PETIT GUIDE DE SÉCURITÉ POUR MILITER

DÉJOUER L'ÉTAT POLICIER

Anti-répression - Sécurité numérique - Auto-organisation

Version Mars 2024

ANTI-RÉPRESSION - SÉCURITÉ NUMÉRIQUE - AUTO-ORGANISATION

Militer en sécurité c'est lutter en adoptant des pratiques visant à réduire les risques. Ce petit guide a pour vocation de donner une vue d'ensemble sur plusieurs problématiques auxquelles nous sommes toustes confronté·es en tant que militant·es. Cette brochure s'adresse à tout le monde, que vous soyez novice ou expérimenté·e. Dans le climat actuel, il est primordial de s'informer sur les bonnes pratiques à adopter. On a voulu aborder trois grands sujets qui nous semblaient primordiaux. L'anti-répression de la rue aux tribunaux et quelques astuces pour la manif. En seconde partie, la sécurité numérique à travers la téléphonie, l'informatique et des traces que l'on laisse en utilisant ces dispositifs, on vous apportera des applis et des outils complémentaires afin de réduire les risques. Pour finir, nous aborderons les questions d'auto-organisation et la culture de la sécurité. Nous n'avons pas la prétention d'être expert dans tous les sujets, de nombreuses brochures et guides bien plus complet sont disponibles. À la fin de cette brochure vous trouverez une petite bibliographie que nous vous conseillons grandement de consulter pour compléter nos informations.

Militer en sécurité c'est lutter en adoptant des pratiques visant à réduire les risques. Ce petit guide a pour vocation de donner une vue d'ensemble sur plusieurs problématiques auxquelles nous sommes toustes confronté·es en tant que militant·es. Cette brochure s'adresse à tout le monde, que vous soyez novice ou expérimenté·e. Dans le climat actuel, il est primordial de s'informer sur les bonnes pratiques à adopter. On a voulu aborder trois grands sujets qui nous semblaient primordiaux. L'anti-répression de la rue aux tribunaux et quelques astuces pour la manif. En seconde partie, la sécurité numérique à travers la téléphonie, l'informatique et des traces que l'on laisse en utilisant ces dispositifs, on vous apportera des applis et des outils complémentaires afin de réduire les risques. Pour finir, nous aborderons les questions d'auto-organisation et la culture de la sécurité. Nous n'avons pas la prétention d'être expert dans tous les sujets, de nombreuses brochures et guides bien plus complet sont disponibles. À la fin de cette brochure vous trouverez une petite bibliographie que nous vous conseillons grandement de consulter pour compléter nos informations.

4 - SOURCES À LIRE

Voici une liste non exhaustive des sources qui nous ont permis d'écrire ce petit guide. Elles apporteront beaucoup de précision sur tout les sujets que nous avons abordés. Nous vous conseillons vivement la lecture des brochures et articles disponibles sur le site infokiosques.net !

ANTI-RÉPRESSION :

« PETIT MANUEL DE DÉFENSE COLLECTIVE : DE LA RUE AU TRIBUNAL ! » Défense Collective Paris-Banlieues, 2022

« EN GAV JE N'AI RIEN À DÉCLARER » Manuel BD de conseils en garde à vue, 2021

« LISTE DE DISPOSITIFS DE SURVEILLANCE DÉCOUVERTS » 2022

« LA FOLLE VOLONTÉ DE TOUT CONTRÔLER » 2020

« MANUEL DE SURVIE EN GARDE À VUE » 2010

« COMMENT LA POLICE INTERROGE ET COMMENT S'EN DÉFENDRE » Projet Evasion sur projet-evasions.org 2022

« AFFAIRE "LAFARGE". LES MOYENS D'ENQUÊTE UTILISÉS ET QUELQUES ATTENTIONS À EN TIRER » 2023

« PAS VUE PAS PRISE, CONTRE LA VIDÉOSURVEILLANCE » 2023

SÉCURITÉ NUMÉRIQUE :

« GUIDE DE SURVIE EN PROTECTION NUMÉRIQUE À L'USAGE DES MILITANT·ES » 2021

« GUIDE D'AUTO-DÉFENSE NUMÉRIQUE » sur guide.boum.org 2023

« TÉLÉPHONIE MOBILE » 2023

« FADETTES UFED ET DONNÉS DE CONNEXION » sur paris-luttes.info

« TUTORIEL TAILS » 2020

AUTO-ORGANISATION :

« COMMENT FORMER UN GROUPE AFFINITAIRE » sur crimethinc.com

« CULTURES DE LA SÉCURITÉ » 2007

« COMMENT SE PROTÉGER ET PROTÉGER NOS LUTTES » 2023

La culture de la sécurité ne doit pas non plus fermer votre groupe, il est précieux de trouver des allié·es et des sympathisant·es qui pourraient vous prêter main forte, ou des personnes de confiance qui pourraient vous rejoindre. Il est important de faire du lien avec les autres individu·es et groupes, à vous de voir si vous souhaitez vous ouvrir et comment.

