifestations déclarées que dans les actions plus clandestines. Même si la photographie militante est un outil de propagande puissant en multipliant le nombre de personnes touchées par une action, elle doit aussi être réfléchie au sens de la défense collective puisque les photographies et vidéos que nous prenons peuvent être réutilisés par la police et la justice pour faciliter notre propre répression.

J'écris ce (court) texte pour rapporter les réflexions que j'ai eu dans ma propre pratique de la photographie militante, et en m'appuyant sur ma propre expérience de la répression mais aussi celles des personnes autour de moi. Comme la répression évolue perpétuellement, avec des moyens toujours plus techniques, et que nos moyens de propagande évoluent aussi, ces réflexions autour de la propagande et de la défense collective devraient être réactualisées en permanence, mais aussi et surtout discutées collectivement.

Je ne suis pas non plus juriste (et même si la question de la loi est intéressante, il faut aussi considérer que la police peut agir sans la respecter), et certaines questions restent ouverte pour moi car je n'ai pas eu les temps de les approfondir (comme la possibilité d'encryption des photos prisent avec certains appareils photo numérique) ou parce que je manque de connaissance.

a - "l'usage personnel" et les téléphones

Avant de se concentrer sur la photographie amateur, on parlera rapidement de la forme de photographie en manif/action la plus dangereuse et aussi la plus dure à contenir: les photos et vidéos "à usage personnel" prises avec des téléphones.

On a sans doute toustes pris une photo d'une scène amusante ou impressionnante en manifestation sans y réfléchir plus que ça. Certain.es ont même ensuite poster ces photos ou vidéos. Et c'est assez logique puisqu'on est habitué.es à avoir son téléphone à portée de main pour immortaliser n'importe quel souvenir. Pourtant dans un cadre militant ces photos peuvent mettre en danger d'autres militant.es, et parfois soi-même.

Toutes les questions qui seront développées plus bas s'appliquent évidemment aux photos et vidéos prises avec un téléphone (particulièrement le problème de la fouille des téléphones en cas d'arrestation). Le problème est qu'il est plus dur de convaincre les personnes qui sortent simplement un téléphone en manif d'avoir de bonnes pratiques vis-à-vis de la défense collective.

Il y aurait une "culture de l'antirep" à developer, et qui devrait rentrer en concurrence avec la culture de tout prendre en photo et poster (qui a largement empiré la repression lors des emeutes suite au meurtre de Nahel par un flic). Mais c'est assez difficile puisque la première ne peut se développer que dans le milieu militant, alors que la seconde se développe dans l'entièreté de la société.

1 Consentement

*Disclaimer: Ce texte se concentre beaucoup plus sur **l'aspect technique et l'aspect d'antirep** de la photographie que l'aspect politique et humain qu'il y a dans quand et si on prend des photos.*

Pour autant ce n'était pas possible de parler de photographie militante sans faire un très court paragraphe sur ces questions, donc voilà:

Le but globalement c'est de **respecter le consentement des gens**. Donc si possible avant de prendre des photos de gens demander si c'est ok.

Quand c'est dans une foule, parfois c'est pas possible, donc peut être qu'on peut ou pas prendre des photos (ou pas, c'est un débat, je pretend pas y répondre), mais dans ce cas on anonymise les gens parce qu'on leur a pas demandé de montrer leur visage (on dit pourquoi plus loin dans le texte).

Parfois on a **explicitement pas le droit de prendre des photos** (c'est une décision collective dans certaines ZAD et même manif). Bah dans ce cas on respecte cette décision.

Parfois il y a pas de possibilité de decision collective (quand les actions sont organisée de manière autonomes et sans forcement des gros lieux d'organisation formel), mais **c'est mal vu de prendre des photos** (pour des raisons souvent assez légitime). Bah ce "mal vu" peut être vu comme une forme de refus. **Si tout le monde grince des dents quand on prend une photo, c'est qu'on devrait peut être pas en prendre.**

Et surtout, **soyez pas des rapaces !**

- Evitez de vous jeter sur les blessé.es pour les filmer/photographier: c'est humiliant et ça peut augmenter le stress.

- Evitez de vous jeter sur chaque actions violentes pour les filmer/photographier: ça fait des preuves pour la police et la justice, et ça devient caricatural tous les photographes qui s'attroupent autour de chaque poubelle qui brûle.

Et un conseil perso que je m'applique: Ne prenez pas toujours votre appareil photo, profitez d'une manif ou d'une action sans de temps en temps. Si vous prenez des photos, ne restez pas devant les banderoles et allez dans les cortèges de temps en temps. Sinon vous n'êtes plus un.e militant.e, mais un.e journaliste.

