AUTODÉFENSE NUMÉRIQUE – QUELQUES BASES

Quelques infos et pratiques utiles, non exhaustives, pour l'usage militant d'ordinateurs, téléphones et internet.

« Une chaîne à la force de son maillon le plus faible »

Que faire ?

Tout dépend de ce qu'on a à cacher. C'est pas la même chose de préparer des collages d'affiches ou des gros sabotages d'infrastructures clefs. À chaque groupe/personne d'adapter sa sécurité. Mais en général, c'est toujours une mauvaise idée d'avoir son téléphone sur soi en manif ou en action. On peut se dire aussi qu'il ne faut jamais échanger d'informations compromettantes par SMS ou par appel téléphonique. Plus globalement, il est conseillé de ne pas se servir d'outils numériques pour préparer des choses compromettantes, sauf quand on en a vraiment besoin et alors avec moults précautions. **Il faut aussi se souvenir que les keufs utilisent toujours leurs bonnes vieilles méthodes, d'enquêtes, d'espionnage et de renseignement, que c'est plus simple pour elleux de faire des contrôles d'identité à toustes les participant.es d'un rassemblement plutôt que d'identifier toutes les personnes ayant borné sur les lieux de ce rassemblement**, et de « filer », de suivre, quelqu'un.e que d'installer un logiciel espion récupérant la géolocalisation d'un téléphone. Et attention aux caméras qui sont partout !

Il faut adapter nos pratiques de sécurité en fonction de ce qu'on fait, des niveaux de répression, de ce qu'on est capable de tenir sur la durée (changements d'habitudes à mettre en place). Distinguons ici 3 types d'actions militantes différente. C'est grossier et simpliste, dans la réalité les frontières peuvent êtres plus floues et mouvantes, mais ça permet d'entrer dans du concret.

1. Le militant de gauche « classique »

Cette personne type ne fait que des actions à peu près légales : manifs, rassemblements, grève, tractage, écriture d'articles, pétitions, organisation d'événements légaux…
Tant qu'on n'est pas dans un régime franchement fasciste/dictatorial, elle pourrait se dire qu'elle n'a rien à cacher et donc qu'elle n'a pas besoin de prendre de précautions particulières.
Erreur, pour 4 raisons principales :

1. Evolution - Un jour elle pourrait passer à des actions illégales (par exemple si toute contestation devient illégal). Etant déjà fichée/repérée, elle pourrait plus facilement être retrouvée/confondue.
2. Maillon faible - Dans le(s) réseau(x) dont fait partie cette personne, il y a peut-être des personnes pratiquant des activités illégales (ou s'y mettant un jour). Si cette personne militante ne prend aucune précaution numérique, elle est le maillon faible facilitant l'identification de tout le réseau par les flics.
3. Solidarité - Si de nombreuses personnes (militantes ou non) utilisent régulièrement plusieurs outils/pratiques de sécurité numérique, alors les personnes pratiquant des activités illégales utilisant ses mêmes outils seront noyées dans la masse et plus difficilement identifiables/ciblables que si elles sont les seules à les utiliser.
4. Le régime en place est déjà très autoritaire, et se dirige vers bien pire encore, donc éviter de lui laisser trop d'infos sur qui arrêter/ficher/surveiller est important pour limiter plus tard les possibilités de raffles massives de personnes affiliées à gauche.

2. L'activiste

Cette personne participe occasionnellement ou régulièrement à des actions illégales (ou plus offensives), de type émeute avec barricades et de la casse ciblée, manifestation spontanée qui se voit interdite, blocage, péage gratuit, tags, dégradations, messages incendaires sur le web, affichage sauvage avec messages subversifs…
Elle ne va a priori pas être visée par les lourds moyens antiterroristes (même si les fichages et écoutes divers s'étendent, notamment grâce aux logiciels automatisés de surveillance), mais il est indispensable qu'elle prenne de grandes précautions, d'autant qu'elle pourrait très bien un jour aller vers des actions encore plus offensives.

3. Le sabotage

Une personne pratiquant occasionnellement ou régulièrement des destructions conséquentes de biens, d'infrastructures, de bâtiments, de voitures, de câbles... par le feu ou avec des outils.
Ici, la surveillance, les enquêtes et la répression se font beaucoup plus forts, avec souvent de gros moyens et même l'utilisation abusive des services antiterroristes.
La sécurité numérique doit donc être maximale ici. Le plus sûr étant de ne pas utiliser d'outils numériques, si possible, pour ces activités là.