Voici plusieurs exemples de 'niveaux' de confidentialité répondant à des besoins différents :

1 - Seul·e·s celleux qui sont impliqué·e·s directement dans l'action ont vent de son existence.
2 - Le groupe décide au cas par cas de dévoiler l'action à des personnes de confiance dont le soutien est nécessaire.
3 - Le groupe peut inviter à participer à l'action des personnes qui pourraient refuser — il en résulte que des personnes extérieures peuvent être au courant de l'action, tout en étant censées tenir leur langue.
4 - Aucune liste précise de personnes invitées n'est dressée ; les participant·e·s peuvent inviter d'autres personnes et les encourager à faire de même, tout en insistant sur la nécessité de garder l'information dans des sphères dignes de confiance pour en conserver le secret.
5 - Des « rumeurs » de l'action peuvent être largement répandues au sein de la communauté, mais l'identité des personnes centrales pour son organisation doit rester secrète.
6 - L'action est largement annoncée, tout en conservant un minimum de discrétion, afin que les autorités les plus somnolentes n'en aient pas vent.
7 - L'action est annoncée publiquement par tous les moyens possibles.

Le mot action ci dessus peut-être aussi une réunion, un rendez-vous, un groupe etc.

Auto-formation et sources

Les techniques de répression évolue, c'est très utile de se renseigner sur les enquêtes et procès en cours ou passés, des articles documentent régulièrement sur les derniers outils de surveillance et les moyens mis en oeuvre afin de coincer les militants. On vous conseille la lecture de la brochure « AFFAIRE "LAFARGE". LES MOYENS D'ENQUÊTE UTILISÉS ET QUELQUES ATTENTIONS À EN TIRER » dispo sur infokiosques.net ou expansive.info (un site du réseau Mutu).

SOMMAIRE

1 - ANTI-REPRÉSSION 4
Avant la manif 4
Pendant la manif 5
Garde à vue 6
Tribunal 6
Protection de la vie privée sur internet 7
2 - SÉCURITÉ NUMÉRIQUE 7
Sur smartphone 8
Communications 8
Messageries chiffrées 9
Notifications 10
Quelques pistes pour être anonyme 10
Sur ordinateur 11
Tor Browser 11
Chiffrement des données avec VeraCrypt 12
Système d'exploitation non persistant - Tails 13
Mail 14
Transfert de fichier 14
3 - AUTO-ORGANISATION 15
S'organiser 15
Groupe affinitaire 16
Culture de la sécurité 16
4 - SOURCES À LIRE 19

1 - ANTI-REPRÉSSION

Vous le savez surement déjà, la répression des mouvements politiques contestataires s'amplifie depuis de nombreuses années. De la rue aux tribunaux, nul·le n'est épargné·e par les arrestations préventives en manif, les gardes à vue, les perquisitions. Cela n'arrive pas qu'aux autres, alors pour se préparer au mieux à la répression policière et judiciaire, voici quelques conseils. Nous recommandons vivement la lecture du « *PETIT MANUEL DE DÉFENSE COLLECTIVE : DE LA RUE AU TRIBUNAL !* » par la Défense Collective Paris-Banlieues dont nous nous sommes inspiré, disponible sur infokiosques.net.

Avant la manif

Avant une manif, il est bon de préparer ses garanties de représentations en cas de GAV. Ce sont des papiers (factures EDF/tél à son nom, contrat de travail ou promesse d'embauche, justificatif de domicile, certificat de scolarité) qui prouvent que vous êtes inséré socialement, que vous avez des contraintes (travail) et que vous n'allez pas vous barrer à l'autre bout du monde. Ces documents ont de la valeur aux yeux des juges, et cela peut nous éviter d'être placé en détention provisoire en vue d'un éventuel procès. Ces papiers doivent être donnés à un·e proche qui ne se rend pas en manif et qui se tient prêt à fournir ces documents à votre avocat·e.
Il peut être aussi judicieux de faire le ménage chez soi, les perquisitions peuvent avoir lieu pendant la GAV pour saisir du matos informatique, des stickers ou des brochures militantes par exemple et ainsi permettre de vous incriminer.
Il est bon de préparer ses affaires et de ne rien laisser au hasard. Évidemment pas de drogue ou tout objet dangereux pouvant être considéré comme une arme, les contrôles préventifs aux abords des manifs sont monnaies courantes. Laissez votre téléphone à la maison pour éviter le bornage sur les lieux de la manifs ou pire, qu'il finissent entre les mains des flics. Prévoyez du cash pour éviter de payer en CB si vous le devez (payement par CB = traçabilité). Si vous prenez les transports en commun, optez pour un ticket plutôt que votre pass à votre nom pour les mêmes raisons. Des médics sont souvent présent·es pendant les manifs, mais vous pouvez toujours emmener une petite trousse de secours au cas où.

Ce n'est pas parce que vous ne commettez rien d'illégal qu'il ne faut pas adopter une culture de la sécurité. En faisant cela, vous participez activement à la protection de vos proches et même des militant·es éloigné·es, qui ont elleux peut-être des activités subversives à cacher dont vous n'avez pas connaissance. Plus nous sommes nombreux·euses à adopter ces pratiques, moins ces pratiques deviennent suspectes et exposent à de la répression.
Si tout le monde sait qu'il ne faut pas parler de chose sensible par téléphone, alors les écoutes ne serve plus à rien. Un principe de base : personne ne devrait être mis au courant d'une information sensible qu'iel n'a pas besoin de connaître. Plus des infos compromettantes sont répandues, plus il y a de chance qu'elles tombent entre de mauvaises mains. Alors pour éviter les surprises, le mieux est de ne pas en parler, vous ne pourrez jamais gérer une information qui vous échappe. Et puis partager avec quelqu'un une info sensible, c'est la mettre dans une position inconfortable, elle ne pourra plus clamer honnêtement son innocence, iel aura quelque chose à cacher pendant une GAV par exemple.