2 Anonymisation

Anonymiser les photos que l'on prend et publie est un aspect très important de la défense collective car les photos que l'on prend **peuvent être utilisées par la justice ou la police**: par la justice dans des procès pour prouver la culpabilité d'une personne, ou par la police pour justifier des mesures répressives (perquisition, arrestation, etc..) lors d'une enquête.

Il faut donc cacher les visages (flouter est déjà bien, mais les recouvrir d'une couleur uni est encore mieux) sur les photos montrant des actions illégales avant de les publier.

Mais même les photos ne montrant à priori pas d'actions illégale peuvent (même si plus rarement) être utilisées par la police et la justice: **en identifiant les vêtement d'une personne dans une photo non-flouté ne montrant rien d'illégale pour ensuite les recroiser avec une photo lors d'une action illégale, en justifiant la présence à une manifestation (même légale) à une personne qui ne devrait pas être là (OQTF, interdiction de manifester, etc)**.

2.1 Floutage de toute la photo/video

Certaines personnes, quand iels veulent poster des photo et surtout des vidéo rapidement les floutent entierement.

Ça peut soit être fait en **floutant la photo avec un logiciel** (mais du coup les risques en cas d'arrestation ou perquisition permettant aux flics d'avoir accès à la photo/vidéo claire subsistent), ou **en filmant la vidéo hors de focus** ce qui assure que la vidéo ne sera pas (ou difficilement) exploitable même si elle est récupéré avant que vous partiez de la zone de manifestation.

2.2 Floutage automatique

Il existe une multitude d'outils pour flouter/couvrir les visage automatiquement, dont beaucoup en ligne. L'outil que j'utilise personnellement car il est rapide pour un grand nombre de photos est "***deface***" (une librairie python qui peut être installée et utiliser comme un script sous linux, avec de nombreux paramètres).

Mais simplement couvrir de carré noir les visages à la main dans un editeur de photo (canva, photoshop ou autre) suffit largement.

3 Risques en cas d'arrestation ou de perquisition

Même si l'on fait attention à ne mettre personne en danger lorsque l'on publie des photos, il reste le risque de **se faire arrêter/perquisitionner avec son appareil sur soi et qu'il soit fouillé**.

Avec des photos sur un appareil digital ou un téléphone et sans carte de presse qui pourrait vous protéger (ou pas), se faire arrêter en manif ou action donnera (potentiellement, légalement ou pas) accès à la police à vos photos.

3.1 Encryption sur un appareil photo digital

3.1.1 Sur un téléphone

Bonne nouvelle ! Les smartphones sont encryptés (je ne m'y connais pas assez: **faites vos propres recherches**). Il est *sans doute possible - mais peut être compliqué* - pour la police d'accéder à vos photos prises sur un téléphone sans votre consentement.

Même si c'est compliqué d'accéder à vos photos sans votre consentement, la police s'attend à trouver des choses sur votre téléphone et cherchera donc à le fouiller en vous demandant votre code. **Lisez des guides d'antirep**. Vous êtes parfois "obligé.e" de le donner, vous pouvez ne pas le faire (ce qui est une bonne idée si c'est pour vous protéger et protéger d'autres personnes), mais il peut y avoir quelques conséquences (encore une fois, lisez des guides d'antirep).

Il existe aussi sans doute des applications pour téléphone permettant d'encrypter et surtout de cacher des photo dès qu'elles sont prisent pour rendre leur accès impossible sans une clé. Il faut cependant s'assurer de leur bon fonctionnement avant de leur faire confiance.

3.1.2 Avec un plugin

C'est assez difficile d'empêcher l'accès aux photos prise avec un appareil digital, même si il existe certaines rare piste pour crypter des photos sur des appareils digitaux (un plugin non-fini de "***MagicLantern***" pour **les appareil Canon**, un firmware custom pour le **Samsung NX-300** et sans doute quelques autres pistes aussi peu nombreuse que compliqué à appliquer).

3.1.3 Avec une carte SD encryptée

Disclamer: Fuck toutes les marques, le but ici n'est pas de faire l'éloge d'une marque. Mais malheureusement il n'y a qu'une entreprise qui fait un produit comme ça donc on va devoir en parler.