Outils qui « devraient » être utilisés par tout le monde, au moins pour les usages militants :

- Installer Signal sur smartphone, pour appels, messages et envois de fichiers
- Créer une boite email anonyme chez un hébergeur « militant » (type riseup.net), et créer des email alias différents pour les éventuels divers cercles/réseaux (en gardant secrète l'adresse de la boite elle-même)
- Si possible, venir aux réunions, actions et autres sans

son tél (ou alors l'éteindre avant de venir, le mieux étant de le laisser allumé à la maison)
• Installer un lecteur de flux RSS (non commercial) pour suivre les sites web engagés/militants
• Utiliser un VPN (Mullvad..., Proton & Riseup ont une version gratuite)
• Utiliser un maximum le navigateur furtif TOR (https://www.torproject.org), surtout si vous n'avez pas de VPN (TOR remplace un VPN pour nombre d'usages), notamment pour consulter votre boite mail militante et des contenus subversifs
• Remplacer applis tél commerciales par des applis libres
• Si possible, utiliser Mastodon et Invidious.io au lieu des réseaux sociaux commerciaux et de Youtube
• Utiliser Jitsi pour les réunions en visio
• Sur votre navigateur web stantard (Firefox de préférence), installer les extensions : Ublock, Privacy Badger et Cookies autodelete
• Utiliser des mots de passe solides et les stocker dans le gestionnaire KeePassXC
• Supprimer vraiment des fichiers avec Eraser (Windows) ou Bleachbit (Linux) – Vider la Corbeille est très insuffisant

Suppléments pour le type 2 activiste :

• Se documenter davantage pour comprendre le numérique et les moyens de la police
• A la place de Windows ou Mac, installer un système linux avec chiffrement du disque dur
• Ne pas utiliser les réseaux dits sociaux, ou uniquement pour des choses persos/familiales
• Crypter le téléphone et utiliser un mot de passe pour l'ouvrir
• Voir peut-être d'autres messageries pour tél ? Comme olvid.io ?
• Se réunir sans « micros »
• Venir aux réunions, actions et autres sans son tél
• Créer un compte XPMPP et installer Conversation sur son tél pour les messages instantanés
• Paramétrer Signal pour l'anonymat maximum (auto-effacement des messages, utiliser un pseudo…)
• Utiliser le système d'exploitation 'furtif' Tails (qui démarre sur clef usb), surtout pour les choses les plus sensibles
• Conseillé aussi : Stocker ses données sur ordi dans un volume caché VeraCrypt
• Pour les envois de gros fichiers (qui ne passent pas par email), utiliser des hébergeurs sûrs ou militants (riseup.net, proton.me/drive, swisstransfer.com…)
• Anonymiser toutes les publications web (et supprimer les métadonnées des images et fichiers publiés)
• Si besoin, utiliser en action des téls « anonymes » (acheté en espèces, pas utilisé chez soi, avec carte SIM type Lycra), ou des talky
• Utile aussi : Stocker ses données dans un volume caché VeraCrypt
• Utiliser des dispositifs permettant de détecter des intrusions physiques au clavier ou un ordi (vernis multicolore sur vis, marques spéciales…)
• Bonus : Sur tél, à la place d'Android, installer un OS alternatif type LineageOS

Suppléments pour le niveau 3 « sabotage » :

• Ne pas utiliser le tél et internet (ou le moins possible) (mais garder éventuellement un usage perso standard consensuel, et plus généralement avoir une vie publique de « bon citoyen »)
• Se rencontrer dans des lieux neutres et variés
• Eviter de transporter des docs et outils, éviter le stockage
• Installer Mumble sur Tails pour les appels
• Utiliser XMPP chez un hébergeur militant, et utiliser Pidgin sur Tails pour les messages instantanés
• Avoir éventuellement un ordi portable non relié à soi (acheté en espèces et jamais utilisé via une connexion internet reliable à soi), l'utiliser avec Tails, et si besoin d'internet, le faire qu'avec des connexions publics (en vérifiant l'absence de caméras)
• Créer et partager ses clés PGP pour les messages mails via Tails
• Utiliser OnionShare sur Tails pour les envois de fichiers
• Vérifier par moment l'absence de dispositifs de surveillance et de traçage sur les véhicules/vélos utilisés, dans et autour du domicile…
• etc.

Culture de la sécurité

Etre vigilant.e et respecter le niveau de sécurité de chacun.e.
Demander, ou donner, une info uniquement si cela est nécessaire.
On ne raconte pas à tout le réseau ses actions illégales.
Ne conserver un document que s'il est nécessaire.
Ne pas avoir sur soi de document ou d'outil dont on n'a pas besoin.

Quelques brochures utiles, trouvables sur internet :
sur https://infokiosques.net/ :
• Guide de survie en protection numérique à l'usage des militants
• Cultures de la sécurité (dépasse la question numérique)
• Téléphonie mobile
• TuTORiel Tails
« Fadettes, UFED et données de connexion » (sur https://paris-luttes.info et d'autres)
(de nombreuses ressources sont dans ces brochures, qui elles-mêmes renvoient à d'autres ressources)

Ce doc est une synthèse de divers documents, il est sans doute incomplet, subjectif, imparfait, et peut comporter des erreurs.