Il faut aussi se demander quelles traces laisse t-on : paiements en CB, transport en communs, bornage téléphonique, envoie d'un sms, passage devant une caméra de vidéo-surveillance etc. Toutes ces traces sont des informations qui peuvent être récupérées, certaines sont moins sensible que d'autres, mais en les croisant toutes cela permet de dresser un profil de qui vous êtes. Il faut prendre conscience de ses traces, pour savoir lesquelles sont bonnes à cacher, savoir lesquelles laisser. Lorsque l'information est collectée, elle peut-être stockée pour toujours. Une info n'est pas forcément sensible peut le devenir plus tard, en fonction de l'évolution des systèmes politiques. Par exemple, imaginons qu'un régime totalitaire passe au pouvoir, le fait d'être un simple militant antifasciste ou opposant politique pourra alors être criminalisé, ou servir de départ pour une répression plus poussée.

On vous conseille d'avoir un blaze, un peusdo, ou même plusieurs suivant les environnements que vous fréquentez, ou vos activités. Un pseudo ça vous évite évidemment de vous rattacher à votre identité, et d'en avoir plusieurs permet de segmenter suivant plusieurs niveaux de sécurité, mais ça ne résistera probablement pas à une enquête approfondie. N'utilisez pas de pseudo déjà connu ou que vous pouvez avoir sur les réseaux, il ne doit pas évoquer l'une de vos traces laissées.

À vous de réfléchir à la circulation de l'info, qui doit-être au courant ? À quel moment ? Est-ce bien nécessaire ? Ne pas donner une info à quelqu'un ne veut pas dire qu'on ne lui fait pas confiance, mais simplement qu'iel n'a pas besoin de cette information.

Groupe affinitaire

Le groupe affinitaire est un modèle d'organisation qui se veut détaché et libre des structures traditionnelles. S'organisant sur la base d'affinité politique et/ou amicale, être en groupe affinitaire, c'est considérer que vous pouvez constituer une force politique autonome. L'idée est que des personnes qui se connaissent déjà peuvent se faire confiance et s'organiser ensemble.
Dépourvu d'instance hiérarchique, le GA se veut horizontal et autonome, cela à l'avantage d'être libre de s'adapter à n'importe quelle situation de manière réactive. Il est primordial de s'accorder sur des désirs et envies communes, les groupes fonctionnant généralement par décisions prises collectivement au consensus. Il est important de discuter entre vous de vos propre limites personnelles, chacun·e doit se sentir à sa place, il ne doit pas avoir plusieurs vitesses au sein du groupe. À ce sujet il y a « Comment former un groupe affinitaire » disponible sur fr.crimethinc.com.

Culture de la sécurité

Vous devrez adopter une culture de la sécurité, c'est à dire mettre en place des pratiques qui visent à à réduire les risques de se faire prendre, de contenir toute fuite d'information pouvant vous nuire ou vous mettre en danger vis à vis des forces répressives ou de l'extrême-droite, et de renforcer votre sécurité. Il s'agit de protéger sa personne et les individu·es que vous côtoyez.
On vous conseille vivement à ce sujet la lecture de deux brochures : « Culture de la sécurité » traduit et adapté de *CrimethInc,* et « Comment se protéger et protéger nos luttes, premier pas de la mise en place de pratiques de sécurité » disponible tout deux sur infokiosques.net

À vous d'établir votre modèle, cela dépend de vos ennemi·es, contre qui vous luttez. De qui se protéger ? De la police, de la justice, des fascistes, de l'administration ou même de son entourage. De quoi doit on se protéger ? Du fichage et de la surveillance. La surveillance des individu·es et des groupes politiques passe par de nombreuses méthodes : écoutes, filatures, géolocalisation, exploitation des données numériques, les moyens techniques sont nombreux comme nous l'avons vu précédemment. Le fichage quand à lui compile toutes ces infos et les rends disponibles à plusieurs acteurices : flics, justices, fafs, entreprises entre autre. La répression ne touche pas seulement les personnes ayant commise des actes illégaux, mais aussi leur entourage, ou tout simplement des gens identifiés comme simple militant·es même si iels n'ont rien organisé ou n'ont pas participé à l'action.

Attention, en cas de contrôle et suivant le contexte, des lunettes de piscines contre le gaz lacrymo, du sérum physiologique ou un masque à gaz peuvent être très mal considéré et cela peut vous valoir une arrestation préventive. Pensez à bien cacher ces éléments dans un double fond par exemple, pas forcément sur vous, les fouilles corporelles sont aussi courante.
Ne vous précipitez pas au lieu de rassemblement, repérez d'abord les différents accès, les points de contrôles et évitez les tant que possible. Il est judicieux de se renseigner aussi sur les effectifs policiers, leurs tactiques et les armes qu'ils emploient. Si vous n'avez pas vos papiers lors d'un contrôle, les keufs peuvent vous emmener au comico pour une vérification d'identité pour une durée maximale de 4h. Mais ça peut-être aussi une stratégie de ne pas les prendre.