Il existe aussi une carte SD (pour dire le nom du produit qu'une fois: "***swissbit iShield Archive/Camera***") qui permet d'encrypter les photos sur *n'importe quelle caméra*. C'est de l'encryption hardware: basiquement la carte SD créer une "session" quand elle est démarée, la caméra peut écrire et lire dessus normalement, mais quand elle est eteinte cette "session" est encryptée et n'est plus accessible à moins de lire la carte SD sur un ordinateur avec le programme nécéssaire et d'avoir le code PIN.

Quelques experiences perso du produit:

- *Le produit et les logiciels sont **mal documentés**, mais leur support technique est plutot réactif.*
- *Il y a une **courte liste de caméras officiellements supportées** par cette carte SD, **mais ma caméra n'est pas dessus et ça marche**...*
- *...mais **il faut que je formate la carte SD à chaque démarage** de l'apareil photo (je ne perd pas les anciennes photos qui ont été encryptées) sans quoi je risque de la saturer et de ne plus pouvoir prendre de photo au prochain démarage.*
- *Sous **(arch) linux** pour que je puisse controler la carte SD il fallait que je connecte la carte SD avec un **adaptateur micro-SD vers USB** pour qu'elle se monte à un point **"/dev/sdxx" plutot que "/dev/m..."**.*

On joint en bas de ce document un script bash pour decrypter et copier tout les fichiers de toutes les sessions depuis la carte SD.

3.2 L'argentique pour rendre les fouilles plus compliquées ?

L'argentique ? C'est pas un truc de bourgeois qui est redevenu à la mode ? Si, mais on va qand même en parler.

Une technique peut être d'utiliser un appareil argentique pour rendre l'accès aux photos plus complexe, en supposant que **les policiers ont peu de chance de développer les pellicules eux-même**, et risque même de détruire les photos en les exposant à la lumière par erreur. Le plus sécurisé serait alors de développer et (surtout) scanner ses pellicules soi-même.

On peut ensuite aussi anonymiser les photos directement sur la pellicule en rayant/trouant les pellicules avant de les scanner. On peut aussi anonymiser les photos scannées.

Même si la photographie argentique est généralement chère, il faut dire qu'utiliser un appareil prenant des photo demi-format (comme un **Canon demi**) permet de prendre 2 fois plus de photos par pellicule (donc 72 photos par pellicule de 36 pour un coût total de ∼0.40€/photo).

3.3 Archivage et perquisitions

En cas de perquisition, les flics peuvent fouiller vos archives photos ce qui peut les faire remonter jusqu'à des copaines qu'ils n'avaient pas encore identifiés.

Du coup pour l'archivage numérique: **encryptez vos ordis et vos disques durs d'archivages**.

Et pour l'argentiques: **soit vous ne gardez pas d'archives argentiques, soit vous les anonymisez en rayant les pellicules.**

Conclusion

Que ce soit dans la photo ou ailleurs, il faut faire attention dans le militantisme (mais pas que) aux conséquences que peuvent avoir nos actions vis-à-vis des autres et de nous même, surtout par rapport à la répression.

Pour que cela soit efficace, il faut en discuter collectivement, créer une culture de l'antirep (ce qui est possible, certain elements d'antirep comme "j'ai rien à déclarer" sont extrêmement connus), surtout lorsqu'il y a un compromis à faire entre propagande et antirep (en choisissant de s'autoriser ou pas les vidéo, les photos non-floutées et même les photos tout-court).

Je pense qu'il faut surtout que l'on fasse collectivement attention aux "petites actions" qui peuvent être très couteuses, comme l'ont été les photos et vidéo prisent et diffusées lors des emmeutes suite au meurtre de Nahel.

Annexe: script pour sortir des fichier d'une cart SD encryptée *Swissbit*

```
mnt_pt=""
out_folder=""
while getopts 'm:o:' flg; do
    case "${flg}" in
        m) mnt_pt="${OPTARG}";;
        o) out_folder="${OPTARG}";;
        *) exit 1;;
    esac
done

if [ ! -d ${out_folder} ]
then
    mkdir -p ${out_folder}
fi

read -p 'Unlock password (blank if already unlocked): ' -s sec_pin
if [ ! -z "${sec_pin}" ]
then
    iATcli ${mnt_pt} login --pin ${sec_pin}
fi

sess_list=$(iATcli ${mnt_pt} listSessions \
        | tail -n +2 | awk '{print $1;}' | paste -sd " " -)

mnt_fold=$(grep ${mnt_pt} /etc/mtab \
        | awk '{print $2;}')

for sess in $(echo "${sess_list}")
do
    iATcli ${mnt_pt} switchToSession --id ${sess}
    rsync -a --ignore-existing "${mnt_fold}/" ${out_folder}
done
```