Pendant la manif

Pendant la manif, restez concentré·e sur les mouvements des keufs, leurs positions. Une charge peut sortir de nulle part et vous surprendre. Restez en binôme en veillez l'un·e sur l'autre. Les manifs violentes sont éprouvantes psychologiquement, cela peut laisser des traumas, alors si vous ne le sentez pas ce n'est pas grave. Ne courrez pas en cas de gaz, les mouvements de foule peuvent être dangereux et cela pour fait ingérer plus de lacrymo à votre organisme. Attention, renvoyer les palets lacrymogènes est un délit, considéré comme un jet de projectile. Il est difficile de passer inaperçu·e en manif, entre les caméras de surveillance, les objectifs des appareils photos et les smartphones, la capture d'image est omniprésente. Pour éviter de vous faire identifier, cachez vos cheveux, vos bijoux, tatouages etc. Vous pouvez toujours vous réfugier derrière un masque chirurgical pour plus de discrétion plutôt qu'un tour de cou ou une cagoule. Dissimuler volontairement son visage sans motif légitime est un délit depuis les lois "anti-casseur" d'avril 2022. De même, on pourra vous placer en GAV et vous poursuivre au tribunal sans que vous n'ayez rien fait, grâce au groupement en vue de commettre des dégradations ou des violences. C'est à dire que tout élément suspect aux yeux des keufs pourraient se retourner contre vous : une cagoule, un masque à gaz, des pétards, une bombe de peinture, une arme par destination etc.
Ne ramassez jamais une grenade envoyée par les keufs. JAMAIS. Les modèles de grenades lacrymogènes se confondent avec les grenades explosives type GM2L. Pareil on ne shoote pas dans une grenade au risque de perdre son pied. Si vous avez une capuche, portez la sur la tête ou rentrée dans le col de la veste, une grenade ou un palet lacrymo pourraient tomber dedans et se coincer, vous occasionnant des brûlures ou bien pire.

Garde à vue

En cas d'arrestation, vous serez emmené au commissariat ou gendarmerie pour être placé en garde à vue. Celle-ci dure potentiellement 24h, prolongeable d'encore 24h, et pouvant aller jusqu'à 72h dans certain cas. Vous avez le droit de demander un médecin, et de passer un appel téléphonique à un·e proche (généralement les keufs l'appellent à votre place). On va vous demander votre signalétique, c'est à dire une prise d'empreinte digitale et un prélèvement ADN. Vous pouvez refuser mais cela est passible de poursuite. Un OPJ (officier de police judiciaire) va alors vous interroger. Tout ce que vous dites peut alors se retourner contre vous et vous incriminer. Vous avez le droit de garder le silence avec " je n'ai rien à déclarer ". La défense en vue d'un procès ne se construit pas au commissariat, il ne faut pas instruire soi-même son dossier, ou celui de camarades. Les flics vont vouloir vous faire chanter, vous dire que vous sortirez plus tôt si vous parlez. Les flics n'ont pas forcément des éléments à charge contre vous, c'est pour ça qu'ils vont tenter de vous faire parler. Ne rien déclarer c'est aussi protéger les autres, ne parlez pas si l'on vous demande des informations sur les copaines. On va pas vous le cacher, ça va être dur, la GAV c'est éprouvant moralement. Vous s'y préparer, deux brochures à lire : « MANUEL DE SURVIE EN GARDE À VUE » sur infokiosques.net et « COMMENT LA POLICE INTERROGE ET COMMENT S'EN DÉFENDRE » Projet Evasion sur projet-evasions.org 2022

Tribunal

Si poursuite il y a, vous allez être déféré·e devant un tribunal pour une comparution immédiate. Vous êtes en droit de la refuser et de demander un renvoi du procès, ce que nous vous conseillons vivement. En effet vous n'aurez pas le temps de préparer votre défense, de trouver un bon avocat, les commis d'offices sont souvent de mauvais conseils. Et généralement, les peines sont plus sévères en compa immédiate. C'est là que rentre en compte les garanties de représentations citées précédemment. En cas de renvois du procès, lae juge va décider de votre remise en liberté ou non. Avec de bonnes garanties, cela peut vous éviter la détention provisoire. Si l'on vous remet en liberté, cela peut-être assorti d'un contrôle judiciaire avec l'obligation de pointer au commissariat toute les semaines par exemple. On peut aussi vous proposer une CRPC (comparution sur reconnaissance préalable de culpabilité), sorte de deal avec la juge, on vous propose une peine en échange de le reconnaissance de votre culpabilité, il ne s'agit pas d'un procès, vous n'aurez pas le droit à une défense. C'est donc à éviter.

Il est impératif de supprimer ces infos avant que le fichier quitte votre ordi. En effet, une fois partagé, vous n'avez plus le contrôle sur celui-ci, il pourrait tomber entre de mauvaises mains et un adversaire pourrait récupérer les infos contenues au sein du fichier. Il existe des applications sur Windows et MacOs comme ExifCleaner, sur le système Tails il existe une appli dédiée, ou alors faire clic-droit « Remove metadata ».

Mais partez du principe qu'il est toujours préférable d'éviter d'utiliser les outils numériques ceux-ci comportant des failles de sécurité. Rien ne vaut le papier et un crayon ou une conversation orale sans son téléphone. Si l'on devait résumer, il faut séparer ses activités, d'un côté votre vie quotidienne, de l'autre les activités militantes en utilisant les différents outils cités précédemment. Sur internet, ça se passe sur Tor. Une fois TorBrowser installé, vous pouvez naviguer sereinement sur des sites militants, consulter vos mails, des sites comme infokiosques.net ou télécharger Tails et VeraCrypt.

3 - AUTO-ORGANISATION

S'organiser

Vous souhaitez vous organiser pour des enjeux qui vous tiennent à coeur mais vous ne savez pas comment vous y prendre, ni par où commencer ? Il existe peut-être des collectifs ou des organisations proches de chez-vous. Syndicats, collectif écolo, féministe ou antifasciste, de nombreux·euses militant·es sont déjà sur le terrain, il peut être judicieux de vous rapprocher d'elleux si ces sujets vous intéresse. Il existe plein de façon de lutter, on appelle ça la diversité des tactiques. C'est l'idée selon laquelle tout les groupes affinitaires et autres organisations plus formelles peuvent choisir quelles stratégies et quelles tactiques iels souhaitent employer sans se discréditer entre elleux, en vue d'un même objectif. Chacun·e a son rôle à jouer dans la lutte, peut importe la manière, les différents moyens d'actions pouvant être complémentaires.

Mail

Pour communiquer, recevoir des newsletters ou pour tout service qui demande une adresse mail, il est bien évidemment déconseillé d'utiliser son mail personnel et de passer par les hébergeurs classiques : gmail, outlook, laposte, hotmail etc... Nous vous conseillons vivement de créer via Tor un compte sur Riseup, Disroot, Systemli. Nous déconseillons ProtonMail, car iels ont collaboré avec les keufs lors d'une enquête.
Évidemment, pour avoir une adresse mail anonyme, il ne faut pas qu'elle soit rattachée à votre adresse IP, il faut alors impérativement passer par le réseau Tor pour la créer et s'y connecter. Néanmoins les mails peuvent être interceptés si ceux-ci ne sont pas chiffrés. Pour y remédier, il y a le protocole OpenPGP.

Pour chiffrer ses mail de bout en bout, il faut passer par le chiffrement PGP :

1. PGP génère une paire de clés : une clé publique, qui ne sert qu'à chiffrer, et une clé privée, également appelée clé de session, qui sert à déchiffrer.
2. Le destinataire de l'e-mail transmet la clé publique à ses contacts.
3. Le contact utilise la clé publique pour chiffrer l'e-mail, puis l'envoie.
4. Le destinataire utilise sa clé privée, dont il est seul détenteur, pour déchiffrer l'e-mail.

Le fonctionnement de PGP pour authentifier l'expéditeur :

1. L'expéditeur signe son e-mail avec sa clé privée.
2. Avec la clé publique dont il dispose, le destinataire vérifie que c'est bien l'expéditeur qui a envoyé l'e-mail, il s'assure ainsi que le contenu est intègre.

Pour plus d'information, lire le " guide d'autodéfense numérique" sur le chiffrement PGP dispo sur guide.boum.org.

Transfert de fichier

Des services comme Disroot ou Riseup, ou sur Tails avec OnionShare permettent d'échanger des fichiers à distance comme le ferait Wetransfert. Avec Disroot, le fichier est chiffré en sortie du navigateur, ça veut dire qu'il pas lisible pour celleux qui espionneraient vos connexions ou le serveur sur lequel transite les données. Attention, les fichiers (PDF, JPEG, PNG, textes etc) contiennent des métadonnées. Ce sont toutes sortes d'info comme le nom de l'auteur·e, la date et l'heure de création, le logiciel utilisé, l'OS, le numéro de série du téléphone/appareil photo etc.

Protection de la vie privée sur internet

La protection de la vie privée, c'est important. Ce que l'on entend par là, c'est les traces de votre vie intime, quotidienne que vous laissez sur internet à travers les réseaux notamment. En cas de GAV, les flics peuvent fouiller les réseaux sociaux pour trouver des choses incriminantes comme des photos en manifs, des partages d'articles etc. Il ne faut pas se protéger seulement de la police, mais aussi de l'extrême-droite et des fascistes en tout genre. En effet, au vu du climat de plus en plus nauséabond avec la prolifération d'agressions et de rassemblement de l'extrême-droite, les fafs sont sur le qui-vive et cherchent à identifier les opposant·es politiques. Le doxxing, pratique qui vise à révéler des informations confidentielles comme l'identité, l'adresse, dans le but de nuire à une personne est de plus en plus fréquente. Cela se passe tout les jours dans les canaux de discussions fafs sur Telegram. Il est sage de séparer alors sa vie personnelle et sa vie militante, en ayant deux comptes séparés, l'un dédié au militantisme, l'autre à sa vie perso. Passez vos compte en privé, masquez vos listes d'ami·es, les comptes que vous suivez etc. Les fafs font du recoupement d'infos par ces biais là, iels vont chercher à identifier les militant·es antifascistes, syndicaux à travers les likes ou des commentaires laissés sur les publications. Évitez d'utiliser les mêmes pseudos d'une plateforme à une autre. Les photographies prisent en manifestation peuvent aussi servir de base de recherche pour les fafs et les logiciels de reconnaissance faciale disponible sur internet sont des outils puissants et permettent aisément de retrouver un tas de photo de vous sur la toile, permettant peut-être de vous identifier ou de trouver des informations confidentielles et sensibles. Faites le ménage donc et évitez d'être trop bavard·e sur les internets.

2 - SÉCURITÉ NUMÉRIQUE

Les outils numériques sont à la fois de précieux alliés mais aussi de sacrés mouchards comme nous le verront plus loin. Du téléphone à l'ordinateur, les failles de sécurités sont nombreuses, vous laisserez des traces qui peuvent déterminer quelles sont vos activités sur le réseau mobile et sur internet. On peut savoir ce que vous avez fait, les lieux que vous fréquentez, avec qui vous parlez, qui vous rencontrez, la liste est longue. Il ne s'agit pas de tomber dans la paranoïa mais d'être averti·e sur les risques que l'on encours. Le savoir est le pouvoir. Une bonne culture de la sécurité permet au contraire d'être serein·e dans son quotidien.

Sur smartphone

Attention le téléphone est le pire mouchard qui existe. Éviter tant que possible d'avoir des documents, photos sensibles dessus, ou tout ce qui pourrait vous incriminer. Un téléphone c'est quasiment impossible à sécuriser. Mais il existe des solutions afin de laisser moins de trace. Chaque téléphone possède un numéro IMEI qui l'identifie de manière unique, tout comme la carte SIM qui possède un IMSI. La ligne téléphonique est reliée à votre identité, le numéro IMSI vous « appartient » et est jumelé avec le numéro IMEI du téléphone. Ceux-ci sont donnés aux antennes relais lorsqu'on se connecte au réseau, permettant de vérifier que le téléphone a bien le droit de communiquer sur le réseau mobile.

Communications

Pour communiquer, ne jamais passer par des SMS/Appel. Pourquoi ? Parce que toute communication non-chiffrée est interceptable par les keufs. Chaque SMS, appel échangé laisse des traces. Sans directement mettre sous écoute, simplement en regardant les fadettes, sorte de registre de donnée qui comprend pour une ligne téléphonique : les antennes relais auquel le téléphone a borné, la liste des communications qu'elle a eu avec d'autres lignes, et les numéros IMEI et IMSI, les keufs peuvent savoir où vous êtes allé, avec qui vous avez échangé, et ça de manière très simple sans passer par des réquisitions judiciaires. Si vous êtes mis·e sous écoute, le contenu des SMS, appels et les data seront alors disponibles pour les autorités. Le téléphone borne, ça veut dire qu'il envoie et qu'il reçoit un signal d'une antenne téléphonique à quelques minutes d'intervalle et de manière automatique, avec ou sans carte SIM. L'opérateur est donc au courant à quelle antenne vous vous connectez et à quelle distance. Cela veut dire que vous vous êtes rendu dans telle zone géographique qui correspond à celle de l'antenne. Par procédé de triangulation, on peut déterminer précisément votre géolocalisation, et ça sans GPS ! Plus le maillage des antennes est resserré, plus la triangulation sera précise. En ville donc précis à quelques mètres près, en campagne où les antennes sont plus éloignées, ça peut aller de quelques centaines de mètres à plusieurs kilomètres si il y a qu'une seule antenne. Avec le bornage, on peut être en mesure de savoir que plusieurs indivu·es se retrouvent ensemble, en réunion ou lors d'actions par exemple. Pour éviter qu'un téléphone borne, c'est éteint ou en mode avion. Mais bon le mieux c'est évidemment de ne pas prendre son tél avec soit ! Attention, un téléphone éteint ou inactif pendant le temps de l'action peut être considéré comme suspect. (lire attentivement « *AFFAIRE "LAFARGE". LES MOYENS D'ENQUÊTE UTILISÉS ET QUELQUES ATTENTIONS À EN TIRER* » dispo sur infokiosques.net)

l'utilisation d'un tel chiffrement n'exclut pas que la justice parvienne par d'autres moyens à démontrer l'existence de données chiffrées.

Système d'exploitation non persistant - Tails

En utilisant un ordinateur, vous laissez des traces : les sites que vous avez visité même en navigation privée, les fichiers supprimés peuvent être récupéré, vos connexions aux réseaux wifi peuvent être tracée grâce à l'adresse MAC qui identifie de manière unique toute carte réseau (tout ordinateur ou périphérique connecté à un réseau en comporte une). Même sur ordinateur il est difficile de passer inaperçu si l'on veut vraiment cacher ses activités. Les risques d'infection par des virus compromettants vos machines sont réels, on peut alors accéder en théorie à tout ce qu'elles contiennent comme infos, enregistrer votre écran ou ce que vous tapez sur le clavier et voler vos mots de passes enregistrés par exemple. Pour s'en prémunir, nous vous conseillons d'utiliser Tails, un système d'exploitation conçu pour limiter les risques et déjouer la surveillance

Nos ordis tournent sur un OS, par exemple Windows, MacOs, Linux, installé sur un disque dur interne, qui laisse des traces comme nous l'avons vu. Il existe un système d'exploitation libre et gratuit, Tails, qui s'installe sur une clé USB d'au moins 8go et qui ne laisse pas de trace. Au lieu de démarrer sur un OS classique installé sur le disque dur, on démarre sur l'OS de Tails installé sur la clé USB branchée. C'est comme un nouvel ordinateur sur votre machine. Le système est dit amnésique ou non-persistant. C'est à dire qu'à chaque fois que l'on éteint le système, tout est remis à zéro, sans laisser aucune trace. Tails va utiliser la mémoire vive au lieu du disque dur interne, celle-ci est effacée intégralement à chaque fois que l'on éteint l'ordi. Aucun risque donc qu'une donnée perdure dans le temps. Tails permet d'échapper à la censure et évite d'être tracé grâce à sa connexion au réseau Tor et le système usurpe votre adresse MAC pour en donner une fausse, les réseaux WIFI ne sauront donc pas qu'il s'agit de votre ordinateur.

Tails est fourni avec une sélection d'application permettant de travailler en autonomie sur le système : bureautique, montage photo/son/vidéo, navigateur Tor, déchiffrement de volume VeraCrypt etc. Il est aussi possible d'activer la persistance, c'est à dire sauvegarder des données ou des paramètres, ceux-ci seront enregistrés sur la clé USB et non pas le disque dur. Pour plus d'info sur Tails, referez vous à la documentation du site tails.net, ou à l'excellent « *TUTORIEL TAILS*" disponible sur infokiosques.net et au « *GUIDE D'AUTODÉFENSE NUMÉRIQUE* ».

Les FAI ont l'obligation de garder pendant un an les listes de connexions, donc ce que vous faites sur internet, quels sites vous visitez etc.
Ils ont aussi l'obligation de fournir ces informations aux autorités dans le cadre d'une enquête. Sans parler des services de renseignements qui sont en capacité de suivre et d'analyser votre trafic internet. En utilisant Tor, votre connexion transite par trois noeuds (serveur) différents, chaque noeud connaissant seulement le serveur d'avant et d'après. Le serveur 1 connait votre IP et celle du noeud 2, mais ne connaît pas l'identité du 3e ni le site de destination. Le serveur 2 ne connaît pas votre adresse, mais celle du 1er et du 3e noeud. Le 3e ne connait que le 2e et la destination finale. Le site visité quand à lui, ne connaît pas votre IP réelle et pense avoir affaire avec le noeud trois. Si les keufs surveillent le trafic vers un site militant par exemple, iels ne seront pas en mesure de savoir qui se connecte réellement. Si les flics surveillent votre trafic à vous, iels ne pourront pas savoir vers quels sites vous allez, par contre iels sauront que vous utilisez Tor, car la connexion transite toujours via votre FAI en premier lieu avant d'arriver sur le réseau Tor. Pour éviter cela, il est possible de se connecter à un pont. Nous ne détaillerons pas cela, d'excellents tutos sont disponibles sur le site torproject.org.

Chiffrement des données avec VeraCrypt

Sur ordi, les disques durs ne sont généralement pas chiffrés. C'est à dire que les données contenues apparaissent en clair, quiconque peut alors y accéder et les lire. En cas d'enquête et de perquisition, le matos informatique est généralement saisi pour analyse. Ce qui intéresse les enquêtrices se sont les données contenues dans vos disques durs, clés USB, carte SD téléphone etc. Si vous travaillez sur des documents sensibles qui ne doivent pas tomber entre de mauvaises mains, il faut impérativement chiffrer son support de stockage. Chiffrer c'est rendre illisible les données pour une personne ne possédant pas le code de déchiffrement. Néanmoins refuser de donner une convention de chiffrement (code du téléphone, code d'un support chiffré) est passible de poursuite, 3 ans d'emprisonnement et 270 000€ d'amende. Heureusement, une solution existe avec le logiciel VeraCrypt (Windows, Mac, Linux). Il permet de cacher l'existence d'un volume chiffré. Un volume c'est une partition numérique, un gros fichier conteneur, comme une clé USB virtuelle en quelque sorte. Pour cela il y'a un système de double mot de passe, un "faux" et un "vrai". Le faux va donner accès à premier volume chiffré. Si vous devez donner un mot de passe sous la contrainte c'est celui là. Le "vrai" va quand à lui donner accès au volume chiffré caché, celui-là vous ne le donnez jamais car vous n'y serez pas obligé, les adversaires ne pouvant pas en théorie déceler l'existence du volume caché. Mais la prudence reste de mise, il n'y a pas de jurisprudence à ce sujet et

Messageries chiffrées

Signal :

Pour se prémunir de l'interception des communications il existe les applications de conversations chiffrées. La plus connue et la plus efficace reste Signal. Elle permet de converser de manière chiffrée, c'est à dire que seul vous et lae destinateurice peuvent avoir accès au contenu des messages. Ne pas oublier d'activer les messages éphémères (destruction automatique des échanges) par défaut sur un court laps de temps, de quelques minutes à quelques jours suivant les contextes. En effet, en cas de GAV ou de perquisition, les flics pourront toujours avoir accès à votre téléphone et les messages qu'il contient. Signal est aussi disponible sur ordi (Windows et Mac) ce qui peut être utile pour se passer des fichiers par exemple. Les conversations de groupes sont aussi chiffrées contrairement à l'appli Telegram. Cependant avec Signal, les métadonnées peuvent être interceptées, on pourrait techniquement savoir avec qui vous conversez, et à quelle heure, mais cela n'est pas à la portée de tout les flics.[MAJ2024] Depuis une mise à jour, Signal permet de cacher votre numéro de téléphone et de définir un nom d'utilisateur pour vous retrouver. (option> confidentialité>numéro de téléphone, mettre sur « personne » pour « qui peut voir mon numéro de tél » et « qui peut me trouver grâce à mon numéro de tél ») puis définir un nom d'utilisateur en cliquant sur votre pseudo pour aller dans « profil » dans les paramètres.

Briar :

Pour éviter cela il existe une autre appli de messagerie : Briar. Elle permet en plus de s'affranchir du réseau mobile en s'établissant via les connexions wifi et bluetooth des utilisateurices, ou alors via le réseau Tor (nous y reviendrons). Les conversations sont chiffrées, et stockées sur votre téléphone protégée par un robuste mot de passe, et non pas sur un serveur centralisé qui stockerait les messages. L'avantage est que Briar permet de se passer du réseau téléphonique en utilisant les connexions wifi et bluetooth des utilisateurices à portée et qu'il n'y a pas besoin de numéro de tél pour s'inscrire.

Matrix :

L'application Matrix permet de converser suivant le même protocole de chiffrement que Signal, le numéro de téléphone n'est pas requit pour s'inscrire, un mail est cependant demandé. Pour créer un mail sécurisé et anonyme, reportez vous à la section « mail » de la brochure.

Notifications

Il est préférable de désactiver les notifications des messageries chiffrées. Si votre téléphone tombe entre de mauvaises mains, les notifs peuvent s'afficher sur l'écran d'accueil un téléphone verrouillé, donnant ainsi accès aux derniers messages. Plus inquiétant encore, d'après un article sur France Info, les services des gouvernements auraient accès aux notifications qui transitent par les services d'Android (Google) et d'Apple, ces derniers sont en capacité de connaître le contenu pour le bon fonctionnement technique des notifs. Pour éviter de se faire espionner de la sorte, désactivez l'affichage du contenu des notfications, ou désactivez-les tout simplement pour être bien sûr·e que personne n'y aura accès.

De même, ajouter un code de sécurité sur vos applications de messageries chiffrées pour les verrouiller est une bonne idée, ne pas mettre le même code que pour le déverrouillage du téléphone.

Quelques pistes pour être anonyme

Pour être réellement anonyme avec un téléphone, par anonyme on entend qu'un bigot et un numéro ne puissent pas être rattachés à votre identité, il faut suivre quelques précautions : acheter sa carte SIM et le téléphone en liquide. Comme ça le numéro IMSI de la carte SIM ne sera pas rattaché à vous, tout comme le numéro IMEI du téléphone, qui l'identifie de manière unique. Mais attention à ne pas avoir les mêmes habitudes qu'avec son téléphone de tout les jours. Ne jamais utiliser ce téléphone chez soi ou en même temps que son bigot habituel : éviter de le faire borner chez vous, ou dans des lieux que vous fréquentez régulièrement. Ne pas se servir d'un ancien téléphone que vous avez déjà utilisé, le numéro IMEI était associé avec l'IMSI relié à votre identité.

Des services spécialisés de flics ont les capacités d'infecter votre smartphone avec des logiciels espions. Lors de grosses enquêtes, les téls de personnes suspectées sont infiltrés, on peut alors avoir accès à la totalité du téléphone, aux photos, messages sur conversation chiffrée etc. Il suffit d'un mauvais clic, sur un MMS envoyé d'un numéro inconnu, d'un lien dans un mail, d'un message sur Whatsapp. Les failles de sécurités sont nombreuses. Ce n'est pas à la portée de Roger au comico du coin, mais les renseignements type DGSI savent faire, ça s'est vu sur des enquêtes concernant des militant·es écolos ou autonomes, ou dans le cadre d'affaire de terrorisme.

Avec ces logiciels espions, les flics peuvent aussi activer à distance le micro ou la caméra du téléphone pour procéder à des enregistrements. Il est alors bon de tenir loin votre téléphone lors de conversations sensibles, lors de réunion etc. Tout tél ou matos informatique qui tombe entre les mains des flics en cas de perquisition et de saisie, de GAV est à ne plus utiliser, parce que vous ne savez pas ce qu'a fait la police avec, et vous pouvez bien vous retrouver avec du matos infecté.

Pour la navigation web, nous vous conseillons de passer sur ordinateur via Tor. Néanmoins il existe l'appli *TorBrowser* sur smartphone qui permet de se connecter au réseau Tor. Nous y reviendrons plus loin. Il est possible d'installer *Orbot*, une appli qui fait passer les connexions de n'importe qu'elle autre aplli par le réseau Tor., avec le mode RPV. Utiliser un VPN ne manière permanente peut compliquer la tache pour surveiller votre trafic internet, mais cela n'est pas infaillible. Tout est stocké sur un serveur central, qui peut faire l'objet de réquisition en cas d'enquête, la justice pouvant demander à l'hébergeur de fournir les données contenues dans un serveur. Pour l'activité militante sur internet nous vous conseillons grandement d'utiliser seulement Tor, installé sur votre ordinateur, et Tails, un système d'exploitation non-persistant. Nous y reviendrons aussi plus tard.

Sur ordinateur

Sur ordinateur, il est plus facile de se protéger. Des méthodes de chiffrement avec VeraCrypt pour travailler sur des documents sensible en passant par le système Tails pour ne pas laisser de trace, il existe plusieurs solutions afin d'avoir l'esprit plus serein.

Tor Browser

Les activités militantes sur ordinateur, c'est avant tout de la communication et de la recherche d'information. Mais comment faire tout cela sans se faire attraper ? Pour l'accès à internet, c'est par TorBrowser que ça se passe. C'est un navigateur web qui ressemble à Firefox, qui se connecte au réseau Tor.
Qu'est-ce que Tor ? C'est un réseau décentralisé de milliers d'ordinateurs dans le monde qui servent de relais afin de faire rebondir votre connexion sur trois noeuds (des serveurs) différents, masquant ainsi votre véritable adresse IP. Cette adresse identifie de manière unique un appareil connecté au réseau. Celle-ci sera alors connue par le site que vous visitez, et les intermédiaires (votre FAI, fournisseur d'accès à internet) seront au courant des pages que vous consultez.